

WHERE DEMOCRACY'S DEFENCES AGAINST HYBRID THREATS ARE FAILING IN THE CZECH REPUBLIC AND SLOVAKIA

AUTHORS

Veronika Víchová, Andrea Michalcová, Lucia Macháčková

CENTRE FOR AN INFORMED SOCIETY

Daniel Milo, Domician Zahorjan, Patrik Haburaj

NEST INSTITUTE



gerulata



The Center for Informed Society (CIS) is a non-governmental, non-profit organization that is not affiliated with any political party. Our vision is a resilient and self-conscious democratic society that is not subject to authoritarian tendencies, defends human rights and the rule of law, and does not discriminate against anyone.

www.informedsociety.cz



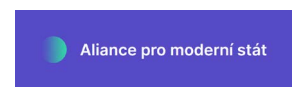
The New Security Threats Institute (NEST Institute) is a civil association whose aim is to raise awareness of threats affecting the security of the Slovak Republic and other EU countries. The Institute is also a platform for research, education and communication, especially on the topic of hybrid threats, as these threats are crucial for the security of citizens and the preservation of democracy in Slovakia. Its ambition is to provide proposals for solutions based on expertise, data and examples of good practice.

www.nest-institute.org



The publication was prepared within the framework of the project **Insurance of the democratic system** with the support of the Alliance for a Modern State. The project strengthens democratic institutions in the Czech Republic, prevents their weakening and destabilization through legislative changes and monitoring of the implementation of already enforced changes.

www.modernistat.org



gerulata

The content analysis of social platforms in the preparation of the case studies was carried out using the Juno tool with the support of **Gerulata Technologies**.

The views expressed in this publication are those of the authors and do not reflect the views of donors and other partners.

CONTENTS

PREAMBLE	6
KEY FINDINGS	7
SLOVAKIA	7
CZECH REPUBLIC	8
KEY RECOMMENDATIONS FOR CZECH POLITICAL AND STATE INSTITUTIONS	10
NON-LEGISLATIVE MEASURES	10
LEGISLATIVE MEASURES	11
INTRODUCTION	13
METHODOLOGY	14
ANALYSIS OF THE POLITICAL, LEGAL AND INSTITUTIONAL FRAMEWORK	16
RESPONDENT RATINGS:	17
LEGAL FRAMEWORK	18
Slovakia	18
Czech Republic	21
Summary of the state of legislative frameworks	23
PUBLIC POLICIES	24
Slovakia	25
Czech Republic	28
INSTITUTIONAL CAPACITY	32
Slovakia	32
Czech Republic	34
Analysis of capacity, funding, processes and policy prioritization	38
Summary	40

CASE STUDIES 41

HYBRID ACTION41

- CASE STUDY 1:** Successfully uncovering Russian intelligence activities in Slovakia 41
- CASE STUDY 2:** Brat za brata 45
- CASE STUDY 3:** A Czech Foreign Ministry Employee Leaked Information to the Russian Secret Service 48
- CASE STUDY 4:** Sanctions Legislation in the Czech Republic 52

DISINFORMATION 57

- CASE STUDY 1:** Successful government response to an information operation related to the redevelopment of a cemetery in Ladomirová 57
- CASE STUDY 2:** Website blocking 61
- CASE STUDY 3:** Spreading disinformation about refugees from Ukraine 65
- CASE STUDY 4:** Unveiling the Voice of Europe network 71

STRATEGIC COMMUNICATION76

- CASE STUDY 1:** Creating a strategic communication system in the Slovak Republic 76
- CASE STUDY 2:** Lack of Strategic Communication of the Slovak Government on Values Related to Homeland Defense 80
- CASE STUDY 3:** Ministry of the Interior's Wall Campaign 84
- CASE STUDY 4:** Strategic Communication Associated with the Czech Munitions Initiative for Ukraine 89

RECOMMENDATIONS FOR CZECH POLITICAL AND STATE INSTITUTIONS 94

GENERAL RECOMMENDATIONS 94

- Short-term framework 94
- Long-term framework 95

HYBRID THREATS AND DISINFORMATION 96

- Short-term framework 96
- Long-term framework 97



STRATEGIC COMMUNICATION	97
Short-term framework	97
Long-term framework	99

PREAMBLE

The information space has become a battleground where hybrid threats, including disinformation and influence operations, threaten the foundations of our democracy. As [the BIS Annual Report 2023](#) points out, Russia represents the greatest threat to the security of the Czech Republic, Europe and the world. Russian intelligence services use the virtual environment to recruit agents and spread disinformation to undermine our support for Ukraine and destabilize the European security system. This warning is crucial - this is not a theoretical threat, but the everyday reality in which our democracy operates.

Slovakia is a cautionary example of how Russian influence operations can effectively undermine democratic processes. The inaction of the democratic government in actively defending the state against hybrid threats, the confused communication, the lack of coordination of state institutions and the normalization of Russian narratives in society have enabled the return of Robert Fico who is turning the country towards Russia.

While the Czech Republic has the tools and institutions to combat these threats, their potential is not fully exploited and there is a lack of clear accountability for their implementation. We do not need new strategies, but an effective follow-up to the existing ones. Our publication provides concrete steps on how to put these tools into practice and strengthen national defenses.

The Czech government has one last chance to show political will and act. If it does not act immediately, hybrid threats will further weaken our democracy. The Slovak experience clearly shows that inaction leads to destabilization of the state. If we give space to hostile influences, we risk the future and security of our country.

As the example of Slovakia shows, the threat comes not only from outside, but also from internal political decisions. It is time to act.



ANDREA MICHALCOVÁ

Director, Centre for an Informed Society

KEY FINDINGS

SLOVAKIA

1. State of the legal framework

- There is a lack of legislation to combat hybrid threats and disinformation, with precise definitions and sanctions.
- There is a lack of legislative anchoring of competences and responsibilities for the coordination of measures in this area, which complicates an effective response to threats.
- Enforcement of existing legal instruments is insufficient, especially in the area of hybrid threats.

2. State of public policies

- Insufficient implementation of existing strategic and conceptual documents, which are often only formally adopted and not required to be implemented.
- There is no consensus in the understanding of strategic and conceptual documents, and there is no continuity between strategies and action plans when governments change, which weakens their effectiveness and implementation.
- Insufficient formalization of cooperation with civil society, academia and private companies.

3. State of the institutional framework

- Coordination and communication are insufficient, as the issue has no main coordinator and 'resortism' and formalism prevail.
- There is no position that has a comprehensive overview of security issues and is responsible for political support in dealing with hybrid threats. This role could be filled by a national security advisor or a new specialized institution.
- The absence of units for combating hybrid threats in most state institutions. Specialized units, which still exist after the new government took office, are inadequately staffed. They do not fulfil their originally intended role and are forced to carry out an agenda that is not related to hybrid threats or strategic communication.
- The absence of institutional mechanisms to ensure continuity across policy cycles makes it easy for a new government to dismantle or fundamentally weaken already established strategic frameworks and measures.
- Weak political support and frequent misunderstanding of the topic of hybrid threats by senior government officials.

4. State of professional and financial capacities and internal processes

- Lack of qualified experts for communication, analysis and strategic communication.
- Political appointments to professional positions without the necessary qualifications.
- Technical tools and resources are lacking.
- Financing is dependent on European funds, which limits long-term sustainability.
- Internal procedures are inadequate, lacking binding guidelines and standardized processes.
- Coordination is weak and procedures are inefficient, lacking a coherent and systematic approach.

5. State of political support

- Perception and understanding among politicians is very low, with both government and opposition politicians underestimating the threats and not actively engaging in addressing them. Some even block such measures. The political and professional levels are not always strictly separated.

CZECH REPUBLIC

1. State of the legal framework

- There is a lack of clear definitions of key concepts and some partial legislative shortcomings remain, particularly in the Criminal Code, in the area of political party financing, implementation of sanctions legislation or in the residency agenda.
- There is a lack of legal definition of powers and duties in the area of strategic communication and hybrid threats, which makes inter-agency coordination and effective response to threats difficult.
- Insufficient enforcement of existing legal instruments to combat hybrid threats.
- There is no legal framework to deal effectively with illegal or harmful content in the online space. In public discourse, a law allowing the blocking of websites is often mentioned as a way of providing legal preconditions in case the state has to resort to this rather extreme step. However, the effectiveness and necessity of such a measure is still questionable. Much more serious is the failure so far to adopt the Digital Economy Act, which focuses on defending against harmful and illegal content on social networks and is based on a European Union regulation, namely the Digital Services Act.

2. State of public policies

- Although there are a number of strategies and action plans on hybrid threats, their implementation is often formal and does not translate into real change.
- There is no clear strategy or action plan on strategic communication or disinformation and no clear structure or responsibilities in these areas.



3. State of the institutional framework

- A new Government Coordinator for Strategic Communication of the State has been appointed and a Department of Strategic Communication has been established at the Office of the Government, which should be responsible for, among other things, coordinating strategic communication across ministries. These newly created institutions should replace the existing informal national coordination. However, it is uncertain whether these functions will be maintained after the forthcoming elections. Their structure, mandate and powers are not enshrined in any statutory, sub-statutory or strategic document or concept.
- Although the area of hybrid threats falls under the purview of the Ministry of Defense, this role is again rather formal and does not include sufficient mandate and capacity to carry out this activity effectively. The National Security Council, or its Expert Working Group on Hybrid Threats, also fails to fulfil this coordinating role.

4. State of professional and financial capacities and internal processes

- There is a shortage of experts in communications, cyber security and other key areas, not only in the force but especially in the non-force ministries. Technical resources and tools are insufficient and information sharing between ministries is not systematic.
- Funding for activities is undersized and not used effectively.
- There is no general consensus within national, regional and local governments on what strategic communication is for and how they can use it. There are no institutional manuals and set processes for crisis communication or response to hybrid threats.

5. State of political support

- Awareness among government politicians is rather rhetorical and does not manifest itself sufficiently in practical measures.

KEY RECOMMENDATIONS FOR CZECH POLITICAL AND STATE INSTITUTIONS

The following measures should be implemented by Czech state and political institutions within the next 12 months to effectively prevent or reduce the impact of hybrid action from the Russian Federation and strengthen the strategic communication of the state.



NON-LEGISLATIVE MEASURES

1. Increasing professional and financial capacity to counter hybrid threats

- Increase capacity for strategic communications and countering hybrid threats, both personnel and financial.
- Ensure sufficient technical equipment, in particular analytical tools for monitoring and analysis of information space and social networks, financial analysis and monitoring of financial flows, etc.

2. Establishment of an independent commission to oversee the implementation of the strategies

- Establish an independent commission composed of experts from the academic, non-governmental and government sectors to monitor the implementation of strategies and action plans aimed at combating hybrid threats.
- This commission should be established by the President of the Czech Republic under the auspices of the Office of the President of the Republic. It would present the results of the interim evaluation to the President of the Czech Republic, the Government of the Czech Republic and other constitutional officials. Upon request, the results of the evaluation should also be made available to the Standing Committee on Hybrid Threats of the Parliament of the Czech Republic and other relevant committees and commissions of the Parliament of the Czech Republic.

3. Introduction of systematic training of civil servants in the field of hybrid threats and strategic communication

- Establish mandatory training and e-learning for government officials from both force and non-force departments, at local and regional level, focused on identifying and responding to hybrid threats and strategic communication.
- Provide all these levels with manuals and recommended procedures for response and communication in the event of a crisis.



4. Improving coordination and information exchange between ministries and other relevant institutions in the field of hybrid threats and communication

- Ensure regular coordination and exchange of information between ministries and other institutions in the field of strategic communication, through a secure online platform and regular meetings. The Department of Strategic Communication should take on the full role of coordinator.
- The National Security Council already has an Expert Working Group on Hybrid Threats, whose members include all relevant institutions involved in the defense against hybrid threats. However, it meets minimally and shows no real coordination activity. The government should require this working group to meet regularly, exchange information, and at the same time monitor the current status and developments in the area of hybrid threats. Outputs from this working group should be actively used by the government to further task and coordinate activities outside the working group.

5. Strengthening cooperation with the non-governmental sector, academic institutions and the private sector

- Systematically support collaboration with NGOs, academia and business working on hybrid threats and disinformation through grants and partnerships.
- Use the analytical capacity of the NGO and academic environment, especially where the state does not have the professional or financial capacity to respond adequately.



LEGISLATIVE MEASURES

1. Approval of the Digital Economy Act

- The Czech government has already approved a draft law on the digital economy, which is crucial for the implementation of the Digital Services Act, a European Union regulation that the Czech Republic is currently not complying with. This law now needs to be urgently debated and passed in the Czech Parliament.

2. Specification of the criminal law in the field of cooperation with a foreign power

- Amend the Criminal Code to clearly define crimes related to espionage (especially the leaking of sensitive but unclassified information) and aiding and abetting the influence of an enemy power.
- Enable the use of intelligence as evidence in criminal proceedings in investigations of hybrid threats.
- According to current information, the amendment to the Criminal Code should reach the Government within a few months. However, Russian influence and espionage operations are intensifying by the month. It would therefore be advisable to speed up the process as much as possible.



3. More effective implementation of sanctions legislation and the fight against money laundering

- By the end of 2024, the Ministry of Justice should draft and submit to the government a bill regulating the criminal version of the confiscation of illegally acquired property, which would also implement the EU confiscation directive.
- The legislative process of implementing the EU directive against the violation of international sanctions should be completed by the end of the parliamentary term. According to this directive, the Czech Republic should enshrine the criminal the illegal nature of violations of certain international sanctions committed through gross negligence and thus strengthen their enforceability. The proposal should also allow for the removal of the object of the international sanction, i.e. the property subject to the international sanction in respect of which the offence of breach of international sanctions has been committed, including property belonging to the community property of the spouses.

INTRODUCTION

Hybrid threats represent one of the most significant challenges for modern democracies, including the Czech Republic and Slovakia. These threats, including disinformation, cyber-attacks, influence operations and other forms of subversion, threaten not only national security, but also the stability of democratic institutions and public trust. This study analyses the approaches of the Czech Republic and Slovakia to defending against hybrid threats, identifies key weaknesses and provides recommendations for strengthening the defense capabilities of both countries.

The study is based on extensive research and analysis of legislative documents, public policies and institutional arrangements in both countries. Based on the assessment of individual areas as well as specific case studies, the main strengths and weaknesses of the current system of defense against hybrid threats in the Czech Republic and Slovakia were identified.

The aim is not only to highlight the current problems but also to offer concrete recommendations for solving them. Proposed actions include legislative changes, strengthening institutional capacity, increasing the efficiency of the use of funds and improving strategic communication. The study also highlights the need for long-term political support and prioritization of hybrid threat issues, which is crucial for the successful implementation of the proposed measures.

Finally, it should be emphasized that defending against hybrid threats requires a comprehensive and coordinated approach involving all parts of society, including state institutions, the academic sector, civil society and the media. This is the only way to effectively face these modern challenges and to protect the democratic values and security of our countries. This study provides not only an analysis of the current state of affairs, but also a clear way forward that can contribute significantly to the Czech and Slovak defenses against hybrid threats.

METHODOLOGY

This study uses a complex methodological approach including analysis of legislative and strategic documents, interviews with experts and case studies, complemented by data analysis of social media.

The research includes an in-depth **analysis of legislative documents, policy documents and security reports** published between 2020 and 2024. We analyzed legal frameworks, national strategies, action plans and other relevant documents to identify the main legislative and policy instruments used to combat hybrid threats and disinformation. Particular attention was paid to changes in legislation and the implementation of strategic documents in response to current threats.

In each country, at least 10 current or former government employees working on hybrid threats, strategic communications or disinformation were interviewed. These individuals will not be named, but the information gathered from these **semi-structured interviews** is key to understanding the practicalities and challenges in these areas. Respondents also provided their own numerical ratings for each area based on a standardized questionnaire, which allowed for a quantitative analysis of experts' views on the effectiveness of ongoing measures. It should be stressed that while this numerical assessment helps to understand the current situation in a given country, it cannot be seen as completely accurate. In spite of the numerical scale with explanations provided, an inevitable part of the respondents' assessment is their subjective impression of the situation, and therefore the resulting figure can be perceived as the respondents' level of satisfaction with the situation rather than a completely objective and unchanging assessment.

To illustrate specific threats and responses to them, case studies have been selected that meet the following criteria:

- **Country specific:** Each case study focuses on local vulnerabilities and the country context.
- **The element of foreign influence:** Each case study includes an element of foreign (primarily Russian) influence, either through direct actor connections to Russia or data analysis showing foreign influence.
- **Apolitical focus:** Case studies do not focus on domestic political disputes, but may include domestic political actors as actors or objects of hybrid campaigns.
- **Timeliness:** The case studies focus on events from January 2020 and later.
- **Response focus:** Each study demonstrates the countermeasures taken by government and state structures and/or civil society, or lack thereof.

The case studies were selected in the following categories:

- **Hybrid:** A state's response to country-centric operations that involve multiple aspects that fall under hybrid operations (e.g. economic influence, espionage, strategic corruption, etc.).
- **Information operations:** State response to specific information and disinformation campaigns with a wide impact.
- **Strategic communication:** Implemented state communication campaigns aimed at combating disinformation and foreign influence and systemic state measures in the field of strategic communication.

For the case studies, **social media data analysis** using the Juno tool from Gerulata Technologies was used. This tool allows for the analysis of trends and information dissemination on social media, identification of key actors and the links between them. By using this tool, we were able to quantify the impact of individual measures in the information space and better understand how this information is disseminated and influences events in society and who the main disseminators are.

The timeframe for social media data analysis varied across case studies as examined events occurred in different times, but no impacts were measured beyond May 2024. Unless otherwise specified in the chapters discussing individual case studies, data visualizations, also created using Juno, were prepared in December 2024.

When it comes to the terminology we used while examining different groups active in social media information space, if not stated otherwise within the different case studies, it involved following:

- **Reliable sources** which consisted of:
 - **Mainstream media** – Established and trustworthy media outlets.
 - **State StratCom** – Accounts engaged in the strategic communication of the state, such as official accounts of the president, the Office of the Government, the prime minister, the presidents of the Chamber of Deputies and the Senate, ministers, ministries, state administration, the army, and the police.
 - **Civil society**
- **Quasi-media and disinformation actors**
- **Politicians and political parties** – Official accounts of politicians and their political parties.

These groups were selected because of their direct involvement within the case studies and their noticeable presence on social media while communicating events examined within the case studies.

The methodology of this study combines qualitative and quantitative approaches, using a wide range of sources and tools to provide a comprehensive picture of defense against hybrid threats and disinformation in the Czech Republic and Slovakia. This approach enables not only the analysis of the current state of affairs, but also the formulation of concrete recommendations for improving and strengthening the defense capabilities of these countries.

ANALYSIS OF THE POLITICAL, LEGAL AND INSTITUTIONAL FRAMEWORK

This chapter focuses on a detailed assessment of the legal, institutional and policy framework of the Czech Republic and Slovakia in the field of defense against hybrid threats and disinformation. The research is based on analysis of legislative and strategic documents, interviews with experts and quantitative assessments of individual areas provided by respondents. The respondents, which included current and former government employees, provided valuable insights and numerical ratings on a scale of 1 to 5 (similar to grading at school), which allows for a comparison of the state of each aspect in both countries and a somewhat subjective assessment of the situation by the respondents. At least 10 respondents were interviewed in each country.



Within this chapter, we will focus on several key areas:

1. **Legal framework:** We analyze existing legislation and identify its weaknesses and strengths in the context of combating hybrid threats and strategic communications.
2. **Public policies:** We evaluate strategic documents and their implementation, including concepts and action plans focused on hybrid threats, disinformation and strategic communication.
3. **Institutional capacity:** We are examining the organizational structures and capabilities of the various institutions involved in defending against these threats, and in strategic communications.
4. **Personnel and technical capacity:** We assess the number, qualifications and equipment of personnel in the area of strategic communications and hybrid threats.
5. **Funding:** We analyze the financial resources allocated to countering hybrid threats and strategic coordination and their effectiveness.
6. **Effectiveness of procedures:** We assess the effective implementation and use of procedures and the familiarity of institutions and their staff with these procedures.
7. **Political support:** We assess the level of political support and prioritization of the topics of hybrid threats and strategic communication.

This chapter provides a comprehensive look at how both countries are equipped to address current and future challenges associated with hybrid threats and identifies areas where improvements are needed. The goal is to provide a basis for formulating specific recommendations that can contribute to strengthening both countries' defenses and resilience to these advanced threats.

RESPONDENT RATINGS:

This is not an exact assessment of the situation. The following table is not a clear assessment of the situation, but a subjective assessment of the respondents from the public administration who expressed their personal satisfaction and view of the situation in the country in this way. This can be influenced by a number of factors, including the current political situation. For example, Slovak respondents included former employees of departments that dealt with hybrid threats and disinformation in 2022-2023, but at the time of the interviews, Slovakia was undergoing major changes that caused the closure or disintegration of a number of institutions and activities in this area.

Country:	 Slovakia	 Czech Republic
Overall rating:	4,25	3,11
Legal framework	4,41	2,55
Public policies	4,23	3,60
Institutional capacity	4,36	3,15
Staff and technical capacity	4,05	3,35
Funding	3,86	3,06
Efficiency of procedures	4,36	3,40
Political priority	4,45	2,65

Each of the respondents rated each area on a 1-5 point scale, following the pattern of grading in schools. Specifically, the point scale was labeled as follows:

- **Excellent (1 point):** The situation is extremely positive and does not require any major changes or action.
- **Very good (2 points):** The situation is positive but there is room for further improvement.
- **Average (3 points):** The situation is stable but needs to be improved.
- **Below average (4 points):** The situation is problematic and needs immediate improvement.
- **Insufficient (5 points):** The situation is critical. Urgent action is needed.

LEGAL FRAMEWORK

Country:	 Slovakia	 Czech Republic
Scoring:	4,41	2,55
Summary:	<p>The legal framework is assessed as insufficient. There is a lack of legal norms aimed at combating hybrid threats and disinformation. There are no clear definitions of these threats in the law, which causes inconsistency and inefficiency in the application of the law. There is also a lack of law enforcement and problems with the application of existing legal instruments that could be used in these areas.</p>	<p>The legal framework is assessed as average. Weaknesses were identified in the lack of legal definition of relevant terms. There is also a lack of effective and transparent tools for blocking websites in crisis situations. The law of competence does not include competences in the field of hybrid threats and strategic communication, which makes coordination difficult. Partial shortcomings were also identified in the financing of political parties, the implementation of sanctions legislation or the granting (or withdrawal) of residence rights to foreigners.</p>

Slovakia

"We have no legislative framework to combat hybrid threats. Even what has been adopted is not working."

Quotes from the research interview

1. Missing definitions of terms

The basic problem of legal regulation of hybrid threats in Slovakia and related phenomena is the lack of legal definition and definitional framework of many basic terms. Some of them are present in public policies, but for reasons of legal certainty, clarity and predictability it would be advisable to enshrine them in legislation.

The Slovak legal system lacks legal definitions of the following terms:

- Hybrid threat
- Hybrid action
- Disinformation
- Misinformation
- Malinformation
- Influence operation
- Semi-military group and others

This lack of terminology causes application problems when using legal precepts to regulate conduct or sanction activities that fall within the realm of hybrid threats. When it is necessary to regulate or sanction such activities, the accepted conceptual apparatus cannot be used.

In practice, this deficiency was manifested, for example, in the introduction of the institute of blocking websites by an amendment to the Act on Cyber Security (Act No. 69/2018 Coll.). Although the February 2022 amendment introduced the possibility of blocking malicious activity that included "serious disinformation and other forms of hybrid threats". However, neither of these terms was (and still is) defined in Slovak law at that time.

The same problem exists with the other two pieces of legislation. Act on Military Intelligence No. 500/2022 Coll. in Section 5, the Military Intelligence Service's remit to obtain and evaluate information also covers hybrid threats and disinformation if they threaten the defense or defense capability of the Slovak Republic, but nowhere does it define these terms. In the amendment to Act No 110/2004 Coll. on the functioning of the Security Council of the Slovak Republic in peacetime, the Committee on Hybrid Threats was established as one of the committees of the Security Council of the Slovak Republic (hereinafter referred to as the SRSC) without any legal definition of this concept. The regulation of this concept in the statute of the committee or in public policies does not replace the legal definition and causes problems in application in practice.

2. Insufficient legislative anchoring of competences and identification of primary responsibility for combating hybrid threats

Given the breadth and complexity of the hybrid threat issue, which affects the competencies of many (if not all) ministries and takes many forms, it is necessary to clearly define the competency frameworks and coordination between the individual central government authorities (CAOs). While the current wording of the Competence Act (Act No. 575/2001 Coll.) sets out general principles, including the provision of cooperation, exchange of information or the processing of analyses in the area of assigned competences, none of the SAIs has a clearly defined remit in the area of hybrid threats among its competences.

The partial solution of amending the Act on the functioning of the Security Council of the Government of the Slovak Republic in times of peace did not resolve the primary competence in this area. A committee of an advisory body of the Slovak Government (which, moreover, according to the information from the interviews conducted, has not yet met even once) cannot replace the actual exercise of competences and coordination of activities in such a crucial area. Given that hybrid threats are characterized by an inter-ministerial to inter-sectoral nature, the absence of a clear definition of competences and coordination of the execution of measures in this area significantly reduces the resilience of the whole society to this type of threats.

3. Sub-sectoral and sectoral legislation

A separate problem is the shortcomings of legislation in individual sub-areas related to the issue of hybrid threats. Due to the limited scope of this analysis, only a selection of some of the legislation that touches on this issue is presented below.

- **Elections, campaigns and financing:**

- Influencing political parties and their covert funding is a frequently used tool of hybrid influence and has been demonstrated in many cases¹. Although Slovakia formally prohibits foreign financing of political parties and political campaigns in Act No. 181/2014 Coll. on Election Campaigns, it is relatively easy to circumvent this prohibition through third parties (legal or natural persons from Slovakia). The source of financing of donations to political parties and campaigns does not need to be proven in any way, nor does the adequacy of the donation to the donor's income need to be examined.
- With the growing importance of the internet and social media in particular for election campaigns, the current legal framework appears inadequate. The current forms of election campaigning in the online space go beyond the existing legal framework, which at the time of its creation could not respond to the significant increase in the importance of this way of campaigning. Examples are online-only TV and radio stations, influencers (where it is unclear whether and when they report for payment), deepfake audio and video messages, automated networks of social media accounts. These and many other specific forms that election campaigns take in the online environment require more precise and clearer regulation.

- **Operation of paramilitary groups:**

- The issue of paramilitary groups usurping the competences and powers reserved for state armed forces is very broad and complex. The key to their meaningful regulation, however, is a clear definition of the term. In Slovakia, there is no legally binding definition of the term paramilitary group that contains a clear definition. The absence of such a definition means that the state's activities in this area are not conceptual and predictable. In fact, paramilitary groups can be considered to be a whole spectrum of organizations characterized by the use of uniforms, military training and the handling of weapons or imitation weapons. A clear distinction should be made between those that pose no security risk (military history clubs, airsoft associations, shooting clubs) and organizations preparing for armed action against the state or linked to a foreign power.

- **Application of international sanctions:**

- Application practice has shown problems in the implementation of measures related to international sanctions. In particular, the unclear definition of the powers of internal state authorities in the law on the implementation of international sanctions seems to be problematic.

1 The Russian bank's loan to the French Front National, the covert financing of the Italian La Liga from the proceeds of Russian oil sales.

"We have legislation. But we don't have enough case law and we don't have the effort to enforce the law consistently."

Quote from the research interview

Hybrid threats, disinformation and strategic communication are also areas in the Czech Republic where legislative regulations show shortcomings similar to those in Slovakia.

1. Missing definitions of terms

Czech legislation, like Slovak legislation, does not know the terms "disinformation" or "hybrid threats". These terms are not legally enshrined and are only punished if they fall under the general criminal offences defined in the Criminal Code (Act No. 40/2009 Coll.). Such offences may include, for example, damage to the rights of others (Section 181), defamation (Section 184), espionage (Section 316), defamation of a nation, race, ethnic or other group of persons (Section 356), spreading of alarmist news (Section 357) and other offences. However, respondents to our survey largely agree that, with the exception of the as yet non-existent offence of "collaboration with a foreign power", the lack of a definition or the lack of legislation in general is not the central problem in these areas.

2. Legal regulation of website blocking

The Czech Republic, unlike Slovakia, has no legislation for blocking websites. This situation proved problematic during the crisis in early 2022, when some websites spreading disinformation related to the full-scale invasion of Ukraine by the Russian Federation were shut down by the domain provider NIC.cz. However, blocking websites without a legal basis is controversial in terms of legal certainty and freedom of speech, and its absence may limit the state's ability to respond effectively to these crisis situations.

3. Lack of powers and responsibilities in the area of hybrid threats and strategic communication in the Competence Act



The Czech Republic also lacks clear competences, responsibilities and boundaries in the area of hybrid threats or strategic communication at the legal (and in the case of strategic communication also sub-legal) level. The Competence Act (Act No. 69/1993 Coll., the Act of the Czech National Council on the Establishment of Ministries and Other Central Bodies of the State Administration of the Czech Republic) does not contain any defined competences in the area of hybrid threats and strategic communication, which may complicate the coordination between the individual state administration bodies. This proves to be a significant problem when trying to effectively respond to hybrid threats, which require inter-ministerial cooperation and coordination, but also when assigning the responsibilities of individual sub-activities related to the area of hybrid threats.

4. Sub-sectoral and sectoral legislation

- **Financing of political parties from abroad:** similarly to Slovakia, the Czech legislation shows shortcomings in individual sub-areas related to hybrid threats. Almost identical problems can be identified in the case of Act No. 424/1991 Coll., on Association in Political Parties and Political Movements, which regulates the financing of political parties, both in the possibility of circumventing the ban on foreign financing through third parties, and in the area of campaigning on the Internet and social networks, which go beyond the scope of regulation and require more precise regulation.
- **Penalty legislation:** On the other hand, the adoption of the Sanctions Act (1/2023 Coll.) and the significant amendment to the Act on the Implementation of International Sanctions (240/2022 Coll.), which was adopted in response to full-scale Russian aggression in Ukraine, were viewed very positively. The Czech legislation allows, among other things, for the placement of legal and natural persons who violate the factual grounds determined by the EU sanctions regimes on the national sanctions list. According to the respondents' assessment, the weaknesses of this legislation do not lie only in the legislation itself. Rather, it is often the lack of state capacity to implement them, the complexity of judicial review and the complicated coordination between a wide range of state institutions and bodies.
- **Weaknesses in the residency agenda:** The residence agenda is regulated in Act No. 236/1999 Coll., i.e. the Act on the Residence of Foreigners in the Czech Republic. However, according to the respondents' assessment, this legislation does not sufficiently reflect the security interests of the state and, when granting residence permits, it disproportionately favors persons who may pose a security risk but have sufficient financial resources to ensure the conditions of residence and other supporting circumstances (such as establishing a company in the Czech Republic, purchasing real estate in the Czech Republic, quality legal services, etc.). The fact that the right of residence (like citizenship) cannot be revoked if it is retrospectively established that it was obtained illegally, for example on the basis of forged documents, was also identified as problematic.

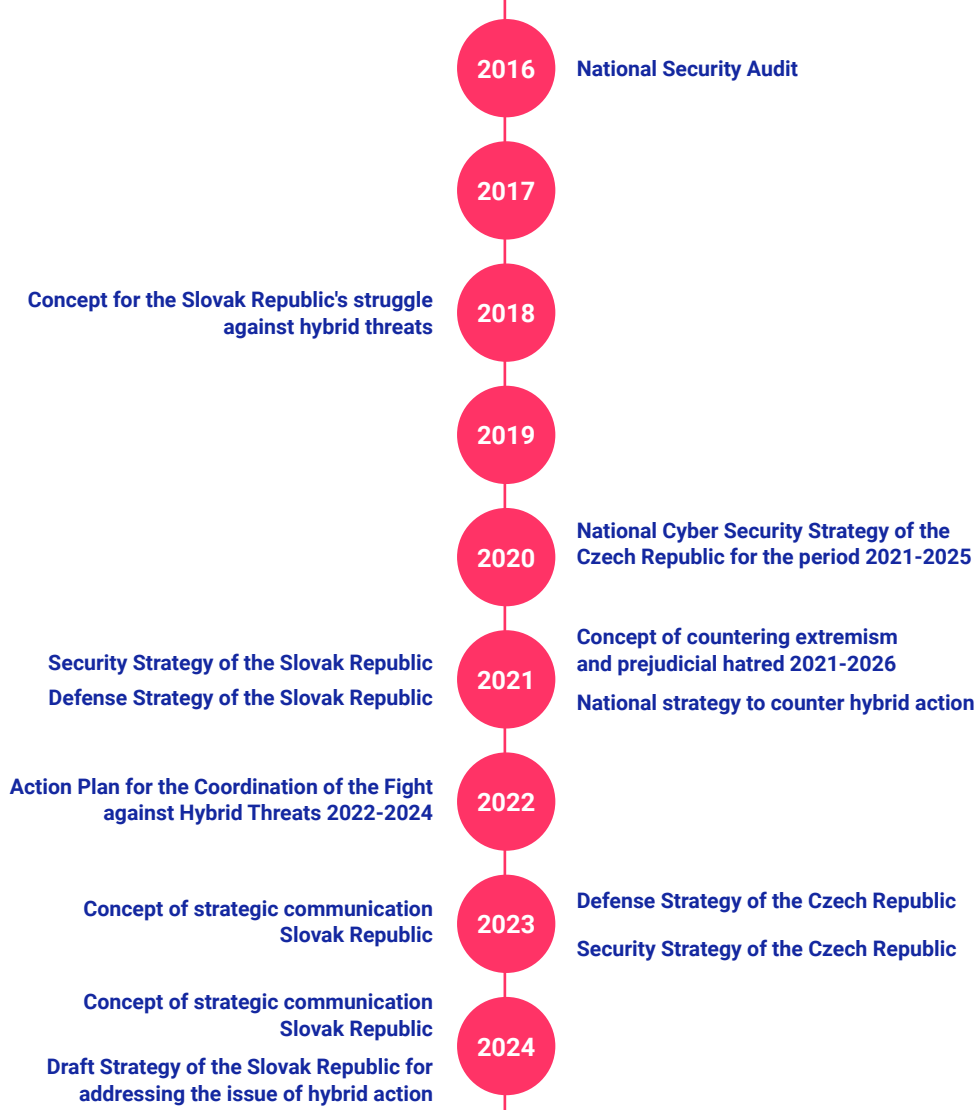
Summary of the state of legislative frameworks

The Czech Republic and Slovakia face similar challenges in the areas of hybrid threats, disinformation and strategic communication, particularly in the absence of legal definitions and clear lines of authority. The Czech Republic has some legislative arrangements but suffers from a lack of consistent enforcement, while Slovakia has problems with unclear legislation and coordination between authorities. Both countries need to improve their legal frameworks and implementation capacities to better counter hybrid threats.

 Slovakia	 Czech Republic
Missing definitions of terms:	
The lack of consensus and legal definitions of hybrid threats, disinformation, misinformation, and more.	
Legal regulation of website blocking:	
There is an Amendment to the Cyber Security Act 2022, but the terms are not clearly defined.	There is no legislation, which proved problematic during the Russian invasion of Ukraine in 2022.
Lack of clear powers and responsibilities:	
There is no clear definition of competencies and coordination between different authorities in the field of hybrid threats, which reduces the effectiveness of the state response.	It lacks clear competences and responsibilities in the area of hybrid threats and strategic communication.
Enforcement:	
There is a lack of legislative framework and definitions of terms, which leads to problems in law enforcement and lack of coordination.	Although definitions are also lacking, applicable legislation exists. However, there is a lack of sufficient case law and a strong effort to enforce the law.
Specific legislation and implementation of sanctions:	
In this area, insufficient legislation or setting of responsible functions in this area was also identified.	Sanctions legislation allows for the placement of persons on the national sanctions list, albeit with capacity problems in implementation.
Sub-sectoral and sectoral legislation:	
There is a lack of regulation in the area of political party financing, the operation of paramilitary groups and the application of inter-national sanctions.	Identical problems with the financing of political parties as in Slovakia, positive impact of the Sanctions Act and the Act on the Implementation of International Sanctions, shortcomings in the residency agenda.

PUBLIC POLICIES

Country:	 Slovakia	 Czech Republic
Score:	4,23	3,60
Summary:	Public policies are rated as inadequate . Across existing strategies and action plans, implementation in practice is weak and depends on political will. Implementation of strategies is often only formal and lacks real action. Changes and abolition of policies adopted by the previous government weaken the measures taken in this area.	Public policies are rated as below average . The Czech Republic has several strategies and action plans, but their implementation is often rather formal, with no effort to bring about real change. Existing strategies often lack concrete measures. There is also a complete lack of an Action Plan on disinformation and strategic communication and a clear set of structures and responsibilities in these areas.



"We have adopted documents, but they are often not implemented and there is a lack of follow-up."

Quote from the research interview

Strategies aimed at combating hybrid threats began to be prepared in the Slovak Republic in 2017. This was a response to the strategies adopted at the EU level, which in 2016 adopted the first measures in this area in the Common Framework for Combating Hybrid Threats.² The EU in its global strategy³ defined hybrid threats as one of the main security challenges, to which Slovakia responded by adopting the first concept paper in 2018.

The main concepts in the field of hybrid threats and strategic communication in Slovakia are as follows (in chronological order):

Concept for the Slovak Republic against Hybrid Threats (2018)

It is the main concept document in the field of hybrid threats⁴, and also the only document adopted in this field until 2021. The concept provides a proposal for an institutional framework and measures to increase the resilience of the state. It also defines for the first time the biggest hybrid threats to the Slovak Republic as part of the EU and NATO. It proposes an institutional framework, the aim of which is not to create a new institution, but to make effective use of existing security risk assessment systems by individual institutions.⁵ The Concept provides a framework for measures to increase resilience and also emphasizes effective prevention through raising public awareness of hybrid threats.

Security Strategy of the Slovak Republic (2021)

The Strategy defines one of the strategic security interests of the Slovak Republic as "the ability of the state and society to respond to hybrid threats, including disinformation, in an effective and coordinated manner."⁶ The Strategy identifies the most significant manifestation of hybrid action as the targeted spread of propaganda and disinformation against the democratic system and the Slovak Republic's anchorage in NATO and the EU. The aim of these activities is also to influence political decision-making and public opinion, the results of democratic electoral processes, to polarize society and sow distrust of the public towards the state, to question the value orientation of society, as well as to manipulate various groups of the public in order to negatively affect the implementation of the security interests of the state.

2 A common framework for countering hybrid threats European Union response. 2016. European Commission. April 6, 2016. <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018>.

3 European Union. 2016. "Shared Vision, Common Action: A Stronger Europe a Global Strategy for the European Union's Foreign and Security Policy." https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

4 "Material detail | Portal OV." 2018. Rokovania.gov.sk. 2018. <https://rokovania.gov.sk/RVL/Material/23100/1>.

5 Ibid.

6 "SECURITY STRATEGY OF THE SLOVAK REPUBLIC". n.d. Accessed August 28, 2024. https://www.vlada.gov.sk/data/files/8048_bezpecnostna-strategia-sr-2021.pdf.

The strategy in the area of countering disinformation and propaganda defines a focus on the creation of a coordinated national mechanism to strengthen structures and decision-making processes for the early identification, assessment and response to influence and disinformation, as well as the implementation of systemic measures. Within the framework of strategic communication, the strategy defines the intention to actively present foreign policy and security interests of the Slovak Republic, develop the capacity of public administration and strengthen cooperation with the non-governmental, academic and media sectors.

Defense Strategy of the Slovak Republic (2021)

The strategy⁷ identifies propaganda and disinformation as security risks that threaten the stability of the democratic system and undermine citizens' trust in the state. It stresses the need to strengthen the state's resilience to military and non-military threats, including hybrid actions, and defines the role of the Slovak Armed Forces in this area. It also stresses the importance of strategic communication and public debate for the long-term continuity and social support of defense policy.

Action Plan for the Coordination of Countering Hybrid Threats 2022-2024 (hereinafter referred to as "APHH") (2022)

The Action Plan⁸ is based on the Security Strategy of the Slovak Republic until 2021 and the Program Statement of the Government for the period 2021-2024. The aim of the APHH is to address the coordinated action of foreign and domestic actors against the interests of the Slovak Republic in order to strengthen the resilience of state institutions and society to hybrid threats. Hybrid threats may include interference in elections, strategic corruption, negative impacts on foreign investment, dissemination of hate content and disinformation, etc.

The plan includes specific tasks aimed at raising public awareness, building inter-agency cooperation, creating a system of strategic communication and strengthening international cooperation. The document defines active cooperation between the state and the economic sector, academia and civil society as the basis for successful implementation.

7 "DEFENCE STRATEGY OF THE SLOVAK REPUBLIC APPROVED BY THE NATIONAL COUNCIL OF THE SLOVAK REPUBLIC ON JANUARY 27, 2021." n.d. Accessed August 28, 2024. https://www.vlada.gov.sk/data/files/8049_obranna-strategia-sr-2021.pdf.

8 "Material detail | Portal OV." 2022. Rokovania.gov.sk. 2022. <https://rokovania.gov.sk/RVL/Material/27021/1>.

Strategic Communication Concept of the Slovak Republic (2023)

The concept of strategic communication⁹ is part of the Action Plan for the Coordination of Combating Hybrid Threats for the period 2022-2024 (see above). The aim of the Concept is to increase citizens' trust in the democratic institutions of the state and to increase public awareness and support for the long-term strategic interests of the Slovak Republic. The Concept has defined a framework for increasing public awareness of state activities and services and for improving communication between the state and citizens. It set up mechanisms for more effective cooperation of state institutions in the field of strategic communication with the involvement of the academic, media, private and non-governmental sectors with the intention of ensuring a faster response of the state in the fight against disinformation.

Strategic Communication Concept of the Slovak Republic (2024)

This concept¹⁰ provides a new framework for strengthening the state's ability to communicate effectively and in a timely manner with the public. The aim of the Concept is to ensure unified and coherent state communication aimed at informing citizens about government priorities, decisions and results. According to the draft report, the purpose of this document is to "eliminate the absence of a systemic anchorage mechanism for coordinated strategic communication, which allowed mainly foreign and domestic NGOs to arbitrarily implement the strategic communication of the state without taking responsibility for its impact on Slovak society".¹¹

With regard to the previous Concept of Strategic Communication of the Slovak Republic adopted in summer 2023, the form, language and measures are a step backwards, which, moreover, completely neglects the society-wide approach and confuses government communication with state communication.

Draft Strategy of the Slovak Republic for Addressing the Issue of Hybrid Operations (2024)

The draft strategy¹² defines a systemic approach of the Slovak Republic to strengthen its security and defense capabilities as well as the resilience of the state and society to hybrid actions. The proposal has the ambition to establish a functional model of an institutional framework consisting of processes for collecting and evaluating indicators, management and coordination, as well as policy development and implementation in the field of hybrid action.

9 "Resolution detail | Portal OV." Rokovania.gov.sk. 2023. <https://rokovania.gov.sk/RVL/Resolution/20958/1>.

10 "Resolution detail | Portal OV." Rokovania.gov.sk. 2024. <https://rokovania.gov.sk/RVL/Resolution/21521/1>.

11 "SUBMISSION REPORT." n.d. <https://rokovania.gov.sk/download.dat?id=5AAB64AFB46F4240B1DC1DA7C4A1C5EB-2DB70C4D5D383ACF396140E07D3A0EB7>.

12 "Legislative Process - SLOV-LEX." Slov-Lex.sk. 2024. <https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2024/291>.

Czech Republic

"We can write good strategies, but nobody follows them. Partly because of the state apparatus' inability to work with them and partly because of politicians who throw pitchforks into it."

Quote from the research interview

"There is no document that clearly articulates a strategy, or at least a framework for strategic communication. This leads, among other things, to a misunderstanding within the administration of what it actually is."

Quote from the research interview

The main policies in the area of hybrid threats and strategic communication in the Czech Republic are as follows (in chronological order):

National Security Audit (2016)

This document, prepared on the basis of the Prime Minister's assignment in 2016, focuses on ten areas of threats that have been identified as crucial for the Czech Republic. Among these threats are (1) hybrid threats and their impact on the security of the citizens of the Czech Republic and (2) the influence of foreign powers. Each threat is analyzed in the document in terms of its potential impact, but also in terms of the Czech state's ability to identify and respond to this threat. The document also describes the main responsibilities of institutions in each area and includes a number of specific recommendations to address the most serious weaknesses of the state. The National Security Audit was also accompanied by an Action Plan elaborating the recommendations into individual tasks and measures with the given gestors. However, this document is not public.

National Cyber Security Strategy of the Czech Republic for the period 2021-2025 (2020)

This strategy, prepared by the National Cyber and Information Security Agency (NÚKIB), identifies priorities for the period in the area of cyber security, which can certainly be and is the domain of hybrid action. Interestingly, the NÚKIB also includes strategic communication among its strategic objectives and says that intensive strategic communication should be set up both within the country and internationally.

Concept for Countering Extremism and Prejudicial Hatred 2021-2026 (2021)

Among other things, the concept points to the connection between extremism and prejudiced hatred and the spread of disinformation to the public, including by non-democratic foreign countries. It also mentions the work of both domestic and foreign conspirators and disinformers. One of the goals of the concept is to strengthen the ability to combat disinformation with xenophobic elements so that the Czech Republic is able to respond to disinformation waves. Specifically, it proposes raising the qualifications of experts, networking and creating platforms

for cooperation between security forces, institutions dedicated to cyber-security, civil society, academics and the commercial sector. An Action Plan was later developed to accompany this concept.

National Strategy for Countering Hybrid Action (2021)

The strategy is based on the then valid security strategic documents of the Czech Republic and sets three strategic goals in the area of countering hybrid action: (1) a resilient society, state and crisis infrastructure, (2) a systemic and holistic approach, and (3) the ability to respond adequately and in a timely manner. Although the strategy provides a description of what a hybrid attack might look like, the document does not include specific cases or actors that pose this threat. Among other things, it aims to build a strategic communication system capable of effectively communicating information to the public, both on an ongoing and preventive basis and in crisis situations. This document has also been accompanied by an Action Plan with more specific steps, tasks and responsibilities.

Defense Strategy of the Czech Republic (2023)



This conceptual strategic document prepared by the Ministry of Defense describes itself, among other things, as "a fundamental tool for strategic communication of the government." It describes the systematic hybrid activities to which the Czech Republic is exposed and lists cyber attacks, disinformation campaigns, economic pressure, and sabotage, subversion, and intelligence activities among specific hybrid threats. It identifies the People's Republic of China and Russia as the originators of hybrid activities. The document identifies strategic communication as an important tool for strengthening state and societal resilience. The key role, according to the document, is played in particular by the Office of the Government in the area of coordination of countering hybrid actions and strategic communication of the state, as well as by the Ministry of the Interior in the area of countering hybrid actions threatening internal security.

Security Strategy of the Czech Republic (2023)

Also in 2023, a new Security Strategy of the Czech Republic was issued. Similar to the Defense Strategy, it mentions Russia and the People's Republic of China (and additionally non-state actors) as the primary agents of hybrid action. It also highlights the role of the Ministry of the Interior in preventing and countering hybrid threats and foreign power activities, and emphasizes the importance of strategic communication as a tool for achieving the Strategy's objectives. The document further states that countering disinformation, information operations and efforts to manipulate the information space is a crucial part of strengthening societal resilience, and describes the promotion of information literacy education, strengthening civil society, strategic communication of the state, and capacity building for threat detection and analysis as effective responses to these threats. In the document, the government commits itself to facilitate targeted communication between the public administration, academia, the non-profit and private sectors on security issues. However, the document does not include specific steps and actions that the government or state institutions should take in this regard.

Summary of public policies

The analysis of public policies of the Czech Republic and Slovakia in the area of hybrid threats, strategic communication and disinformation shows that both countries face similar challenges and threats, with a similar level of awareness of these facts, which is reflected in the strategic documents. Although Slovakia showed a higher degree of formal acceptance of the concept of strategic communication and its formalization within state structures and continuity of strategies, this development proved to be unstable and subject to political changes, as the development of strategic communication was not only halted but even regressed with the arrival of the new government. The Czech Republic has so far experienced a lack of implementation of relatively well-written strategies. A key factor for the success of both countries will be to ensure effective implementation of the adopted strategies, to increase the level of cooperation between state institutions and to ensure transparency and public support for these policies.

 Slovakia	 Czech Republic
Strategic documents and their implementation:	
Both countries have developed different, often very good strategic documents and concepts aimed at combating hybrid threats, disinformation and cyber threats. In both cases, however, there is frequent criticism for the lack of implementation of these strategies in practice. In both countries, the implementation of these policies is often perceived as formal, with little real action, which depends on the political will and capacity of the state administration. Moreover, they are adopted without adequate financial provision for the costs needed to implement them.	
Security threats:	
Hybrid threats such as disinformation, propaganda and cyber attacks are considered significant risks in the Czech Republic. Czech strategic documents identify similar threats coming mainly from Russia and China. In the case of Slovakia, the situation was similar until 2023, when new documents and strategies were adopted that reversed this approach in Slovakia.	
The role of strategic communication:	
Both countries recognize the importance of strategic communications as a key tool in combating hybrid threats. Both Czech and Slovak strategic documents include aspects of strategic communication aimed at informing and educating the public. Strategic communication is seen in both countries as a means to strengthen the resilience of society to disinformation and propaganda.	
Enforcement:	
There is a lack of a legislative framework and definitions of terms, leading to enforcement problems and lack of coordination.	Although definitions are also lacking, applicable legislation exists. What is lacking is sufficient case law and a consistent effort to enforce the law.

Institutional framework and specific documents:	
<p>Slovakia has a broader chronological overview of adopted documents in the area of hybrid threats and strategic communication, and some of the documents show more consistency in setting up structures and mechanisms than in the Czech Republic, especially in the area of strategic communication. At present, however, the newly adopted documents (2023-2024) have halted previous developments, contain a number of errors and inaccuracies, and strategic communication is intertwined with governmental and political communication according to the new strategies.</p>	<p>In the Czech Republic, on the other hand, the implementation of strategies is often criticized for the lack of a clearly formulated strategic framework, which leads to a lack of understanding within the state administration. Documents such as the National Security Audit or the National Strategy for Countering Hybrid Activities identify threats and suggest measures, but their implementation is perceived as insufficient. A concrete, transparent and clear distribution of responsibilities and structures between institutions in the areas of disinformation and strategic communication is completely lacking, as is its very concept and priorities. This can lead not only to unclear coordination, but also to a general misunderstanding of what strategic communication actually is and what it is for, both among political representatives and government representatives.</p>
Sub-sectoral and sectoral legislation:	
<p>There is a lack of regulation in the area of political party financing, the operation of paramilitary groups and the application of international sanctions.</p>	<p>Identical problems with the financing of political parties as in Slovakia, positive impact of the Sanctions Act and the Act on the Implementation of International Sanctions, shortcomings in the residency agenda.</p>



INSTITUTIONAL CAPACITY

Country:	 Slovakia	 Czech Republic
Scoring:	4,36	3,15
Summary:	<p>The institutional framework is assessed as inadequate. Despite the reinforcement of the professional services between 2022 and 2023, these services are currently paralyzed or directly abolished and do not fulfil their original purpose. The lack of a clear designation of a lead coordinator in the field of hybrid threats and unclear communication between institutions is also a problem. Political appointments to expert positions and the lack of technical and staffing capacity exacerbate the situation. Cooperation between institutions is minimal and often limited to formal matters.</p>	<p>The institutional framework is assessed as transparent. Although a number of institutions exist, notably in the leading ministries and more recently in the Office of the Government, their coordination mechanisms are not formalized and fully used, their work is not sufficiently resourced and their functioning is not sufficiently stable, as they are subject to possible political changes.</p>

Slovakia

"We have institutions for strategic communication and countering hybrid threats only on paper, in reality they are not fulfilling their intended function."

Quote from the research interview

The Slovak Republic, although facing similar security challenges as many other countries, started to deal with hybrid threats and strategic communication relatively late. The 2018 Concept of Combating Hybrid Threats of the Slovak Republic did not set out a framework for the creation of specialized state administration units, but only defined tasks for already established structures, in particular the Slovak Government Office and the Slovak Information Service. It was only the EU-funded project in 2022 that allowed for the strengthening of existing and the creation of new specialized units focused on hybrid threats and strategic communication, their staffing and technical support. However, after the elections in September 2023, there has been a gradual departure of specialized personnel, the closure or reorientation of some units, and a general degradation of solutions to this security issue.

The following institutions and services are currently active in the field of hybrid threats, disinformation and strategic communication in Slovakia:

National Security and Analytical Centre of the Slovak Information Service: it is a key component in the fight against hybrid threats in Slovakia. It is responsible for monitoring and analyzing information on hybrid threats. It acts as a coordinator in the field of hybrid threats at the national level.¹³

Situation Centre of the Slovak Government Office: it also serves as a national focal point for hybrid threats and fulfills the duties arising from the Concept for Combating Hybrid Threats of the Slovak Republic. It should coordinate and share information with partner intelligence services and security agencies of EU and NATO countries, as cooperation at the international level is key to effectively combat hybrid threats.¹⁴

Department of Strategic Communication of the Office of the Government of the Slovak Republic: responsible for coordinating strategic communication at the national level.¹⁵ In cooperation with other branches of the government, it is to focus on communication with the public and the media, to prepare and implement communication strategies aimed at communicating democratic values and the foreign policy anchorage of Slovakia in accordance with the concept of strategic communication. However, the current state of staffing, with all professional staff having been dismissed in the months following the last parliamentary elections, does not allow for professional and effective preparation of strategic communication, as demonstrated by the absence of strategic communication during the events surrounding the attack on the Prime Minister of the Slovak Republic in May 2024.

Centre for Countering Hybrid Threats of the Ministry of the Interior (CCHT): this is a specialized unit that focuses on hybrid threats in the areas under the jurisdiction of the Ministry of the Interior. The main tasks of the CCHT include prevention, monitoring, analysis and proposing measures within the scope of the Ministry of the Interior, education and awareness-raising, and cooperation with other relevant parts of the state.¹⁶ In the future, the Centre has the ambition to coordinate the tasks of the state administration in building resilience to hybrid threats. Due to a lack of understanding of the seriousness of the issue, the Centre's activities are currently considerably subdued.

Department of Strategic Communications of the Ministry of Defense: since 2022, the Ministry has had a specialized unit dealing with hybrid threats and strategic communications, which to some extent cooperated with the armed forces and military intelligence. After the last parliamentary elections, the leadership of the Ministry of Defense reconsidered the mission of the unit and since May 2024 the specialized unit has continued as the Department for Strategic Communication, without the competence to deal with hybrid threats. The Ministry of Defense also participates in international exercises through the Armed Forces of the Slovak Republic and cooperates with NATO and the EU to strengthen capabilities to withstand hybrid attacks.

13 "Material detail | Portal OV." 2018. Rokovania.gov.sk. 2018. <https://rokovania.gov.sk/RVL/Material/23100/1>.

14 "Material detail | Portal OV." 2024. Rokovania.gov.sk. 2024. <https://rokovania.gov.sk/RVL/Material/29267/1>.

15 "Resolution detail | Portal OV." Rokovania.gov.sk. 2024. <https://rokovania.gov.sk/RVL/Resolution/21521/1>.

16 Minv.sk. 2024. <https://www.minv.sk/?institut-spravnych-bezpecnostnych-analyz-isba&subor=497835>.

Department of Cyber and Hybrid Threats of the Ministry of Foreign and European Affairs of the Slovak Republic: the Department is responsible for cyber diplomacy and policies related to resilience building at the EU and partly NATO level. It cooperates intensively with international partners in the EU to ensure a coherent and effective approach to addressing the challenges related to hybrid threats. Strategic communication within the Ministry is the responsibility of the Communication Branch staff.

The National Security Agency's Hybrid Threat and Disinformation Unit: the Office plays a key role in cybersecurity and critical infrastructure protection. It provides coordination between various government and private entities and support in dealing with cyber incidents. The NSA established the office in 2020 with the intention of systematically detect, evaluate, analyze and respond to information operations aimed at disseminating potentially harmful information.¹⁷

Department of Strategic Priorities of the Ministry of Education, Research, Development and Youth of the Slovak Republic: monitors threats in the education, research and development sector and makes recommendations for increasing resilience to these threats. The Ministry has also established a Strategic Communication Unit, which ensures the Ministry's communication on the topic of increasing the resilience of pupils, students and staff in the education, research and development sector to hybrid threats. It provides the Ministry's strategic communication on hybrid threats in the education, research and development sector.¹⁸

Czech Republic

"The institutions have no clear anchor, the new government can dissolve them at any time."

Quote from the research interview

The fundamental problem of the institutional framework of defense against hybrid threats, disinformation or strategic communication in the Czech Republic is the unclear responsibility and coordination authority. The germs of the institutional framework exist in the form of sub-departments and departments, but there is no clear hierarchy and no institution with coordinating authority. This is crucial in the field of hybrid threats and strategic communication.

Formally, this responsibility should have been assigned to several actors in the past - hybrid threats, for example, to the Ministry of Defense, the coordinator of the counter-hybrid agenda of the National Security Council, or the National Security Adviser. Disinformation was then to fall under the Strategic Communications Division of the Office of the Government, for example, or under the position of the Media and Disinformation Commissioner. The fact remains, however, that none of these institutions or functions has taken on this responsibility in a holistic manner. Also, attitudes towards whether disinformation or hybrid threats fall within their remit have changed repeatedly.

17 Nbu.gov.sk. 2024. <https://www.nbu.gov.sk/nbu-zriadil-pracovisko-pre-hybridne-hrozby-a-dezinformacie/>.

18 "Statute and Organizational Regulations of the Ministry of Education, Research, Development and Youth of the Slovak Republic." 2024. Minedu.sk. February 21, 2024. <https://www.minedu.sk/statut-a-organizacny-poriadok-msvvam-sr/>.

This is confusing not only externally to citizens, which can lead to increased distrust in these institutions, but also internally. Civil servants themselves do not have a clear framework within which to operate, and this often leads to parallel coordination activities, for example, or strictly departmental activities. This is further burdened by the lack of a mandate for any institution to intervene in these activities.

The new position is the creation of a new government coordinator for strategic communication, who should be in charge of the state's communication, defense against disinformation and foreign influence. This function can be expected to contribute to greater inter-ministerial coordination. However, the concrete outcomes are not yet known.

Even existing departments and unions are usually not clearly anchored and a change in political leadership could lead to a rapid dissolution or change in the very purpose of these institutions, as in Slovakia.

The different departments and institutions show the ability to coordinate with each other at least informally, "voluntary" level, especially in crisis situations. However, this is again based on internal relationships and the experience of the individuals working on the agenda, rather than a systematic and sustainable long-term strategy.

The following institutions and services are currently active in the Czech Republic in the field of hybrid threats, disinformation and strategic communication:

National Security Council (NSC): the Expert Working Group on Countering Hybrid Activities was established within the structures of the National Security Council. Its purpose is to exchange information between departments and coordinate the response to hybrid action. In addition to the coordinator of the counter-hybrid agenda and the Director of the BRS Secretariat, its members include representatives of members of the Government, the Czech National Bank, the State Office for Nuclear Safety, the National Security Office, the National Office for Cyber and Information Security, representatives of intelligence services, the Czech Army, the Czech Police and other institutions. In practice, this Expert Working Group is not fulfilling its purpose, partly because of the very low frequency of meetings, but also, according to respondents, because it has no real ambition to coordinate activities significantly.

Strategic Communication Department at the Office of the Government: this department (not a department) is responsible for analyzing the information environment, preparing communication recommendations for members of the Government and individual ministries, monitoring threats, coordinating strategic communication and a range of other activities that should be carried out with a relatively small number of staff. In practice, the department acts as a "support center" for ministries interested in interacting with it. It offers links to relevant actors, analytical support and support in specific communication practices. In practice, however, cooperation and collaboration is more informal and based on experience and trust between individual staff members, rather than based on formal principles. With the appointment of a government strategic communication coordinator, this department should become a larger department, with around a dozen people dedicated to government communication and disinformation issues.

The National Cyber and Information Security Agency (NÚKIB): is the key institution that ensures the cyber security of the Czech Republic and is therefore responsible for the key area of defense against hybrid threats. Among other things, it is responsible for the protection of classified information for information and communication systems, prepares laws in the field of cyber security, and is also involved in awareness-raising and education. It also plays an important role in the field of strategic communication.

The Defense Policy and Strategy Section of the Ministry of Defense: this section also includes the Hybrid Threat Response Division within the Crisis Management Department. Among other things, this section is responsible for the preparation of major strategic documents (such as the aforementioned Defense Strategy).

Army Cyber and Information Forces Command (VeKySIO): the Command is responsible for operations in cyberspace, including information and psychological operations, and is also involved in civil-military cooperation. It also includes specialists from the 103rd CIMIC/PSYOPS Center, i.e., experts in civil-military cooperation and psychological operations. According to a number of respondents, the Army of the Czech Republic is the only Czech institution that has sufficient skills, capacity and knowledge for effective strategic communication. However, its task is not to work inside Czech society.

Centre against Hybrid Threats of the Ministry of the Interior (CHH): it is the first specialized institution focused on hybrid threats in the Czech state administration. It was established in 2017 on the basis of recommendations from the National Security Audit. It functions as an expert analytical and conceptual workplace focused on foreign power influence or disinformation with an impact on internal security. It is also dedicated to increasing the resilience of the public administration and other entities against foreign power influence through training and education.

Ministry of the Interior Crisis Information Team (KRIT): this team within the Ministry of the Interior does not have direct formal responsibility for strategic communication as such, but its activities are an important part of this agenda. It prepares communication recommendations for ministries on topics related to internal security, but also designs and implements its own information campaigns to address specific crisis situations, such as those related to the Russian invasion of Ukraine or escalating conflicts in society.

Department of Communication of the Ministry of Foreign Affairs: Within this department, there is also a Strategic Communication Unit, which is responsible for the strategic communication of the Ministry of Foreign Affairs and is in charge of cooperation with other ministries and international partners in this area.


PR Emergency of the Ministry of Regional Development: this is not a specialized department, but an "activity" implemented in the Ministry of Regional Development, funded by Norway Grants. The aim of this activity is to assist municipal and city officials, municipal and city council employees and other local actors in communication, especially in crisis situations, upon request. They offer not only the preparation of communication strategies, but also assistance with the preparation of specific deliverables or training.

Intelligence services: the Security Information Service, the Office for Foreign Relations and Information and the Military Intelligence play an important role in the defense against hybrid threats and present the results of these activities in their Annual Reports. However, for obvious reasons, the specific department/unit dealing with these topics is unknown.

Parliament's Standing Commission on Hybrid Threats: established in 2020, its task is to monitor election protection and map the situation in the field of defense against hybrid threats. It can make recommendations or call on the government to address specific facts relating to hybrid threats.

Analysis of capacity, funding, processes and policy prioritization



Staff and technical capacity

Country:	 Slovakia	 Czech Republic
Spot Assessment:	4,05	3,35
Summary:	<p>Staff and technical capacities are rated as below average. There is still a shortage of qualified staff and technical resources and equipment in this area. Some institutions have only a few well-trained staff, and there is a lack of co-management experts, analysts and conceptual staff. Technical equipment, especially in the area of analytical tools and software, is inadequate or missing altogether.</p>	<p>Staffing and technical capacity are rated as average. There is a lack of technical equipment in state institutions, especially software for open source and social network analysis, but also a lack of staff who can work effectively with these tools. There is also a lack of communication experts who can plan and creatively design campaigns. Similarly, there is a lack of experts in hybrid threats, cyber-security or information literacy. Knowledge of advanced technologies or artificial intelligence is completely non-existent. Moreover, ministries and individual institutions do not have channels for the continuous sharing of information and know-how. There is a lack of specific knowledge and experts, who are few and almost exclusively in security institutions and departments.</p>

Funding

Country:	 Slovakia	 Czech Republic
Spot Assessment:	3,86	3,06
Summary:	<p>Funding is rated as below average. The financial resources allocated to this area are insufficient, there is a lack of transparency and strategic planning, which leads to inefficient use of the available funds. Funding is often dependent on European funds, which limits flexibility and long-term sustainability. Moreover, the resource structure is based on staff costs, with a lack of resources for training, technical equipment and public campaigns. Continuity of funding for capacities and budgets for hybrid threat and strategic communication activities has not been ensured across commitments from the previous period. As of 2024, any funding for activities implemented by NGOs in this area is suspended.</p>	<p>Financing is assessed as pass-through. The institutions and the costs of their operations and activities are generally assessed as under-budgeted, both in terms of staff costs and technical support. Inefficient use of the resources allocated to this area was repeatedly raised as a major problem. Tens of millions a year have been allocated to strategic communication campaigns, but it is not clear whether these activities have had an effect. In the absence of a clear strategic plan with specific objectives identified, it is also unclear what results these campaigns were intended to achieve.</p>



Efficiency of procedures

Country:	 Slovakia	 Czech Republic
Spot Assessment:	4,36	3,40
Summary:	The effectiveness of the procedures is rated as below average . Some institutions carry out analyses and make recommendations, but these are rarely put into practice. Inter-ministerial coordination is weak and procedures are often ineffective.	The effectiveness of the procedures is rated as average . Inter-ministerial coordination is insufficient and no information transfer system has been institutionalized. There is still a lack of understanding of strategic communication within individual ministries, which should not consist of one-off campaigns but should be based on the continuous building of different channels to reach citizens, which should complement each other. It is not inherent to the non-power ministries to work with monitoring and to approach disinformation campaigns preventively. All cooperation is based more on informal relations between individual staff members and their personal commitment, rather than on formal, agreed-upon procedures.

Political priority

Country:	 Slovakia	 Czech Republic
Spot Assessment:	4,40	2,65
Summary:	The political priority is rated as below average . The perception of the importance of mobile threats and strategic communication among government politicians is very low. These topics have become the subject of political struggle, which fundamentally weakens the will to implement any action in the area. Politicians often ignore these issues or consider them less important. After the new government took office, only a few departments, such as the Ministry of Education and the Ministry of Defense, have shown a certain degree of awareness and initiative. Politicians often underestimate these threats and do not actively engage in addressing them.	The political priority is rated as pass-measurable . In general, awareness among government policymakers regarding hybrid threats and strategic communication was rated as more rhetorical but not translating into practical action. Misunderstanding of strategic communication as a concept was identified as a major problem, with politicians often not understanding what to expect from a strategic communication system and how strategic communication differs from political communication.

Summary

 Slovakia	 Czech Republic
Lack of coordination and clear division of responsibilities:	
<p>Both countries face challenges in terms of coordination and clear lines of authority in dealing with hybrid threats and implementing strategic communications. In the Czech Republic, this lack of coordination is due to an unclear hierarchy and, to date, the absence of a centralized institution with clear coordinating authority. In Slovakia, there are specialized units, but their effectiveness is weakened by political changes and organizational problems.</p>	
Political instability:	
<p>Both countries are experiencing the impact of political change on the effectiveness of institutions. In the Czech Republic, institutions can easily be dissolved or their focus changed with the arrival of a new government, similar to Slovakia, where the 2023 elections have seen the departure of professional staff and the degradation of the solutions to this issue.</p>	
Existence of specialized departments:	
<p>In both countries, there are specialized units focused on hybrid threats and strategic communications. In the Czech Republic, for example, the Centre against Hybrid Threats of the Ministry of the Interior, in Slovakia the National Security and Analytical Centre of the Slovak Information Service.</p>	
Formal anchoring and centralization:	
<p>In Slovakia, there was an attempt to create specialized EU-funded services in 2022, although the effectiveness of these services is now threatened by political changes.</p>	<p>In the Czech Republic, the problem lies in the unclear anchoring of individual departments and the lack of centralized coordination.</p>
Staff and technical capacity:	
<p>Both countries suffer from a lack of technical equipment and qualified experts in the field of hybrid threats and strategic communication. There is a lack of both technical tools for open-source analysis and experts in communication and cyber security.</p>	
Financing and efficiency of procedures:	
<p>In both countries, funding for activities in the area of hybrid threats and strategic communications is assessed as insufficient. Both the Czech Republic and Slovakia face problems with inefficient use of available resources and inefficient funding, which in the case of Slovakia is dependent on European funds and in the Czech Republic is generally rated as undersized. The efficiency of procedures is also low in both countries, with a lack of inter-ministerial coordination and informal working relationships rather than formal procedures.</p>	
Political priority:	
<p>Both countries show low political priority on hybrid threats and strategic communications. In the Czech Republic, awareness among government officials is rather rhetorical, while in Slovakia these topics are often completely ignored and become the subject of political disputes in both countries.</p>	

CASE STUDIES

This chapter presents a detailed analysis of selected case studies that illustrate specific examples of hybrid threats, disinformation campaigns and strategic communications in the Czech Republic and Slovakia. The case studies have been carefully selected to cover different types of threats and responses. They provide deeper insight into the practical functioning of defense mechanisms in real situations.

The case studies were selected in the following categories:

- **Hybrid:** A state's response to country-centric operations that include multiple aspects that fall under hybrid operations (e.g., economic influence, espionage, strategic corruption, etc.).
- **Information operations:** State response to specific information and disinformation campaigns with a wide impact.
- **Strategic communication:** Implemented state communication campaigns aimed at combating disinformation and foreign influence and systemic state measures in the field of strategic communication.

For the case studies, **social media data analysis** using the Juno tool from Gerulata Technologies was used. This tool enables the analysis of trends and information dissemination on social media, the identification of key actors and the connections between them. By using this tool, we were able to quantify the impact of certain actions in the information space and better understand how this information is disseminated and influences the events in society, who the main disseminators are and how they influence the events in society.

The aim of this chapter is to provide practical examples that show how hybrid threats manifest themselves in the real world and what strategies and tools are effective in countering them. These case studies serve as models for further improvement and adaptation of defense mechanisms in both countries.

HYBRID ACTION

CASE STUDY 1: Successfully uncovering Russian intelligence activities in Slovakia



Description: Bohuš Garbár at a meeting with the RF military attaché Solomasov, where he accepted cash in exchange for obtaining sensitive and classified information, source: Denník N

Summary:

In the summer of 2021, **Military Intelligence revealed the activities of individuals working for Russian intelligence services in Slovakia.** Among them were a contributor to the quasi-media portal Hlavné správy (Main News) and the rector of the Armed Forces Academy of general Milan Rastislav Štefánik. Among the suspects was also a former assistant to the MP for the ĽSNS party (People's Party Our Slovakia). As a result of the operation, the activities of the Russian intelligence services were uncovered, two persons were charged, and one person was convicted. An example of good practice was the implementation of the whole operation, the cooperation between the intelligence services and the police, and the media coverage of the whole case, which was the first time that hybrid activities in Slovakia were publicly exposed.

The course of the case:

This case was publicized in March 2022, a month after the start of Russia's full-scale invasion of Ukraine, during a period of heightened state attention to hybrid threats and disinformation campaigns. The heightened attention of the security and intelligence services also resulted in a counter-intelligence action by the Military Intelligence Service, which had already uncovered the activities of Russian GRU military intelligence on the territory of Slovakia in 2021. The National Criminal Agency of the Presidium of the Police Force (NAKA) subsequently charged and detained several persons suspected of cooperation with Russian intelligence services and of leaking classified information.

The first accused was Bohuš Garbár, an external contributor to the pro-Kremlin quasi-media portal Hlavné správy. According to the police, the accused had been collecting information for members of the Russian military intelligence agency GRU since April 2021.¹⁹ According to the court, Garbár met with a diplomat of the Russian Federation, for whom he sought and obtained sensitive and classified information for a financial reward of EUR 1,000. The Specialized Criminal Court found Garbár guilty of the crime of espionage and the crime of taking bribes in February 2023, as part of the approval of the plea agreement.

The second defendant, Pavel Bučka, the former vice-rector of the Armed Forces Academy of general Milan Rastislav Štefánik in Liptovský Mikuláš, has worked for Russian intelligence since 2013. In the period 2013-2016, Pavel Bučka had thirteen meetings with his senior officers from the Russian Embassy. He received a reward of at least EUR 46,000 for bringing out classified information.²⁰ Police are continuing to prosecute this case.²¹

19 Klaudia Jurkovičová, SITA, and TASR. 2023. "Rusom Dával Aj Prísne Tajné Informácie. Dostal Podmienku Aj Peňažný Trest." Kosice.korzar.sme.sk. SME.sk. February 28, 2023. <https://kosice.korzar.sme.sk/c/23141361/rusom-daval-aj-prisne-tajne-informacie-dostal-podmienku-aj-penazny-trest.html>.

20 Tódová, Monika. 2022. "Ako Vyzerala Špionáž Pre Rusko: Mŕtve Schránky, Tajné Stretnutia Pri Soche Hurbana a Pravidelná Odmena Dvetisíc Eur." Denník N. Denník N. March 25, 2022. <https://dennikn.sk/2783187/ako-vyzerala-spionaz-pre-rusko-mrtve-schranky-tajne-stretnutia-pri-soche-hurbana-a-pravidelna-odmena-dvetisic-eur/>.

21 TASR. 2023. "Polícia Pokračuje v Stíhaní Plukovníka Bučku, Ktorý Je Obvinený v Kauze Vyzvedačstva Pre Rusko." Hnonline.sk. Hnonline. en. July 25, 2023. <https://hnonline.sk/slovensko/96095683-policia-pokracuje-v-stihani-plukovnika-bucku-ktory-je-obvineny-v-kauze-vyzvedacstva-pre-rusko>.

Timeline:

- 2013** • Vice-Rector of the Armed Forces Academy Bučka starts collecting information for the Russian Federation.
- April 2021** • Bohuš Garbár starts collecting information for members of Russian military intelligence GRU.
- March 2022** • Police arrested and charged the suspects with collaboration with Russian intelligence services. Denník N (Daily N) subsequently publishes a video recorded by Slovak security forces during the detection of Russian espionage in Slovakia.
- February 2023** • The Specialized Criminal Court found Bohuš Garbár guilty of the crime of espionage and the crime of taking bribes.
- April 2024** • The Specialized Criminal Court ruled that Garbár should spend a pro rata portion of his sentence of one year, five months and 25 days in prison for failure to pay the fine.

Reflection of the case in the information space:

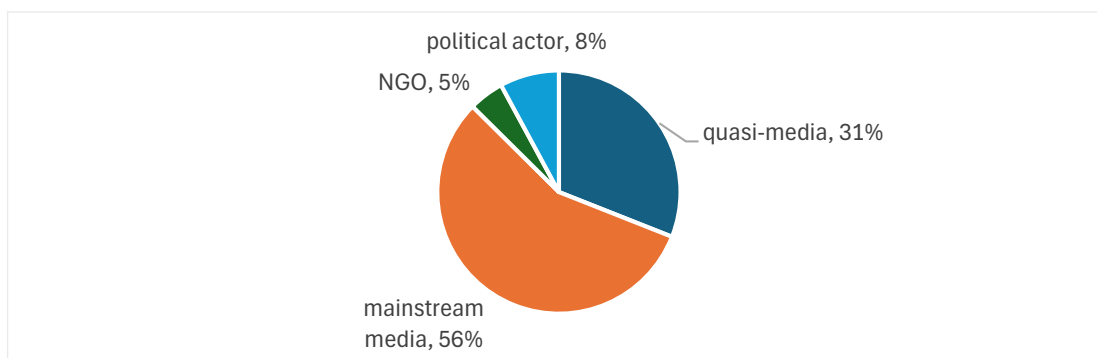
The case resonated in the information space shortly after its revelation in February and March 2022, then especially during the trial in 2023 and 2024. However, the spread of posts on the subject was not very extensive. In the entire period under review, only 342 posts were identified in the information space.



Evolution of the number of posts responding to the case of the exposure of Russian intelligence activities in Slovakia. (Data retrieved from Juno in May 2024.)

The information space was dominated by mainstream media contributions, mainly on web platforms and Facebook. Quasi-media contributions focused primarily on factual communication of the news. An exception was the reaction of the Hlavné správy portal, with which the convicted Garbár

collaborated.²² Political actors tended not to communicate the topic, their contributions did not have a significant impact. Similarly, civil society communicated the case with minimal outreach. The profiles of state institutions on social media did not devote any posts to the case.



Overview of actors who communicated about the disclosure of the Russian intelligence network in Slovakia (% of the total number of posts). (Data retrieved from Juno in May 2024.)

Rating:

This is an **important example of good practice within the Slovak Republic because it is a successful capture of espionage activities, their recording and media coverage.** At the same time, it is one of the few cases of espionage **that has been investigated, in which a trial was held, and the actors were made public and convicted.**

The media coverage of the case has increased public attention to the issue of the hybrid action of the Russian Federation against Slovakia. The public has learned how espionage activities are carried out in practice. However, in the subsequent period, the case has not been sufficiently used to educate and raise awareness of the post-war security threats, either by state institutions or civil society.

There was no abuse of the topic or questioning of the case. The disclosure of the spying activity on video footage contributed to the undeniable evidence of hybrid activity, which was therefore not questioned in the information space. The mainstream media was the dominant source of information. The case, on the other hand, did not receive a wider response in the quasi-media.

Monetary punishment for offenders may be generally considered insufficient deterrent for other potential perpetrators of similar acts, which can be exploited by hostile actors.

22 Štefan Tomášik. 2023. "Hlavné Správy." Hlavné Správy. February 28, 2023. <https://www.hlavnespravy.sk/obvineny-v-kauze-vyzvedacstva-pre-rusko-bohus-garbar-dostal-podmienku/3060594>.

CASE STUDY 2: Brat za brata



Description: Matúš Alexa, chairman of the Brat za brata group, receives the so-called "eternal light" in Moscow from Sergei Naryshkin, head of the Russian foreign intelligence service SVR. Source: FB Brat za brata

Date:

2019 to present

Summary:

The Brat za brata (Brother for brother) motorcycle group is known for its activity on social media, where it spreads pro-Putin propaganda. As a successor to the group Night Wolves it has become an important channel for pro-Kremlin narratives and is used as a tool for Russian hybrid influence in Slovakia. Under the guise of caring for the memorials of fallen Red Army soldiers, it brings Russian imperial ideology to Slovakia, promotes the strategic interests of the Russian Federation and maintains regular contacts with its representatives. So far, state forces have failed to respond effectively to their activities.

The course of the case:

The Brat za brata motorcycle group is an example of the hybrid influence of the Russian Federation on Slovakia through proxy subjects and the abuse of historical events. The group became known to the public through motorcycle rides and public events at monuments to the liberation of Czechoslovakia by the Red Army. At the same time, they have been intensively disseminating content via social networks from the Russian embassy or the Slovak version of the pro-Kremlin disinformation portal NewsFront, which has been placed on the sanctions list for its links to the FSB. Last but not least, Brat za brata representatives have been visiting the Russian embassy in Slovakia and the Russian Federation itself, even after the outbreak of Russian military aggression against Ukraine.²³

23 "The Jan Kuciak Investigative Centre." 2024. Icj.k.sk. 2024. <https://icjk.sk/243/Motorkari-Brat-za-Brata-vyuzivaju-silu-na-socialnych-sietach-na-siren timer-proputinovskej-propagandy-najviac-zdielaju-ruske-velvyslanectvo>.

Matúš Alexa is the chairman of Brat za brata. In the past, he was a member of the Slovak branch of the Night Wolves motorcycle gang, which served Russian propaganda and was known for its close relations with Russian President Vladimir Putin. After the start of the Russian aggression in Ukraine, Alexander Zaldostanov, the leader of the Night Wolves, found himself on sanctions lists, as did the leader of the Slovak branch, Jozef Hambálek. The place of the Night Wolves in Slovakia was taken by the group Brat za brata, which uses the form of the civic association Motorkári Slovenska (Bikers of Slovakia).²⁴ One of the most famous examples where Brat za brata acted in close coordination with the Russian embassy was the Lodomirová case, which is discussed in the next chapter.

The activities of Brat za brata are characterized by close relations with the representatives of the Russian Federation, which did not cease even after the Russian attack on Ukraine. Matúš Alexa received two awards from the Embassy of the Russian Federation in Slovakia for his activities in favor of Russia²⁵, met the head of the Russian intelligence service SVR in Moscow and was also in the group of Slovak observers of the Russian presidential elections in 2024.²⁶

Timeline:

2018	• Separation of the group around Matúš Alexa from the Night Wolves Europe.
2019	• Establishment of civic association Motorkári Slovenska.
2020	• Organizing the Freedom Ride to Russia.
2021	• Acceptance of the Brotherhood by Sergei Naryshkin and the award of the State Medal.
2022	• Increase in Brat za brata activity and popularity on social media.
2024	• Participation of Matúš Alexa in the observation of the presidential elections in the Russian Federation.

Reflection of the case in the information space:

Over time, Brat za brata has become one of the most important and influential sources of Russian propaganda in Slovakia. It uses a sophisticated tactic of tailoring content to the platform. For example, Facebook is dominated by motivational quotes and videos depicting respect for the Red Army, Russian culture and the liberation of Slovakia, while the Telegram account is dominated by overt Russian propaganda.

For the period from January 2021 to the end of May 2024, their content had more than 40 million views on the four platforms in total, half of which were on Facebook and half on Telegram.²⁷ The total number of posts on all four platforms was more than 24,000 for the period under review, of which more than 4/5 were on the Telegram channel Pravda víťazí (The truth wins). This is indicative of the amount of capacity devoted to content production by this group on various platforms and

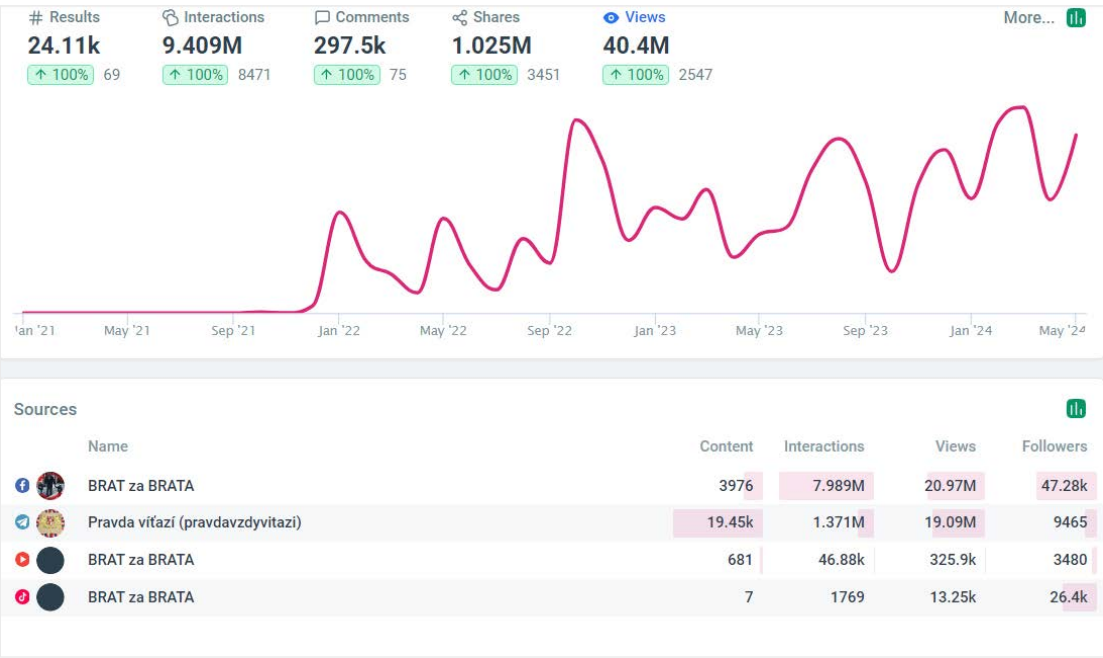
24 Ibid.

25 Ibid.

26 Shekhovtsov, Anton, and Olena Sandul. 2024. Epde.org. Berlin: Edition: European Platform for Democratic Elections. https://epde.org/wp-content/uploads/2024/05/EPDE_Report_FakeObservers_2024.pdf.

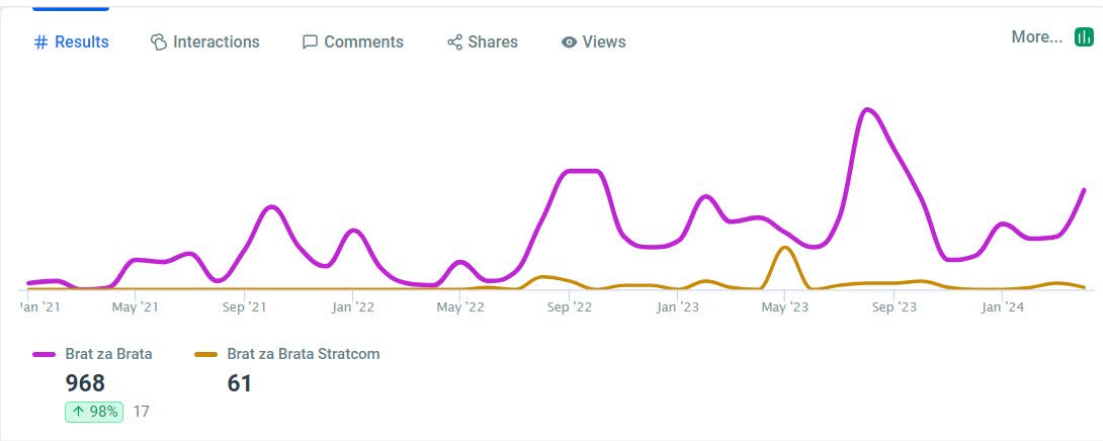
27 The number of views on the Facebook platform includes only videos, on the Telegram platform also views of text posts or images.

its close links with other pro-Russian media projects such as TV OTV or Slovanské noviny, (Slavic news) to which it also frequently links.



Evolution of the views of Brat za brata content across different platforms (Data retrieved from Juno in May 2024.)

Even when comparing the number of posts devoted to the Brat za brata group in other online sources, quasi-media projects clearly dominate in a ratio of 968:61 in favor of quasi-media and other disinformation sources.



Evolution of the number of posts mentioning Brat za brata – a comparison of Quasi-Media and Disinformation actors (pink) versus the state StratCom (yellow). (Data retrieved from Juno in May 2024.)

Given the exceptionally high volume of the Brat za brata group on social media and the steady increase in their online activities, especially after Russia invaded Ukraine, it is very likely that the increase may be due to foreign support. Indicators could be the group's close ties to the Russian

embassy in Bratislava, the mutual sharing of content between the two entities, or the frequent links to well-known sources of Russian propaganda, such as the newsfront.info website.

Rating:

Brat za brata is one of the most influential pro-Russian groups in the online environment in Slovakia. Their accounts serve as a conduit to bring pro-Putin propaganda and Russian strategic narratives into the Slovak information space. Their public activities at World War II memorials bring to Slovakia a Russian vision of the world and a Russian view of the past and present. An important element of their activities is the promotion of the idea of the so-called All-Slavic Reciprocity, which is part of the Russian strategic narratives used in Slovakia. Through trips to the Russian Federation and meetings with officials of the Russian administration, they legitimize and challenge Slovakia's official position on the war in Ukraine.

Despite the reach and influence of the group's activities and its undisguised links to a hostile foreign power, Slovak state institutions have been unable to come up with an effective response to prevent Russian momentum through the group's activities.

Given the number of activities and their financial intensity, it is likely that the group's activities are partly financed by the Russian Federation. However, there is no direct evidence of such a link in open sources.

CASE STUDY 3: A Czech Foreign Ministry Employee Leaked Information to the Russian Secret Service



Source: Seznam Zprávy

Date:

2022



CENTER FOR
AN INFORMED
SOCIETY

Summary:

In September 2022, it was revealed that a former employee of the Ministry of Foreign Affairs of the Czech Republic, later identified as J.A., allegedly passed information to the Russian Federation. The case, which was investigated by the Security Information Service (BIS), and in particular the details that were subsequently revealed by investigative journalists, highlighted possible significant shortcomings in the ability of Czech state institutions to address this type of problem.

Progress of the case:

A former radio operator at the Czech Foreign Ministry who served on diplomatic missions in Africa in the 1990s, and his wife allegedly befriended a man later identified as an agent of the Russian Foreign Intelligence Service (SVR) on a mission to Libya. The person was said to have had a security clearance at the time at the level of "Top Secret." The Czech Security Information Service (BIS) discovered that **this person had been knowingly providing sensitive information to the Russians for several years for financial gain**. However, it is not entirely clear when the BIS became aware of this conduct. The BIS passed this information to the Prime Minister and the Minister of Foreign Affairs in 2021. This information was revealed in the Czech media in September 2022.²⁸

Later, investigative journalists from the server Seznam Zprávy (Seznam News) revealed further details about the person in question, whose initials should be J.A. They also said that the **information leaked was supposed to be primarily about internal diplomatic events and people-to-people relations, not about top secret reports** or documents.

According to Seznam Zprávy, **J.A. continued to work at the ministry after the information was handed over to the BIS** until 15 July 2022.²⁹ At that time, the Security Information Service decided to intervene because it feared the resumption of his contacts after the end of the Covid-19 pandemic. Foreign Minister Jan Lipavský then confirmed to Deník N that he had taken steps "thanks to which the ministry no longer has an employee who cooperated with a foreign power." According to Seznam Zprávy, however, his employment was not terminated by the Ministry of Foreign Affairs, but **J.A. retired into standard retirement**. At the same time, this former employee **did not face any police investigation or prosecution**. According to Deník N, an unnamed source from the judiciary explained this fact by saying that it was intelligence information which, according to Czech law, cannot be used in court.

28 "Pracovník ministerstva zahraničí vynášel tajné informace ruské rozvědky. " Využili jeho slabost pro ženy a peníze " 2022. Deník N. <https://denikn.cz/962394/pracovnik-ceskeho-ministerstva-zahranici-vynasel-tajne-informace-ruske-rozvedce/?ref=tit1>.

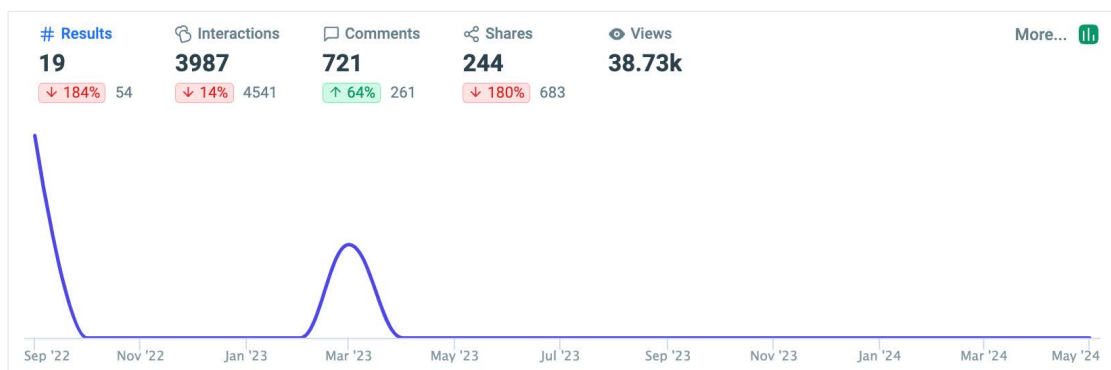
29 "Čech podle kontrarozvědky donášel Rusům. Spojku mu dělala zubařka." 2023. Seznam Zprávy. <https://www.seznamzpravy.cz/clanek/domaci-kauzy-nasli-jsme-cecha-ktery-podle-bis-donasel-rusum-227046>.

Timeline:

- 1990s** • J.A. works as a radio operator at the Ministry of Foreign Affairs of the Czech Republic and is based in Libya. During this time, he and his wife become friends with a Russian couple identified as SVR agents.
- 1990–2020** • J.A. allegedly provided sensitive information to Russian intelligence services for several years.
- 2022** • BIS informs the Prime Minister and the Foreign Minister about the spying activities of J.A.
- 2022** • J.A. retires from the Ministry of Foreign Affairs.
- March 2023** • Seznam Zprávy publishes an investigative article exposing J.A.'s alleged espionage activities and their details.

Reflection of the case in the information space:

The case was not heavily covered by the media; the main inputs in the information space were primarily the mainstream media and journalists who worked on its investigation. As state institutions also commented on the case rather minimally, there was no response from the disinformation scene. With the exception of a narrower community with an interest in security, the case did not ultimately attract much interest from the wider public. It should be added that the data in the graph only monitors social networks. Thus, they do not reflect the readership of, for example, investigative articles on Seznam Zprávy or Deník N, but only data on how people interacted with posts published on this topic.



Evolution of the number of posts responding to the case of the Czech Foreign Ministry employee.



Name	Content	Interactions	Reactions	Comments	Shares	Views	Followers	Avg int. rate
Deník N	5	200	149	34	17	0	53.92k	0.07%
Filip Rožánek	2	57	0	0	57	0	50.99k	0.06%
Visegradský jezdec	2	831	713	81	37	0	84.58k	0.49%
ČT24	2	1483	1114	328	41	8019	927.3k	0.08%
Seznam Zprávy	2	131	114	5	12	20.94k	240.1k	0.03%
Jiří Kubík / Ve stínu	1	65	57	3	5	9768	57.32k	0.11%
Lukáš Prchal	1	441	349	34	58	0	10.9k	4.05%
Orla.sk	1	0	0	0	0	0	477	0%
Deník e15	1	220	166	47	7	0	53.7k	0.41%
Seznam Zprávy	1	206	161	41	4	0	162.4k	0.13%
iDNES.cz	1	353	199	148	6	0	280.6k	0.13%
Summary	19	3987	3022	721	244	38.73k	1.922M	

Impact of individual accounts that responded to the case of a Czech Foreign Ministry employee.

Rating:

The BIS investigation concluded that J.A. had indeed supplied information to Russia, but that it was not highly classified material. Rather, the information passed on concerned internal diplomatic matters and personal issues, which may also be valuable to foreign intelligence services.

The revelation of the case in the media, particularly through investigative reports by Seznam Zprávy, has drawn public attention to weaknesses within Czech state institutions and raised questions about the effectiveness of internal security protocols and the response of state authorities to such serious conduct.

One of the most frequently mentioned obstacles to dealing with cases of this type in a more decisive manner is the fact that **the Police of the Czech Republic cannot use intelligence information from the BIS as formal evidence in court.** However, some respondents pointed to the fact that this is a controversial interpretation of Czech law, which does not explicitly prevent the use of intelligence evidence in criminal proceedings if it is accepted by a competent court. Rather, it is the lack of attempts at such use, which also implies a lack of case law, as well as an established culture of intelligence services that are not set up for such cooperation with law enforcement.

The second obstacle is a similarly **unclear interpretation of Section 316 of the Criminal Code, which speaks** of the act of spying on "classified information," not sensitive information that is not "secret" or "top secret." The second paragraph of the same section, however, states that a person who facilitates an activity by the perpetrator or an organization to challenge classified information will be equally punished. This paragraph could also be interpreted in a way that would make the actions of former radio operator J.A.

CASE STUDY 4: Sanctions Legislation in the Czech Republic



Russian arms dealer Boris Obnosov, who was placed on the Czech sanctions list, visiting Russian President Vladimir Putin. Source: iRozhlas

Date:

2022 – present

Summary:

The Sanctions Legislation, effective January 2023, created a national sanctions list to target individuals and legal entities involved in actions violating or threatening the territorial integrity, sovereignty and independence of Ukraine or actions destabilizing the situation in Ukraine. Despite being a legislative success, challenges emerged and while harmonized with EU policies, rapid political demands strained implementation. Public and media engagement were prominent when new entities were listed, highlighting the law's impact but also its operational shortcomings.

Progress of the case:

The current Foreign Minister Jan Lipavský has been advocating for the adoption of national sanctions legislation, the Czech version of the so-called "Magnitsky Act", since 2018 (he was an MP at the time). After joining the government, he announced the goal of passing this law by the end of 2023.³⁰ This process was fundamentally accelerated by the aggression of the Russian Federation against Ukraine. Law 1/2023 on restrictive measures against certain serious acts applied in international relations (the so-called Sanctions Law) then came into force in January 2023.

This law allowed the creation of a national sanctions list on which individuals and legal entities that have committed acts defined in the EU sanctions regimes can be placed, e.g. violating or threatening the territorial integrity, sovereignty and independence of Ukraine or actions destabilizing the situation in Ukraine.

If such an entity is identified, the Ministry of Foreign Affairs, after approval by the Government of the Czech Republic, first seeks its placement on the EU sanctions list. However, if it is not placed

30 "Lipavský předloží vládě takzvaný Magnitského zákon. Umožní zmrazit další majetky." 2022. CT 24. <https://ct24.ceskatelivize.cz/clanek/domaci/lipavsky-predlozi-vlade-takzvany-magnitskeho-zakon-umozni-zmrazit-dalsi-majetky-20606>.

on the list within one month of the submission of the proposal, it may place it on the national list. If the purpose for which the entity is to be placed on the sanctions list is in danger of being defeated, it may be placed on the national sanctions list immediately after the Government's decision. If the entity is later placed on the Union sanctions list, it shall be removed from the national sanctions list. Specific sanctions are then applied to the listed entities on the basis of Act No. 69/2006 Coll. on the implementation of international sanctions.

Within the Ministry of Foreign Affairs, the Sanctions Policy Division is in charge of sanctions policy, which is mainly responsible for coordination and analytical work on the management of the sanctions regime. It currently comprises seven entities, two legal entities and five natural persons. Three individuals, namely the Russian businessman and arms dealer Boris Obnosov, as well as Viktor Medvedchuk and Artyom Marchevsky, who were behind the activities of Voice of Europe, have been removed from the list because they were included in the European Union's sanctions packages.³¹

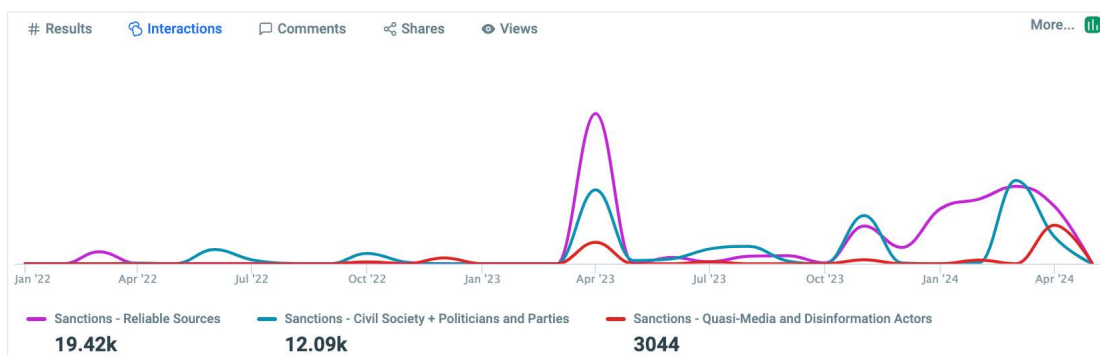
Timeline:

- 2018** • Jan Lipavský starts to push for the adoption of a national sanctions law from his position as an MP
- 2022** • Jan Lipavský, already as Foreign Minister, promises to approve the law by the end of 2023
- January 2023** • Sanctions Act comes into force
- April 2023** • The first entity is placed on the sanctions list

Reflection of the case in the information space:

As the chart below shows, the mainstream media and Minister Jan Lipavský's social media accounts most frequently reported on the sanctions legislation and its implementation. Along with other politicians and civil society, in this case, trusted channels had significantly higher circulation than the disinformation scene. The largest numbers of interactions correspond to the stages when new names were added to the sanctions list - in April 2023 it was the first subject, Patriarch Kirill of Moscow, and in April 2024 it was the legal entity Voice of Europe and individuals associated with it (this case is described in the next chapter).

31 "National Sanctions List." 2023. Ministry of Foreign Affairs of the Czech Republic.
https://mzv.gov.cz/jnp/cz/zahranicni_vztahy/sankcni_politika/sankcni_seznam_cr/vnitrostatni_sankcni_seznam.html.

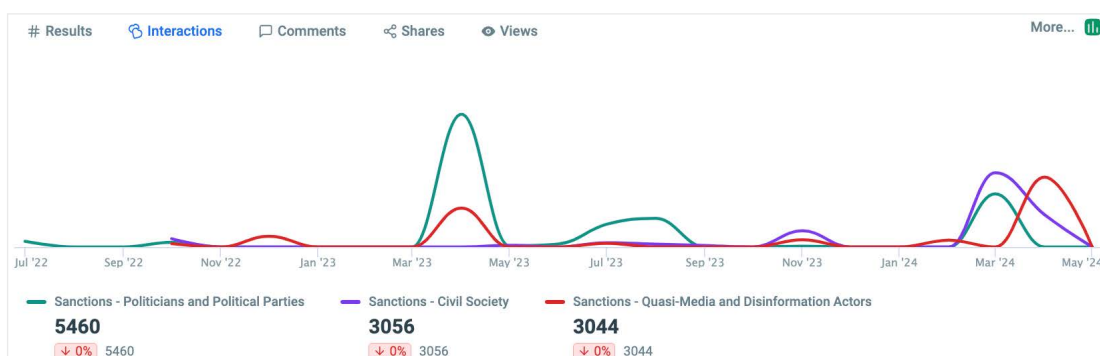


Comparison of the interactions of posts reporting on sanctions legislation for the monitored groups.

Sources		Interactions	
Sanctions - Reliable Sources		Sanctions - Civil Society + Politicians and Parties	
Name	Interactions	Name	Interactions
ČT24	4252	Česká pirátská strana	1531
ČT24	3650	Jiří Hřebenar	1508
Jan Lipavský - ministr...	2760	Ondřej Kolář	1204
Jan Lipavský	2008	Poslední skaut™	623
Události Ludka Staňka	1745	Vladimír Votápek	597
Jan Lipavský	899	Tomáš Czernin	593
Sanctions - Quasi-Media and Disinformation Actors		Name	Interactions
		Roman Kirsch	1392
		neČT24	638
		Selský Rozum	435
		CZ24.NEWS	415
		Zakázané informace	119
		Slovanské nebe	45

Comparison of the accounts of the main actors informing about the sanctions legislation on social networks according to their impact within the monitored groups.

Only the quasi-media projects on YouTube and Telegram, among them neČT24, which, according to the Czech Interior Ministry's Center Against Hybrid Threats, is the successor to the now-blocked Russian government channel Sputnik, have reached the level of the mainstream media, politicians and civil society.³²



A more detailed comparison of the interactions of posts within selected groups reporting on sanctions legislation.

32 "Summary of findings on the Czech presidential election 2023." 2023. Ministry of the Interior of the Czech Republic. <https://www.mvcr.cz/chh/clanek/souhrn-poznatku-k-ceskym-prezidentskym-volbam-2023.aspx>.

Sources			Interactions 		
Sanctions - Politicians and Political Parties			Sanctions - Civil Society		
Name		Interactions	Name		Interactions
 Česká pirátská strana		1531	 Jiří Hřebenar		1508
 Ondřej Kolář		1204	 Poslední skaut™		623
 ODS - Občanská...		539	 Rekonstrukce státu		450
 MUDr. Jiří Mašek		490	 Rekonstrukce státu		302
 Marek Ženíšek		296	 Manipulátoři.cz		173
 Piráti		266			
Sanctions - Quasi-Media and Disinformation Actors			Name		Interactions
			 Roman Kirsch		1392
			 neCT24		638
			 Selský Rozum		435
			 CZ24.NEWS		415
			 Zakázané informace		119
			 Slovanské nebe		45

A more detailed comparison of individual accounts of the main actors informing about sanctions legislation, based on their interactions within the monitored groups.

Rating:

The Czech National Sanctions List is a key legislative instrument, the introduction and subsequent implementation of which has provoked both positive and negative responses. The strength of this law is its quick and effective enforcement, which has minimized the backlash from disinformation channels and given the Czech Republic a leading position within the EU in the application of sanctions. Another important advantage is its harmonization with European sanctions regimes, which increases its international legitimacy and contributes to the overall coordination of European policy.

However, the weaknesses of the Sanctions Act are significant, although not visible at first glance in the media space. One of the key challenges is the lack of preparedness of Czech institutions to implement the law, as well as the absence of mechanisms for processing objections. Political pressure to quickly add new entities to the list has long been at odds with shortcomings in institutional capacity and in handling the process of appealing entities placed on the list. Litigation against sanctioned persons is protracted over a long period of time, allowing appealing sanctioned persons to remain in the Czech Republic. Another challenge is the lack of staff capacity in the Ministry of Foreign Affairs, which significantly reduces the effectiveness of the implementation of the law and further slows down its use.

Despite these challenges, the Czech sanctions regime is considered to be one of the best among EU member states, which indicates its potential if the necessary adjustments to the related processes and mechanisms are made.

Summary:

The uncovering of Russian intelligence activities in Slovakia demonstrates the effective cooperation between military intelligence services and law enforcement in detecting and apprehending persons cooperating with Russian intelligence services. Key elements include a successful counter-intelligence operation, media coverage of the case, and subsequent public awareness of hybrid threats. However, the long-term use of the case to educate and build awareness has been limited, indicating the need for sustained strategic communication.

A case study on the activities of the Brat za brata biker group in Slovakia demonstrates that despite clear links to a hostile power, Slovak state institutions have failed to respond effectively to their activities. This highlights the need for improved strategic communication and legislative changes that would transparently address the activities of such groups.

The case of a Czech Foreign Ministry employee who passed sensitive information to Russian intelligence highlighted the shortcomings in the ability of Czech state institutions to respond effectively to espionage activities. The key problems were the lack of clarity in the legislation, which prevented the use of intelligence information in criminal proceedings, and the absence of sufficient case law. This points to the need for legislative amendments and better coordination between intelligence services and the police.

The latest study focuses on the adoption and implementation of national sanctions legislation in the Czech Republic. The law enabled the creation of a national sanctions list, which has placed the Czech Republic as a leader in sanctions policy within the EU. The key challenge is the lack of institutional preparedness for the implementation of the law, the political pressure to quickly add entities to the list and the lack of staff capacity. These factors point to the need for better preparation of the legal framework and organizational structure for effective implementation of sanctions legislation.

Effectiveness of operations and media coverage: the Slovak case of the exposure of Russian intelligence activities shows the importance of effective cooperation between intelligence services, law enforcement, and subsequent media coverage. Both were lacking in the case of the Czech Foreign Ministry employee.

Legislative arrangements and shortcomings: the case of the Czech Foreign Ministry employee and the sanctions legislation show the need for clear legal frameworks and specifications in the Criminal Code to enable effective prosecution of espionage and hybrid threats.

Strategic communication and public awareness: all studies point to the importance of strategic communication and public awareness. The Slovak Brat za brata case and the revelations of Russian intelligence activities highlight the need not only for one-off campaigns, but for long-term strategic communication and awareness-building on hybrid threats.

Institutional capacity and coordination: the cases show the importance of institutional capacity and coordination between different parts of government. An effective response to hybrid threats requires not only a legislative framework but also sufficient staffing and funding.

DISINFORMATION

CASE STUDY 1: Successful government response to an information operation related to the redevelopment of a cemetery in Lodomirová



Ambassador of the Russian Federation to Slovakia points to allegedly almost destroyed graves

Date:

September 2022

Summary:

In September 2022, the Embassy of the Russian Federation in Slovakia published misleading information on social media about the alleged destruction of a World War I-era cemetery in the village of Lodomirová, where Russian soldiers were supposed to be buried. This message was immediately intercepted by the Slovak administration and identified as an information operation to cover up the leaked reports of further military crimes by the armed forces of the Russian Federation in Ukraine, this time in the town of Izjum. The relevant branches of the SR administration explained in detail to the public the activities of the Embassy of the Russian Federation and, by further actions, significantly minimized the achievement of the objectives of the information operation.

Progress of the case:

The identified information operation concerning the Ladomirová cemetery took place six months after the beginning of the full-scale invasion of Ukraine by the Russian Federation, when the Slovak society was very sensitive to the information about the threat to peace in Europe from Russia. After the unsuccessful attempt of the aggressor's armed forces to occupy Ukraine in a very short time, the Russian armed forces began to withdraw from the besieged cities near Kiev. Following the subsequent occupation of these territories by the Ukrainian armed forces, reports of the aggressor's military crimes gradually began to appear in the world media. Public footage provided credible evidence of the Russian Federation committing military crimes on the territory of Ukraine.

The misleading information about the treatment of the Ladomirová cemetery was published by the Embassy of the Russian Federation in Slovakia in September 2022, **at the time of further published reports of military crimes by the Russian armed forces in the town of Izjum.**³³ This information was immediately disseminated in Slovakia by some quasi-media and disinformation actors spreading Russian propaganda.³⁴ **The Slovak police intercepted this false information in time, investigated it and explained to the public the circumstances of the cemetery's renovation.** After the Ambassador continued to publish further misleading information and its dissemination was recorded in many major media outlets in Russia, even in prime time, the **Embassy's activities were assessed as an information operation.**³⁵ The objective was identified as an effort to cover up other emerging reports significantly damaging the reputation of the Russian Federation.

In the following days, some other government departments of the Slovak Republic, the mayor of Ladomirová, and later the Monuments Office of the Slovak Republic were involved in responding to the information operation.³⁶ The Attorney General shared the original unverified information from the Embassy of the Russian Federation. The police have also opened an investigation into the alleged destruction of the graves, as well as an investigation into threats made to the mayor of the village. Mainstream media carried relevant information about the event, based on sources from the SR administration. These activities, but **especially the activities of the SR Police, managed to prevent further dissemination of false information** about the modification of the cemetery in the village of Ladomirová, and thus minimize the achievement of the objectives of the information operation.

33 "VK.com [VK.]" 2023. Vk.com. VK. 2023. https://vk.com/wall418654168_4897.

34 for example, "Facebook." 2022. Facebook.com. 2022. <https://www.facebook.com/212881357517231/posts/486461830159181>.

35 For example, "MIMORIADNE: HOAX FROM RUSSIAN RELATIONSHIP ABOUT SLOVAKIA GOT INTO THE SURPRISING RUSSIAN RELATIONSHIP Hoaxes and Scams - Police of the Slovak Republic www.instagram.com/Hoaxpz... | by Police of the Slovak Republic Facebook." n.d. [www.facebook.com. https://www.facebook.com/watch/?v=652990386385178](https://www.facebook.com/watch/?v=652990386385178).

36 webex.digital. n.d. "Cemetery of the First World War - Statement | Ladomirová | Official Pages of the Municipality." Ladomirova. <https://www.ladomirova.sk/cintorin-z-1-sv-vojny-vyjadrenie-a22-174>.

Timeline:

September 15, 2022	• Embassy of the Russian Federation in Slovakia publishes a misleading report on the destruction of a military cemetery in Ladomirová.
September 16, 2022	• Ambassador of the Russian Federation accuses Slovakia of violating an international agreement. The police are describing the embassy's activity as an information operation and are launching an investigation into whether the law has been violated in the matter.
September 17 - October 2, 2022	• In addition to the SR Police, other state institutions and mainstream media are covering the information operation.
September 20, 2022	• The Ministry of Foreign and European Affairs summoned the Ambassador of the Russian Federation to clarify the published information. ³⁷
July 2023	• The police stopped the criminal prosecution in the case of the threats against the former mayor of Ladomirová on the grounds that it was not a criminal offence. ³⁸
February 2024	• Police have closed their investigation into the alleged destruction of graves in a cemetery containing soldiers from the First World War stating that it is not a criminal offence. ³⁹
July 2024	• The Ministry of the Interior has announced that an offence has been found in the matter of damage to the mushroom, for which the municipality of Ladomirová has been fined EUR 50.

Reflection of the case in the information space:

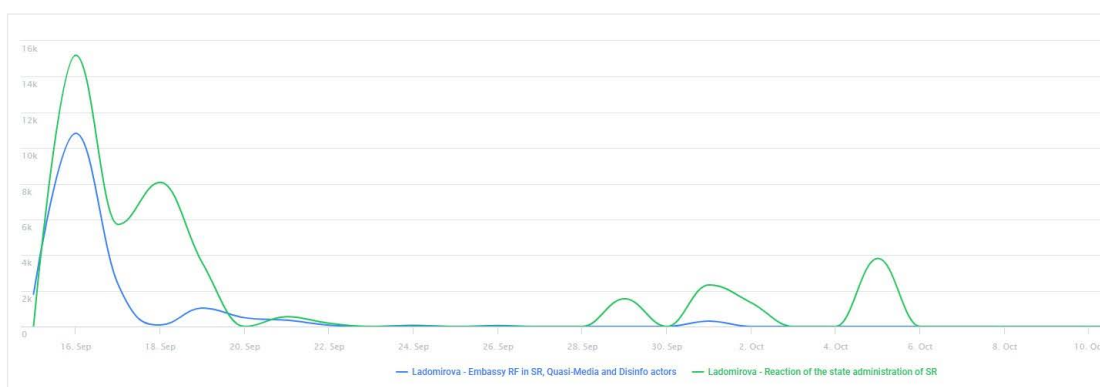
he timely interception of the disinformation by the SR Police and especially its effective response caused the disinformation scene **to engage in sharing and commenting on the news only at the beginning of the event**. It is clear from the graph that the truthful clarification of the circumstances of the whole case had a greater impact on social media than the original disinformation. The graph does not include the reactions of the mainstream media.⁴⁰

37 TASR, and TASR. 2022. "Ministerstvo Si Pre Kauzu Ladomirová Predvolalo Ruského Veľvyslanca." Domov.sme.sk. SME.sk. September 20, 2022. <https://domov.sme.sk/c/23013444/rusko-ladomirova-cintorin.html>.

38 Tomečková, Nicol. 2023. "Polícia Zastavila Trestné Stíhanie v Kauze Vyhrážok Exstarostovi Ladomirovej." RTVS News. July 10, 2023. <https://spravy.rtvs.sk/2023/07/policia-zastavila-trestne-stihanie-v-kauze-vyhrazok-exstarostovi-ladomirovej/>.

39 Frankova, Andrea. 2024. "Polícia Uzavrela Kauzu Poškodených Hrobov v Ladomirovej, Ktorú Rozdúchalo Ruské Veľvyslanectvo." RTVS News. February 14, 2024. <https://spravy.rtvs.sk/2024/02/policia-uzavrela-kauzu-poskodenyh-hrobov-v-ladomirovej-ktoru-rozduchalo-ruske-velvyslanectvo/>.

40 Mainstream media are not included in the chart in order to show more clearly the comparison of state vs. quasi-media.



Interaction between the spread of disinformation about the destruction of the cemetery and the response of the Slovak state administration.

The originally spread disinformation and the reaction of the SR Police **were also responded to on social networks by quasi-media**. But due to the quick clarification of the circumstances of the case, the posts were written with a neutral sentiment. Only a small outreach to individual disinformation actors was noted.

	Name	Content	Interactions	Views	Followers
	Polícia Slovenskej republiky	11	21.26k	32.7k	388.4k
	Ministerstvo zahraničných vecí a európskych...	2	8198	0	47.35k
	nocomment.sk	3	6833	0	66.74k
	Hoaxy a podvody - Polícia SR	2	4712	0	125.3k
	Maroš Žilinka - generálny prokurátor SR	1	3919	0	37.66k

Sources that have reacted most to the news in the case of the cemetery in Ladomirová (Data retrieved from Juno in May 2024.)

Rating:

Although the response of the state institutions was not ideal in all respects, **it can be considered an example of good practice because of the successful coordination of state administration units dealing with hybrid threats and the sufficient minimization of the objectives of the information operation**. The SR Police responded transparently to the event by also launching an investigation into the criminal offence of defamation of graves and also by investigating dangerous threats against the mayor of the municipality.

The system for monitoring and responding to information operations was inadequate, as staff from specialized units continued to respond to the information operation outside working hours, as the incident started on Thursday in the early evening and continued into the following weekend. The successful response took place without approved and rehearsed procedures, executed solely on the basis of staff's own commitment and training.

The Attorney General reacted inadequately by sharing the original status of the Russian Embassy in Slovakia without verification, did not clarify the sharing of the information, and only objected to

the accusation of spreading propaganda. He did not comment further on the case. On the other hand, **the mayor of Ladomirová responded proactively to the dissemination of false information about the destruction of the cemetery by issuing a clarifying statement** on the website of the website of the municipality and also by trying to explain the event to the Ambassador of the Russian Federation in Slovakia in person. However, his request for a meeting was denied.

The Slovak **mainstream media took over the information from the state administration and continuously reported on the development of the case, also with a warning that it was an information operation.**⁴¹ Political actors commented on the ongoing information to a minimal extent and with a positive sentiment, given the clarity of the case.⁴²

CASE STUDY 2: Website blocking

The screenshot shows the website of the National Security Office (NSO) of the Slovak Republic. The main heading is "Zoznam blokovaných subjektov" (List of blocked subjects). Below this, there is a table with columns: "Názov" (Name), "Rozhodnutie podľa" (Decision according to), "Dôvod" (Reason), and "Platnosť do" (Valid until). The table lists several websites that have been blocked, including "hlavnespravy.sk", "armadnymagazin.sk", "hlavnydennik.sk", and "infovojna.bz". The reason for blocking is "škodlivá aktivita" (harmful activity) under the "zákon č. 69/2018, § 27b" (Act No. 69/2018, § 27b). The validity period for all listed blocks is "30. 06. 2022".

Názov	Rozhodnutie podľa	Dôvod	Platnosť do
hlavnespravy.sk	zákon č. 69/2018, § 27b	škodlivá aktivita	30. 06. 2022
armadnymagazin.sk	zákon č. 69/2018, § 27b	škodlivá aktivita	30. 06. 2022
hlavnydennik.sk	zákon č. 69/2018, § 27b	škodlivá aktivita	30. 06. 2022
infovojna.bz	zákon č. 69/2018, § 27b	škodlivá aktivita	30. 06. 2022

Below the table, it states: "Zoznam bude priebežne aktualizovaný." (The list will be updated regularly). The date of the first publication is "14. 03. 2022" and the last update is "21. 03. 2022 12:01".

Source: aktuality.sk

Date: February 26 - June 6, 2022

Summary:

In the wake of Russia's military aggression against Ukraine, the National Assembly approved an amendment to the law on cybersecurity that allowed the National Security Office (NSA) to block access to websites spreading serious disinformation. This measure was temporary and was to be replaced by a more comprehensive regulation. However, it was not adopted and access to the websites in question was restored when the blocking expired in June 2022. The lack of strategic communication about the reasons for the blocking, the lack of transparency of the process and the ves-

41 Čevelová, Jana. 2023. "Polícia Upozorňuje Na Ruskú Informačnú Operáciu: Radiácia Z Ukrajiny Je Hoax." Dennik N. May 18, 2023. <https://dennikn.sk/minuta/3377046/>.

42 for example, "Facebook." 2022. Facebook.com. 2022. <https://www.facebook.com/416203666536739/posts/662638848559885>.

ting of decision-making power in the hands of an executive body (the National Security Authority) raised doubts from the outset and led to the failure of the measure and accusations of censorship.

The course of the case:

At the same time as the war in Ukraine, an information war has been launched, which includes the dissemination of hostile propaganda from across the border. It was disseminated by several websites, and according to published information, some of them were also financially or otherwise linked to entities from the Russian Federation.⁴³ In the context of the ongoing military aggression and due to fears of a possible spread of the conflict, an **amendment to the Cyber Security Act was adopted in an abbreviated legislative session, which allowed the NSA to block these websites in Slovakia by decision.**

Due to the lack of communication from the government about the reasons for the adoption of this amendment and also due to the **problematic aspects of the adopted legislation** (the NSA, not the court, decides on blocking, the decisions are not public, they are not preceded by a call to remove the problematic content), the **crisis began to grow**. Questions about the constitutionality and the conformity of the adopted solution with the case law of the European Court of Human Rights (ECtHR) served as a reason to question the entire adopted solution.⁴⁴ **Moreover, the entire process from the adoption of the initial amendment to the submission of the revised version to the National Assembly in the autumn of 2022 was accompanied by considerable chaos and inconclusiveness** on the part of the representatives of the government coalition.⁴⁵

It was not clear what criteria the NSA used to decide whether to block other websites that spread "serious disinformation", as the decisions were not public. At the time, there were many more sources in the Slovak information space that disseminated this type of content.⁴⁶ However, the NSA did not issue any further decisions on blocking other websites until 30 September 2022. Moreover, in practice, the incompleteness of the entire legal regulation became apparent, as the blocking only applied to the websites themselves and not to the social media profiles of the media in question. As a result of all these reasons, criticism of the adopted amendment and accusations of censorship began to dominate quite quickly, which went hand in hand with a change in the attitude of the Slovak public towards the war in Ukraine.

Similarly chaotic was the preparation of the comprehensive legislation that was to replace the amendment of February 2022. The original proposal from the NSA in May 2022 was withdrawn after a large number of comments and had to be redrafted. The reaction to the adoption of this temporary legislation, which was to be replaced by a more comprehensive and sophisticated regulation, was also influenced by disputes within the government coalition, due to which the new legislation

43 Lukáš Kosno. 2022. "Ako NBÚ Blokuje Dezinformačné Weby. Pri Hlavných Správach Znemožnil Aj Prístup K Zálohám." Živé.sk. Ringier Slovakia Media s.r.o. March 28, 2022. <https://zive.aktuality.sk/clanok/Givgndd/ako-nbu-blokuje-dezinformacne-weby-pri-hlavnych-spravach-znemozil-aj-pristup-k-zaloham/>.

44 "Blokovanie Webových Stránok a Jeho Možný Rozpor S Judikaturou Európskeho Súdu Pre Ľudské Práva - Právne Listy." 2022. legallists. En. 2022. <https://www.pravnelisty.sk/clanky/a1062-blokovanie-webovych-stranok-a-jeho-mozny-rozpor-s-judikaturou-europskeho-sudu-pre-ludske-prava>.

45 Thanks to these shortcomings, for example, the hastily approved extension of the NSA's powers to block serious disinformation until September 2022 did not apply to the decisions already issued (4 blocked websites), which expired on 30 June 2022. On 15 June 2022, the National Assembly of the Slovak Republic approved an amendment to the Cybersecurity Act, which extended the blocking period, but did not apply to the decisions already issued by the NSA.

46 For example, a website linked to the Russian FSB secret service News-front.info, which also existed in Slovak.

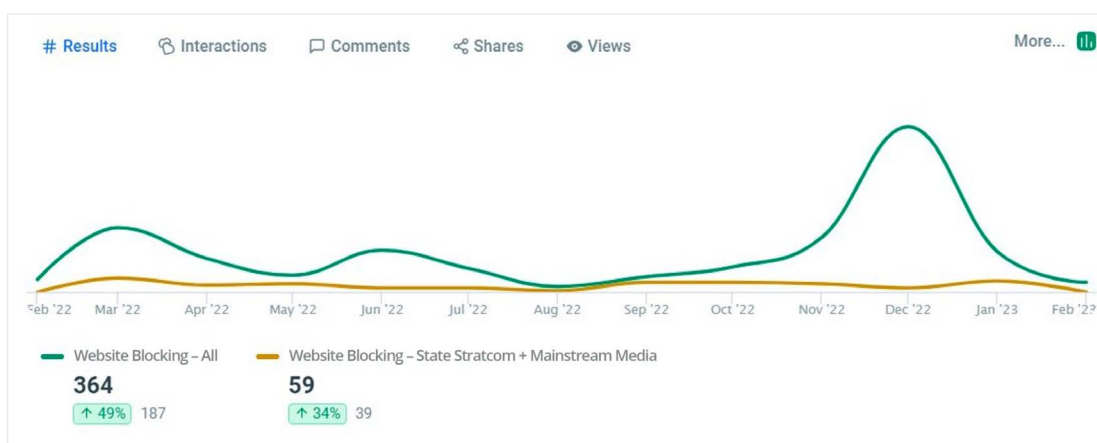
was not approved during the validity of the original amendment. The final straw in the whole process was the fall of the government at the end of 2022. As a result of the change in political processes and the politicization of the issue of blocking, the government's draft comprehensive legislation was not approved in January 2023; the whole legislation was de facto ineffective as of June 2022.

Timeline:

February 26, 2022	• Approval of an amendment to the Cybersecurity Act by the Slovak Parliament as part of the "lex Ukraine" package of measures, which allowed the NSA to block websites containing "serious disinformation".
March 2, 2022	• NSA starts blocking three websites.
March 22, 2022	• Start of blocking of internet radio and infovojna.sk website.
June 15, 2022	• Adoption of an amendment to the Cybersecurity Act to extend blocking until 30 September 2022.
July 1, 2022	• Termination of the NSA's decision to block four websites.
September 30, 2022	• Expiry of the extended deadline for the NSA's decision to block websites.
November 2, 2022	• Approval of a comprehensive amendment to the Cybersecurity Act at the Government meeting.
February 1, 2023	• The National Assembly of the Slovak Republic returned the draft law to the drafters for completion in the first reading.

Reflection of the case in the information space:

The information space was clearly dominated by sources rejecting the measure, with a total of 364 posts over a 12-month period. In contrast, the state and mainstream media (private and public) covered the issue in only 59 articles.



Comparison of the number of posts and articles about blocking websites among a group of state institutions and mainstream media (59) and other sources, including disinformation actors (364). The observation period was 12 months from 24 February 2022 to 28 February 2023. Due to the low number of identified contributions in the media and stratcom group, it was not possible to compare engagement. (Data retrieved from Juno in May 2024.)

Similarly, the comparison of interaction rates was significantly in favor of quasi-media and disinformation actors. Quasi-media had 12 times more interactions on their posts on a given topic, compared to state sources and mainstream media - 24,860 interactions for quasi-media vs. 2,871 for the latter group of sources. In the first days after the blocking was introduced, a great wave of resistance and accusations of totalitarian practices and censorship arose throughout the disinformation scene. This wave was joined by the representatives of some political parties, who used the shortcomings of the legislation and the chaos that accompanied the blocking to politicize the whole issue.

This measure was controversially received by the public. According to a CEDMO opinion poll from July 2022, 33% of the Slovak population agreed with the measure, 25% perceived it as a controversial step and 23% rejected it.⁴⁷

Rating:

In spite of the original good intentions of the promoters - to prevent the propaganda of the hostile foreign power that invaded Ukraine at that time from spreading on the territory of Slovakia - the measure missed the mark. The chaos of the drafting and the lack of sophistication of the adopted solution led to criticism of the whole blocking process. Similarly, the efforts to correct the original temporary measure were accompanied by considerable chaos, which ultimately led to the ineffectiveness of the legislation in question and failed to extend it even until September 2022.

In addition, due to the lack of communication from the government and the lack of transparency of the entire process, the blocking became politicized and the attitude that it was censorship prevailed in public discourse. This is also evidenced by public opinion polls. Given the short period of time during which the blocking of a limited number of websites was effective, it is possible to assess the impact of the blocking as not fulfilling the original objective with which it was adopted.

⁴⁷ Ostrozovicova, Barbora. 2022. "Informačná Vojna (Prieskum CZ+SK)". IPSOS. July 21, 2022. <https://www.ipsos.com/sk-sk/informacna-vojna-prieskum-czsk>

CASE STUDY 3: Spreading disinformation about refugees from Ukraine



Source: Central European Digital Media Observatory - "Post exaggerates spending to support Ukrainian refugees" available at: <https://cedmohub.eu/cs/prispevek-zvelicuje-vydaje-na-podporu-ukrajinskych-uprchliku/>

Date:

February 2022 - May 1, 2024

Summary:

Since 2022, disinformation targeting Ukrainian refugees in the Czech Republic has fueled societal tensions, including false claims of preferential treatment and instigating conflict with Roma communities. Initial measures, like blocking nine pro-Kremlin websites, had limited effects as disinformation shifted to social media. Campaigns such as "We Work Where We Are Needed" promoted refugees' contributions, while efforts to mitigate social unrest succeeded but lacked proactivity.

Progress of the case:

Since the beginning of the full-scale invasion of Ukraine by the Russian Federation, the Czech Republic has become a new home for an unprecedented number of refugees from Ukraine. They have fallen victim to a number of disinformation campaigns.

In the first phase, a number of disinformation channels claimed that people from Africa and Afghanistan were abusing the war in Ukraine to cross the border and that mandatory quotas for redistributing migrants had returned. This was followed by narratives, which continue to this day, concerning the alleged favoritism of Ukrainian refugees by the welfare system.

A number of disinformation campaigns, manipulations and inaccuracies in the information space have at least contributed to the anti-government and anti-Ukrainian protests and to the spread of hatred and violent conflict between the Romani and Ukrainian communities in the Czech Republic.

Immediately after the outbreak of the invasion, domain provider NIC.cz blocked several websites known for spreading pro-Kremlin narratives and propaganda. This was done after consultation with security forces and on the basis of a government recommendation. These were 9 websites in total and some of them are still not functional. In essence, it was only a matter of shutting down specific web domains; the activities of these quasi-media on social media were not affected by this measure. Many of them have moved to social networks or new domains and their activity and impact has been delayed for a while rather than stopped completely.

In July 2022, the Ministry of Labor and Social Affairs published an analysis on Ukrainian refugees, highlighting their status in the Czech Republic and describing their background and the challenges they face. In this way, many of the disinformation spreading in the information space was put to rest. However, the release of the analysis was not accompanied by any major information campaign. The topic of Ukrainian refugees in the Czech Republic was also repeatedly addressed by specific ministers who tried to urge solidarity, as well as by the Police of the Czech Republic, which reported on security incidents.

Czech state institutions did not react proactively or preventively in the information environment at all until the second anniversary of the Russian invasion of Ukraine. As part of this anniversary, Czech NGOs, together with the Office of the Government and the Office of the President of the Republic, organized the "Day for Ukraine" event, the purpose of which was to support Ukraine and its people in their fight against Russian aggression and to express solidarity with Ukrainian society through a series of rallies, marches and concerts.

The Ministry of the Interior, the Office of the Government, the Commissioner for Human Rights, and the Czech office of the International Organization for Migration have prepared a campaign called "We Work Where We Are Needed", which aims to present the stories of Ukrainian refugees who have found work in the Czech Republic and to show their contribution to Czech society. This campaign runs online and offline from April 2024.

At the level of crisis communication, state institutions have been extensively involved in de-escalating conflicts between the Ukrainian and Roma communities. This case has shown that state institutions are able to coordinate multiple actors in crisis communication, and at the informal level, some communication and coordination channels that are still used, but not formalized or institutionalized, have been set up.

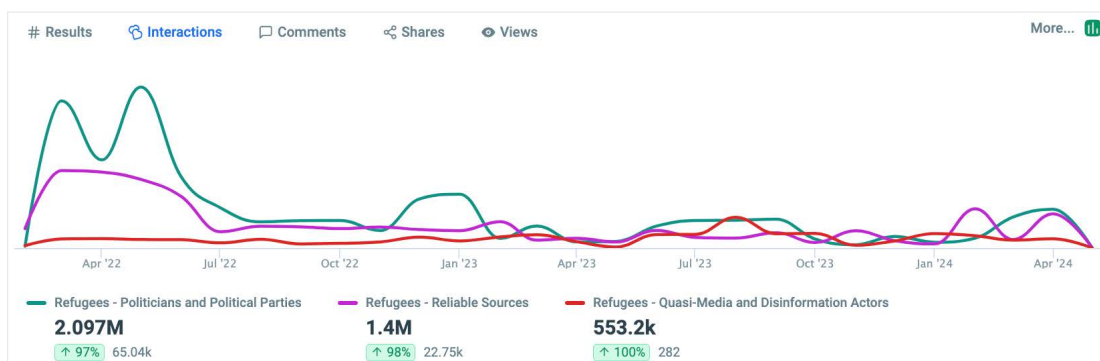
Similarly, state institutions and the Police of the Czech Republic were able to very quickly refute the disinformation that began to spread after the tragic shooting at the Faculty of Arts at Charles University in Prague, which claimed that the shooter might have been Ukrainian.

Timeline:

February 2022	• The Czech Republic is starting to accept the first Ukrainian refugees and the first disinformation is also spreading that people from Africa and Afghanistan are taking advantage of the war in Ukraine to cross the border illegally and that their admission has renewed the mandatory redistribution of migrants.
End of February 2022	• The blocking of several websites that spread pro-Kremlin narratives and propaganda.
July 2022	• The Ministry of Labor and Social Affairs of the Czech Republic has published an analysis on Ukrainian refugees.
February 2023	• Launch of the "Thank You. We couldn't have done it without you."
Summer 2023	• The launch of the Ministry of the Interior's bulletin board campaign, which is discussed in more detail in the next chapter.
July 2023	• Disinformation is beginning to spread containing unsubstantiated claims that Ukrainians are committing violence against Roma and forming gangs.
December 2023	• Disinformation is beginning to circulate that a Ukrainian was behind the shooting at the Faculty of Arts.
Summer/Autumn 2023	• Anti-government/anti-Ukrainian protests.
February 2024	• Commemorating two years since the start of the Russian invasion of Ukraine.
April 2024	• Launch of the "We work where we need to" campaign.

Reflection of the case in the information space:

The information space on the topic of Ukrainian refugees in the Czech Republic has long been dominated by the Czech political representation. Politicians communicated about this topic with greater reach than mainstream media, state institutions and NGOs, despite the lower overall number of contributions. The most frequent were politicians representing the current opposition parties. On the other hand, ministers, who often commented on the topic of Ukrainian refugees, did not achieve nearly the same amount of coverage.



Comparison of interactions between monitored groups of accounts reporting on refugees from Ukraine.

Sources		Interactions	
Refugees - Politicians and Political Parties		Refugees - Reliable Sources	
Name	Interactions	Name	Interactions
Tomio Okamura - SPD	1.308M	ČT24	202.7k
Karla Maříková	106.6k	Visegrádský jezdec	139.4k
Andrej Babiš	71.43k	Petr Fiala	76.73k
Jana Zvrtek Hamplová...	66.18k	Evropa Neasi	61.45k
Radim Fiala - SPD	59.09k	Události Brno	61.42k
MUDr. Jiří Mašek	56.03k	CNN Prima NEWS	53.81k
Refugees - Quasi-Media and Disinformation Actors		Name	Interactions
		Jindřich Rajchl	180.6k
		neČT24	59.42k
		Matouš Bulíř	39.08k
		Selský Rozum	31.52k
		Raptor-TV.cz	30.22k
		Alliance národních sil	29.24k

Comparison of interactions of individual accounts of the main actors reporting on refugees from Ukraine within the monitored groups.

A positive aspect in this case is the visible impact of (albeit late organized) cooperation and coordination between state institutions and civil society. The graph below shows that specific influencers and NGOs and their contributions achieve significantly more popularity than the accounts of government politicians or the President of the Republic.

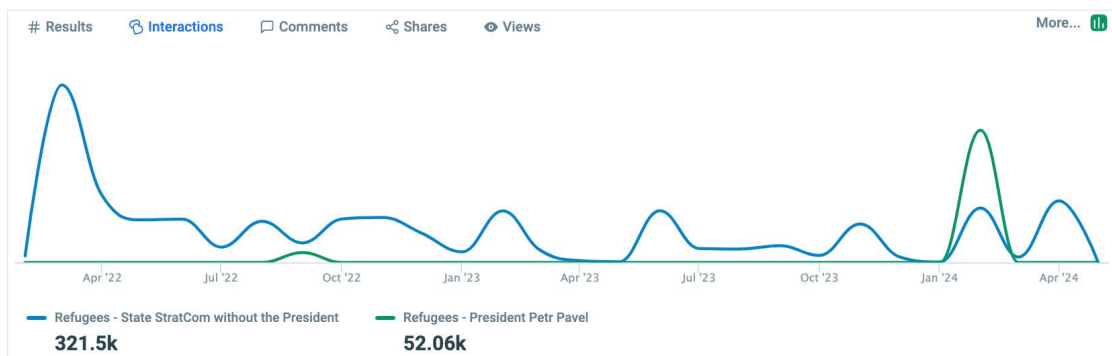


A more detailed look at the interactions of posts from credible sources reporting on refugees from Ukraine within each subgroup.

Sources			Interactions		
Refugees - Mainstream Media			Refugees - Civil Society		
Name		Interactions	Name		Interactions
ČT24		202.7k	Visegradský jezdec		137.6k
Události Brno		61.42k	Evropa Neasi		61.45k
CNN Prima NEWS		53.81k	ROMEA		37.5k
Události Ostrava		50.96k	dnesnaukrajine.cz		31.45k
IDNES.cz		33.66k	Tereza Koubková		20.72k
Blesk.cz		24.7k	Paralelní listy		17.93k
Refugees - State StratCom					
Name		Interactions			
Petr Fiala		76.73k			
Petr Pavel		43.48k			
Vít Rakušan		38.27k			
Markéta Pekarová Adamová		27.55k			
Vít Rakušan		22.33k			
Markéta Pekarová Adamová		21.94k			

A more detailed look at the interactions of posts from credible sources reporting on refugees from Ukraine within each subgroup.

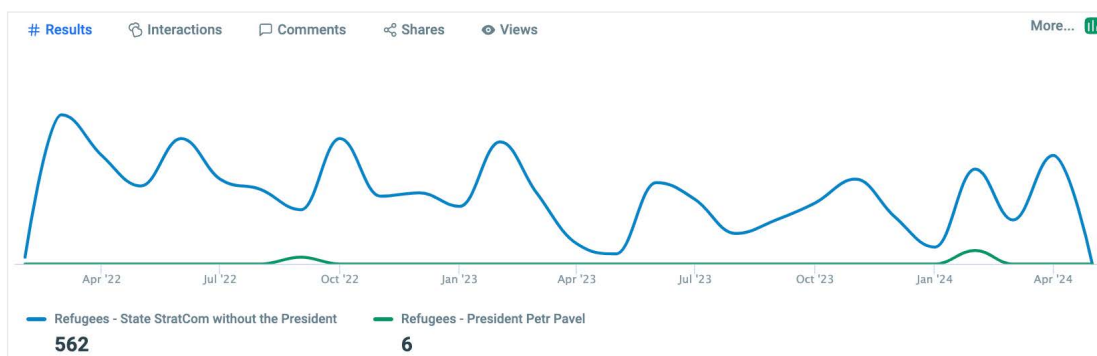
Last but not least, we can see that the President of the Republic's social media accounts are an absolutely crucial part of the strategic communication of the state. Although the presidential accounts produced only 6 posts during the second anniversary of the Russian invasion of Ukraine (3 on Facebook and 3 on Instagram), the number of interactions with these posts clearly exceeds all other state posts.



Comparison of the interaction of the state's StratCom posts on refugees from Ukraine with President Peter Pavel's posts.

Sources			Interactions		
Refugees - State StratCom without the President			Refugees - President Petr Pavel		
Name		Interactions	Name		Interactions
Petr Fiala		76.73k	Petr Pavel		43.48k
Vít Rakušan		38.27k	Petr Pavel		8588
Markéta Pekarová Adamová		27.55k			
Vít Rakušan		22.33k			
Markéta Pekarová Adamová		21.94k			
Vít Rakušan		14.25k			

Comparison of the interaction of the state's StratCom posts on refugees from Ukraine with President Peter Pavel's posts.



Comparison of the number of state's StratCom posts with those of President Petr Pavel.

Sources			Content		
Refugees - State StratCom without the President			Refugees - President Petr Pavel		
Name		Content	Name		Content
Petr Fiala		34	Petr Pavel		3
Vít Rakušan		19	Petr Pavel		3
Markéta Pekarová Adamová		9			
Vít Rakušan		18			
Markéta Pekarová Adamová		9			
Vít Rakušan		16			

Comparison of the number of posts of individual state's StratCom accounts with the accounts of President Petr Pavel.

Rating:

At the start of the invasion, the Czech Republic quickly responded by blocking nine websites that spread pro-Kremlin narratives. This step had only a limited impact, as the disinformationists moved to social networks and new domains. Moreover, the blocking of these sites was carried out by the domain provider in consultation with state institutions, not by the state itself, and thus without a clearly defined legislative framework. It was therefore a swift but non-transparent response with limited impact. If the state were to take a similar step in the future (and it is questionable whether this is a necessity), it should be done on the basis of a clear and legally based procedure.

The next step was the release of an analysis by the Ministry of Labor and Social Affairs in July 2022, which shed light on the status of Ukrainian refugees and refuted much of the disinformation circulating. This analytical approach was an important step towards providing factual information to the public. Campaigns such as "A Day for Ukraine" and "We work where we are needed" then aimed to support Ukraine and present positive stories of Ukrainian refugees in Czech society. These campaigns contributed to building a positive image of refugees and were an important element in the fight against disinformation.

De-escalation of conflicts between the Ukrainian and Roma communities was also an important aspect. The Ministry of the Interior and other state institutions have actively addressed this issue, which has demonstrated the ability of the state to coordinate crisis communication between different actors. This approach was key to maintaining social peace and preventing violence.

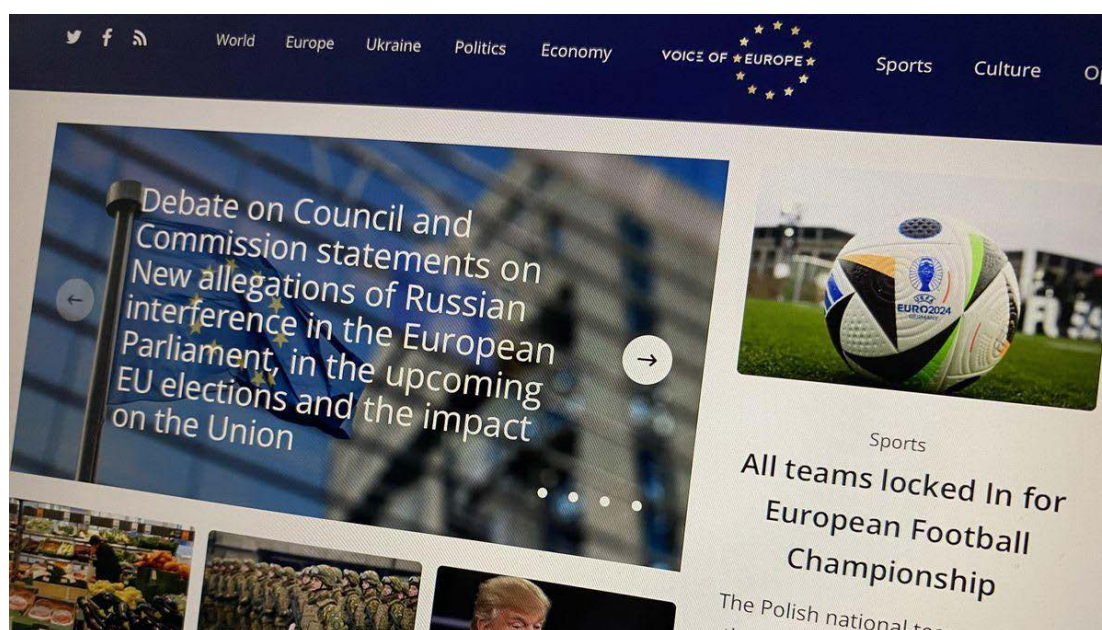
However, the state's response to the spread of disinformation has been largely reactive. The state has not been proactive enough in responding to the spread of disinformation and instead has only reacted to the crisis situations that have already arisen. This lack of proactive communication created an information vacuum that was easily filled by disinformers.

Another weakness was the limited ability of state institutions to reach the general public. Politicians had a greater reach to the public than ministers and state institutions, which weakened the effectiveness of state corruption. Moreover, government communication often lacked a unified and coordinated approach, leading to an inconsistent response to the spread of disinformation. While cooperation with civil society and influencers has helped the situation significantly, it has happened too late and only in fits and starts.

Lack of funding has also limited the state's ability to effectively promote its campaigns. The state lacked funding for social media advertising, which reduced the reach and effectiveness of its communication efforts. The lack of formal strategic communication and coordination with civil society further weakened the state's response to disinformation.

Overall, the state's response to the spread of disinformation about Ukrainian refugees was characterized by a combination of quick and ill-conceived steps at the beginning, followed by reactive and insufficiently coordinated communication. While important steps have been taken to dispel disinformation and de-escalate the conflict, the overall approach has been limited by a lack of proactivity, funding and clear legislation.

CASE STUDY 4: Unveiling the Voice of Europe network



Source: Seznam zprávy

Date:

March 2024

Summary:

The case of the Voice of Europe network is a critical example of the Russian Federation's ongoing efforts to influence political processes and destabilize democratic institutions in the European Union. This platform, operated under the guise of an independent media outlet, has been strategically used to spread pro-Kremlin narratives and covertly fund sympathetic political candidates.

The course of the case:

Voice of Europe was a registered news platform in Prague with a significant online presence, amassing more than 180,000 followers on platforms such as Facebook and X. The platform published content in several languages, including German, and was characterized by its anti-EU and pro-Kremlin stances. It frequently featured articles and interviews with far-right European politicians and promoted narratives aligned with Kremlin interests, including opposition to EU sanctions against Russia or criticism of Western support for Ukraine.⁴⁸

The BIS investigation began in early 2023 and culminated in the public exposure of the network in March 2024, working closely with other European intelligence services, including those in Belgium and Poland, to untangle a tangled web of financial transactions and political connections.⁴⁹

The Czech Republic, with the support of Belgian and other European intelligence services, has taken precautions. Namely, the imposition of sanctions on Voice of Europe, Medvedchuk and Marchevsky, the freezing of their assets, and the associated public statement about their disclosure.

Following this case, the Czech Republic has also proposed legislative measures to restrict the movement of Russian diplomats within the EU.⁵⁰

Timeline:

- | | |
|--------------------------|--|
| Beginning of 2023 | • Security Information Service (BIS) launches Voice of Europe investigation |
| March 2024 | • BIS publicly exposes the network involving Medvedchuk and Marchevsky |
| March 27, 2024 | • Czech government imposes sanctions on Voice of Europe and key persons involved in the project. |
| End of March 2024 | • European and national security services in the EU are carrying out related investigations. |

Reflection of the case in the information space:

Although the exposure of the Voice of Europe network was a significant success for the Czech security forces, the case had minimal impact in the information space. Even though the revelation resonated widely abroad. The case was not used by state institutions to educate the public about the workings of Russian propaganda and the Kremlin's informational and political influence, nor was it used to highlight the work of the Security Information Service or the workings of the national san-

48 "VOICE OF EUROPE." 2024. Seznam Zprávy. <https://www.seznamzpravy.cz/tag/voice-of-europe-110354>.

49 Ibid.

50 "Česko bojuje za omezení pohybu ruských diplomatů v Schengenu." 2024. Novinky.cz. <https://www.novinky.cz/clanek/zahranicni-evropa-cesko-bojuje-za-omezeni-pohybu-ruskych-diplomatu-v-schengenu-40468913>.

ctions list. The relatively weak communication can also be seen in the graph below, which shows a relatively small number of contributions compared to all the sources monitored.

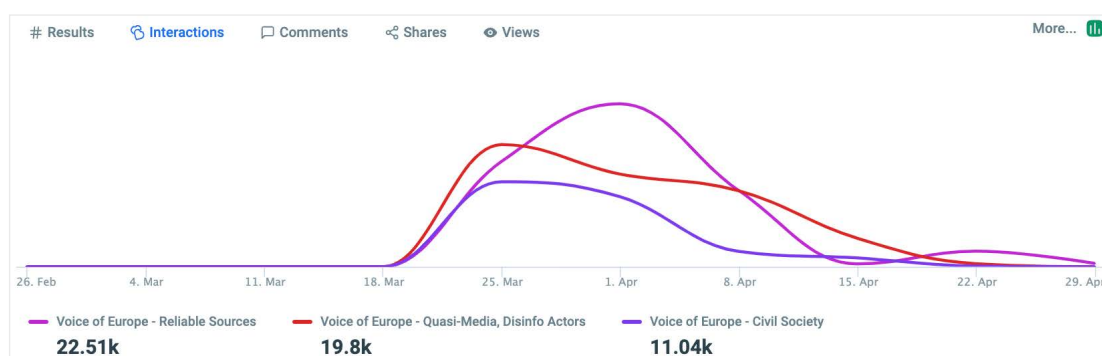


Comparison of the number of posts within monitored groups reporting on the Voice of Europe network exposure.

Sources				Content			
Voice of Europe - Reliable Sources				Voice of Europe - Quasi-Media, Disinfo Actors			
Name	Content	Name	Content	Name	Content	Name	Content
Události Luďka Staňka	2	Jindřich Rajchl	3	dnesnaukrajine.cz	2		
CNN Prima NEWS	3	Roman Kirsch	6	Visegradský jezdec	1		
Deník N	5	Aby bylo jasno	1	Evropa Neasi	2		
ČT24	3	Aby bylo jasno	1	Jiří Hřebenar	7		
Newsroom ČT24	10	Raptor-TV.cz	3	Poslední skaut	2		
Deník N	23	neČT24	2	Milion chvilék pro demokracii	1		

Comparison of the number of posts by individual accounts within the monitoring groups reporting on the Voice of Europe network exposure.

However, it is worth noting that even though the disinformation scene has not devoted a large number of posts to the case, it is not much different from credible sources and mainstream media in terms of the number of interactions.



Comparison of interactions within monitored groups reporting the Voice of Europe network exposure.

Sources				Interactions	
Voice of Europe - Reliable Sources		Voice of Europe - Quasi-Media, Disinfo Actors		Voice of Europe - Civil Society	
Name	Interactions	Name	Interactions	Name	Interactions
Události Luďka Staňka	3035	Jindřich Rajchl	8734	dnesnaukrajine.cz	2734
CNN Prima NEWS	2660	Roman Kirsch	5311	Visegradský jezdec	2650
Denik N	2098	Aby bylo jasno	1736	Evropa Neasi	1843
ČT24	1829	Aby bylo jasno	1485	Jiří Hřebenar	1704
Newsroom ČT24	1651	Raptor-TV.cz	730	Poslední skaut™	684
Denik N	1608	neČT24	619	Milion chviliek pro demokracii	526

Comparison of the interactions of individual accounts within the monitored groups reporting the Voice of Europe network exposure.

Rating:

This case represents a significant step in the fight against Russian disinformation campaigns and hybrid threats. The network, which presented itself as an independent media outlet, was in fact spreading pro-Kremlin narratives and supporting political candidates sympathetic to Russia. The BIS exposed the network and contributed to the freezing of the assets of key individuals involved in the project and the imposition of sanctions on Voice of Europe. These steps were important not only for the Czech Republic, but for the European Union as a whole.

The Czech Republic's response to the Voice of Europe network revelations has brought some increased awareness of Russian interference in internal affairs and may have led to further scrutiny of security protocols in the EU. The revelations have also led to increased attention to far-right and Eurosceptic politicians and parties in Europe, many of whom have faced internal party investigations. The case illustrates the effectiveness of coordinated intelligence efforts and the importance of transparency in combating hybrid threats.

Despite these successes, the Czech response has several shortcomings, especially in the area of communication of the case. The exposure of the Voice of Europe network was not sufficiently used in the information space to educate the public about the workings of Russian propaganda and the political influence of the Kremlin. State institutions did not use the case to highlight the work of the BIS or to raise awareness of the national sanctions list. Communication has been poor, which is also evident from the graphs showing the low number of contributions to this case from all monitored sources.

The state did not inform key persons in the ministries and no documents were prepared for journalists, which led to confusion and unpreparedness when answering media questions. Ideally, a comprehensive communication strategy could have been prepared in advance, both for the Czech public and abroad, to ensure that the public and state officials were well informed about the steps taken in relation to the revelations. It could also have strengthened the solidarity of other EU countries.

Summary:

In Slovakia, the case of the cemetery in Lodomirová has shown a high level of coordination between the different branches of the state administration. When misleading information about the destruction of a military cemetery by the Russian Embassy was published, Slovak state institutions, including the Slovak Police, reacted quickly and efficiently. The police immediately verified and refuted the disinformation, informed the public and minimized the achievement of the objectives of the Russian information operation. The response was also supported by other departments, including the Ministry of Foreign Affairs, which summoned the Russian Ambassador to clarify the situation. Slovak media then took over information from the state administration, which contributed to a unified and informed narrative in the media.

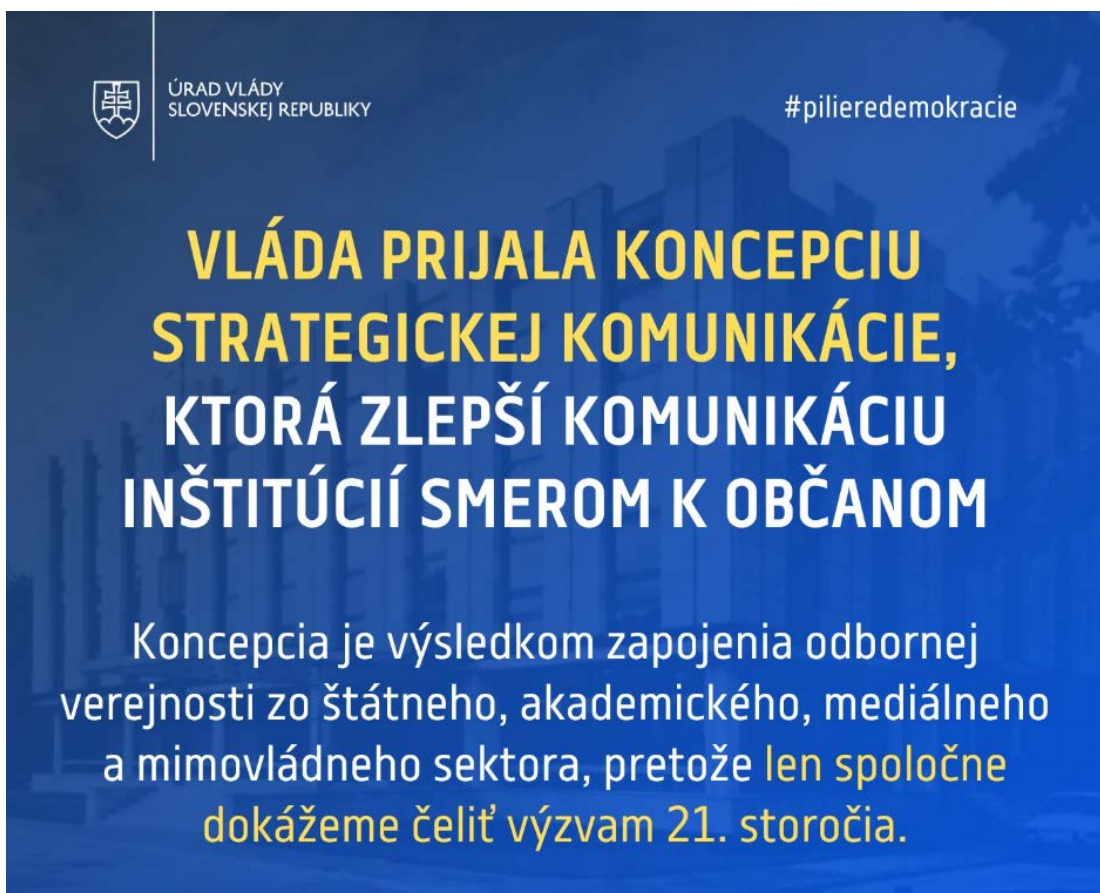
On the contrary, the case of website blocking in Slovakia has shown a number of shortcomings, especially in the area of strategic communication and transparency of the process. Despite good intentions, legislative chaos and a lack of communication led to accusations of censorship and politicization of the measure. The decision on blocking was entrusted to the National Security Office (NSA), not to the courts, raising doubts about the constitutionality of the move. Moreover, the blocking only applied to websites, not their social media accounts, which limited the effectiveness of the measure.

In the Czech Republic, the case of the spread of disinformation about Ukrainian refugees showed the reactive and uncoordinated approach of state institutions. Although some important steps were taken, such as blocking websites spreading pro-Kremlin narratives, publishing an analysis on Ukrainian refugees and organizing campaigns in support of Ukraine, the state response was often delayed and insufficiently coordinated. The response was largely reactive and lacked proactive strategic communication, creating an information vacuum that was easily filled by disinformation agents. Opposition politicians had greater public outreach than ministers and state institutions, which weakened the effectiveness of state communication.

The case of the exposure of the Voice of Europe network in the Czech Republic showed the effectiveness of a coordinated intelligence effort, where the BIS cooperated with European intelligence services and uncovered a network spreading pro-Kremlin narratives. However, the communication of the whole case was weak. State institutions did not use the case to educate the public about the workings of Russian propaganda and the Kremlin's political influence. There was a lack of a coordinated communication strategy and preparation of materials for journalists, which led to confusion and unpreparedness when answering media questions.

In conclusion, all four case studies show that the most important weakness in both countries remains strategic communication, without which no effective action against disinformation campaigns can be taken.

CASE STUDY 1: Creating a strategic communication system in the Slovak Republic



Description: Facebook post by the Office of the Government of the Slovak Republic after the adoption of the strategic communication concept on 13 June 2023

Summary:

Changes in the security environment in Europe after the annexation of Crimea by the Russian Federation in 2014 have increased the risk of hybrid activities and highlighted the need to strengthen the overall resilience of the Slovak Republic to these threats. Hybrid actions aim in particular to destabilize society and undermine trust in the democratic establishment and in the membership of international institutions. Strategic communication acts as prevention and protection of society and the state, as it helps to effectively inform citizens about current security threats and builds resilience to hybrid action. In the period 2021-2023, the Government of the Slovak Republic successfully strengthened existing and built new structures for strategic communication, adopted concept documents and set up a coordination mechanism, thus contributing to a substantial increase in competence in this area.

Date:

2021–2023

Progress of the case:

The Slovak Republic has seen an increased intensity of hybrid threats since approximately 2014, since the annexation of Crimea by the Russian Federation. Since then, the Slovak information environment has been the target of disinformation campaigns and influence operations.⁵¹ The international crises caused, for example, by the COVID-19 pandemic or the Russian invasion of Ukraine have reinforced this trend.⁵² Such hybrid operations are quite successful - according to opinion polls from 2022, up to 54% of the Slovak population tends to believe conspiracy theories or disinformation.⁵³ According to a 2023 survey, up to 50% of citizens distrust state institutions.⁵⁴

Strategic communication is one of the key tools in increasing state security and strengthening the resilience of society against hybrid threats.⁵⁵ The Government of the Slovak Republic has started to develop a system of strategic communication by gradually adopting policies and strategic documents since 2018, when the Concept for Combating Hybrid Threats was adopted, which contained the first mention of strategic communication. The SR Security Strategy (2021) defined a commitment to develop the capacity of the public administration and to strengthen the mechanism of cooperation with the non-governmental, academic and media sectors in the field of countering disinformation and promoting strategic communication.⁵⁶ The Defense Strategy of the SR (2021) set out to support the development of strategic communication for the long-term continuity of defense policy and its social support.⁵⁷ The Action Plan for Coordination against Hybrid Threats of the SR (2022) defined specific tasks to build up the system and structures of strategic communication at the Office of the Government of the SR, the Ministry of the Interior of the SR and the Ministry of Defense of the SR.⁵⁸

The establishment of structures and the adoption of public policies in the field of strategic communication have contributed to the improvement of the Slovak Republic's capability in this area in a relatively short period of time during the period 2021-2023, mainly thanks to an EU-funded national project. During this period, there has been a significant increase in staff capacity dedicated to hybrid threats and strategic communication.⁵⁹ Also, the Strategic Communication Concept of the Slovak Republic (2023) was adopted, which focused in particular on more effective cooperation of state institutions in strategic communication with the involvement of the academic, media, private and NGO sectors and a faster state response in the fight against disinformation.⁶⁰

51 Ministry of Interior of the Slovak Republic. 2023. "O Strategickkej Komunikácii - HybridneHrozby.sk." HybridneHrozby.sk. September 8, 2023. <https://www.hybridnehrozby.sk/2971/o-strategickej-komunikacii-2/>.

52 "Concept of Strategic Communication of the Slovak Republic Bratislava 2023." n.d. Accessed August 28, 2024. https://www.vlada.gov.sk/share/uvsr/koncepcia_strategickej%20komunikacie_sr.pdf?csrt=12155556465759032409.

53 Ibid.

54 Trends in [Non]Trust 2023. 2023. DEKK Institute. 2023. <https://www.dekk.institute/wp-content/uploads/2023/09/dekk-report-trendy-nedovery-2023-web.pdf>.

55 "Concept of Strategic Communication of the Slovak Republic Bratislava 2023." n.d. Accessed August 28, 2024. https://www.vlada.gov.sk/share/uvsr/koncepcia_strategickej%20komunikacie_sr.pdf?csrt=12155556465759032409.

56 "SECURITY STRATEGY OF THE SLOVAK REPUBLIC". 2021. https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf. https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.

57 "DEFENCE STRATEGY OF THE SLOVAK REPUBLIC". 2021. https://www.mosr.sk/data/files/4286_obranna-strategia-sr-2021.pdf.

58 "AKČNÝ PLÁN KOORDINÁCIE BOJA PROTI HYBRIDNÝM HROZBÁM." 2022. <https://www.hybridnehrozby.sk/wp-content/uploads/2023/09/APHH-2022.pdf>.

59 "Národný projekt zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy – základné informácie - HybridneHrozby.sk." 2023. HybridneHrozby.sk. December 12, 2023. <https://www.hybridnehrozby.sk/narodny-projekt/>.

60 "The Government Adopted the Concept of Strategic Communication of the Slovak Republic | Government Office of the Slovak Republic." n.d. [www.vlada.gov.sk. https://www.vlada.gov.sk/vlada-prijala-koncepciu-strategickej-komunikacie-slovenskej-republiky/](https://www.vlada.gov.sk/vlada-prijala-koncepciu-strategickej-komunikacie-slovenskej-republiky/).

After the 2023 parliamentary elections, a new updated concept of strategic communication was adopted, allegedly because of the need to prevent "foreign and domestic NGOs in particular from arbitrarily implementing the state's strategic communication without taking responsibility for its impacts on Slovak society."⁶¹ The new concept aims in particular to "strengthen public trust in government decisions, increase transparency and promote citizen participation in public affairs."⁶²

Timeline:

- 2017** • Establishment of the Strategic Communication Department at the Ministry of Foreign Affairs of the Slovak Republic.
- 2018** • Mention of Strategic Communication in the Concept for Combating Hybrid Threats.
- 2019** • Slovakia became a member of the NATO Centre of Excellence for STRATCOM.
- 2021** • SR Security Strategy commits to support strategic communication.
- 2021** • The Slovak Defense Strategy states that the Government of the Slovak Republic will develop strategic communication.
- 2022** • Adoption of the Action Plan for the Coordination of Combating Hybrid Threats of the Slovak Republic, which defined the tasks in the field of strategic communication.
- 2022** • Beginning of the implementation of the national project - establishment of specialized units at the Office of the Government of the SR, the MoD and the MoI of the SR, strengthening of the unit at the MFEA of the SR.
- 2023** • Strategic Communication Concept of the SR adopted.
- 2024** • Updated Strategic Communication Concept of the SR adopted.

Reflection of the case in the information space:

The term "strategic communication" began to be used more prominently in the information space in the second half of 2021 and then in 2022, which corresponds with the establishment of specialized departments at the Office of the Government of the Slovak Republic and other relevant ministries. A significant increase in the incidence can be seen in 2023 before and after the adoption of the Concept of Strategic Communication of the Slovak Republic and subsequently after the parliamentary elections in 2023. Strategic communication was accompanied by a **gradually worsening negative sentiment** from the end of 2022, **which** corresponds with the negative perception and portrayal of strategic communication in the information space as propaganda, in which NGOs allegedly participated.

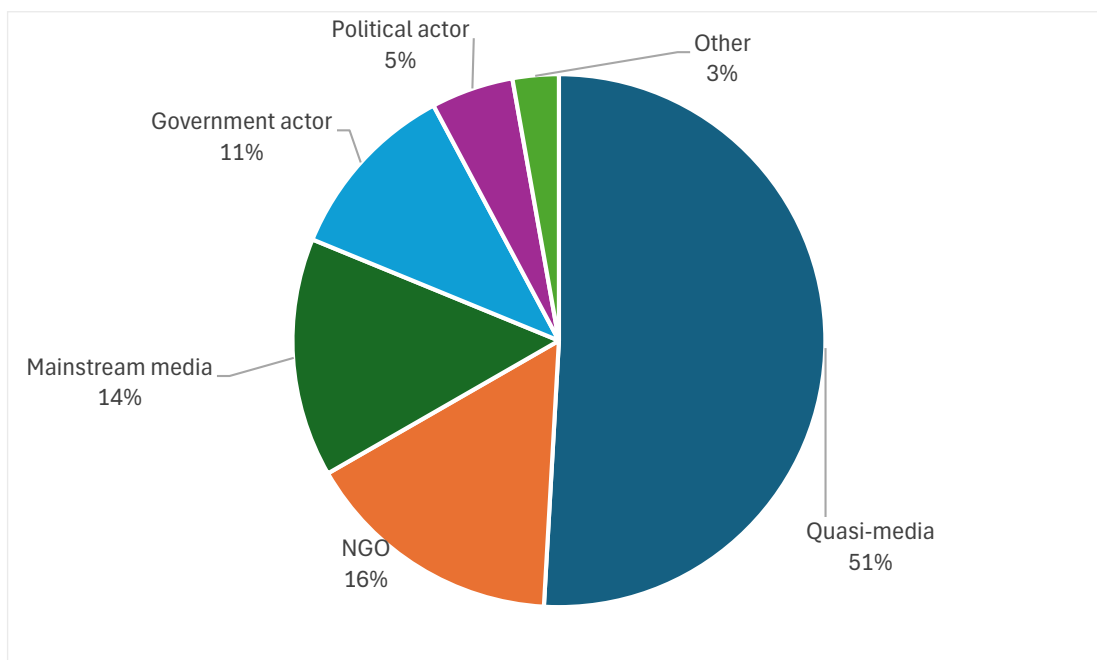
61 "PREPUBLICATION REPORT." n.d. Accessed August 28, 2024. <https://rokovania.gov.sk/download.dat?id=5AAB64AFB46F4240B1DC1DA7C4A1C5EB-2DB70C4D5D383ACF396140E07D3A0EB7>.

62 "Material detail | Portal OV." 2024. Rokovania.gov.sk. 2024. <https://rokovania.gov.sk/RVL/Material/29346/1>.



Evolution of the number of posts mentioning the term "strategic communication". (Data retrieved from Juno in May 2024.)

From the actor's perspective, strategic communication was clearly the most mentioned in the quasi-media. In the references to strategic communication in the mainstream media, factual information about the issue prevailed in Slovakia, but to a much lesser extent than in the quasi-media. A significant part of the contributions on the topic was produced by civil society, mainly through civic associations dedicated to awareness and education in the field of information environment security. The state administration communicated the topic of strategic communication to a lesser extent, with the main communicators of this topic being the Office of the Government of the Slovak Republic, the Ministry of the Interior of the Slovak Republic, the Ministry of Foreign Affairs of the Slovak Republic, the Ministry of Defense of the Slovak Republic and other relevant ministries. Political actors, in most cases from the then government coalition, mentioned strategic communication minimally.



Distribution of the number of mentions of the term "strategic communication" by actors. (Data retrieved from Juno in May 2024.)

Rating:

This is an example of good practice, as there has been a significant increase in the capacity of the state administration during the lifetime of the national project from 2022-2023. **At the same time, there has been a substantial improvement in capacity in the field**, in particular through the adoption of a key concept paper and the establishment of a coordination mechanism in the state administration.

However, the creation of the units in the SR was in most cases financed by European funds, which caused problems with long-term sustainability after the end of the project. After the parliamentary elections in 2023, there was a reduction in capacity and a change in the understanding of strategic communication.

The competency framework did not sufficiently define the coordinating body, so cooperation was often more informal and not all ministries were involved in coordination. In the ministries that did not primarily deal with strategic communication, this topic was not prioritized. The systemic tools, standardization and binding guidelines needed to ensure coordinated strategic communication were lacking.

The politicization and misunderstanding of strategic communication by politicians has led to its abuse for political purposes and self-presentation. Politicians and ministry managers were often unaware of the existence and importance of strategic communication. Moreover, there was a lack of continuity in the field of strategic communication after the elections, with measures taken by previous governments often being reversed or fundamentally changed.

CASE STUDY 2: Lack of Strategic Communication of the Slovak Government on Values Related to Homeland Defense



Description: Illustration from the website Bádateľ, (Explorer) which spread disinformation about the mobilization.

Date:

Beginning of 2023

Summary:

At the beginning of 2023, disinformation began to spread in Slovakia about the alleged mandatory mobilization of men for deployment to the conflict in Ukraine. At the same time with a direct appeal to send a document on refusal to serve in the Slovak Armed Forces to the relevant authorities. Such appeals were periodically made to a small extent in January each year. This was also related to the fact that, in accordance with the legislation in force in Slovakia, it is possible to submit a request for denial of extraordinary service only in the month of January. But in January 2023, the massive spread of disinformation about compulsory mobilization caused widespread anxiety among Slovak citizens, leading to more than 40 000 men sending documents to the state authorities to refuse extraordinary service in the armed forces, culminating in the organization of so-called 'Marches for Peace' with pro-Russian sentiment. These phenomena were widely supported by Russian propaganda and there is a presumption that their impact could have been reduced by timely and effective strategic communication. In this case, to values related to the defense of the homeland.

The course of the case:

The massive unprecedented Russian aggression in Slovakia's immediate neighborhood has created the right conditions for deliberately spreading fear in society. At the same time, it also led to a reduction in the ability of a large part of the Slovak population to rationally assess the importance of military assistance to Ukraine. This was exploited by domestic disinformation actors and quasi-media, supported by Russian propaganda, spreading the narrative that military aid to a defending Ukraine would lead to a confrontation between NATO countries and Russia.

At the beginning of January 2023, a Facebook page called *Bádateľ* (Explorer) published an expressive and fear-inducing post about an alleged planned mobilization in the Slovak Republic, which was to take place in September 2023. The author of the post presented a document on the planning of a complex exercise as evidence. In the post, he also published a link to a model notice of denial of service in the Slovak Armed Forces.⁶³

The SR Police immediately caught the false report and responded by clarifying that it was a periodic exercise and only concerned administrative activities in relation to civilians. However, due to its relatively large reach on social media, the SR Police was unable to counter the massive sharing of disinformation by quasi-media and individual disinformation actors. Citizens of Slovakia were also directly encouraged to send notices of refusal to serve in the Slovak Armed Forces. Other branches of the state administration made minimal comments on the spread of disinformation; their response did not meet the criteria of strategic communication.

The massive dissemination of disinformation about the mobilization caused a significant number of Slovak citizens to succumb to fears that they would be mobilized for war with the Russian Federation. In mid-February 2023, the Slovak Ministry of Defense reported that more than 40,000 Slovak citizens had refused to serve in the Slovak Armed Forces.⁶⁴

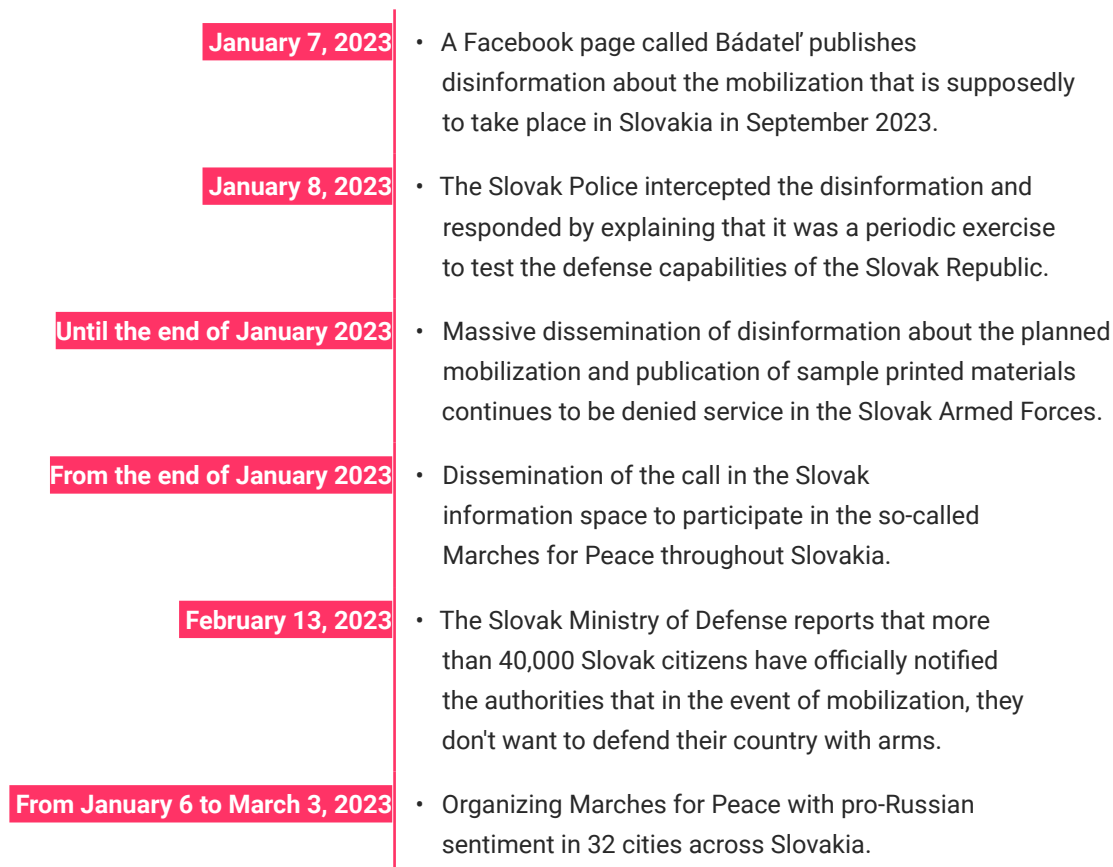
63 "Facebook." 2022. Facebook.com. 2022. <https://www.facebook.com/100071425145281/posts/3272676529544639/>.

64 Bista, Samuel. 2023. "Vyhlásenie o odopretí mimoriadnej služby." INFOSECURITY.SK - Blog About Information Security. February 19, 2023. <https://infosecurity.sk/domace/vyhlasenie-o-odopreti-vykonu-mimoriadnej-sluzby-v-case-mobilizacie-podpisalo-viac-nez-40-tisic-slovakov-stali-sa-obetami-dezinformacnej-kampane/>.

At the same time, since the end of January 2023, calls for participation in the so-called Marches for Peace have been disseminated in the Slovak information space with the proclaimed aim of expressing the wish of the Slovak population not to send military aid to Ukraine and thus avoid future conflict in Europe. In the course of one month, these marches were organized in a total of 32 cities across Slovakia. In total, tens of thousands of people took part in the marches, and the meetings were accompanied by speeches with pro-Russian sentiment.⁶⁵

Timeline:

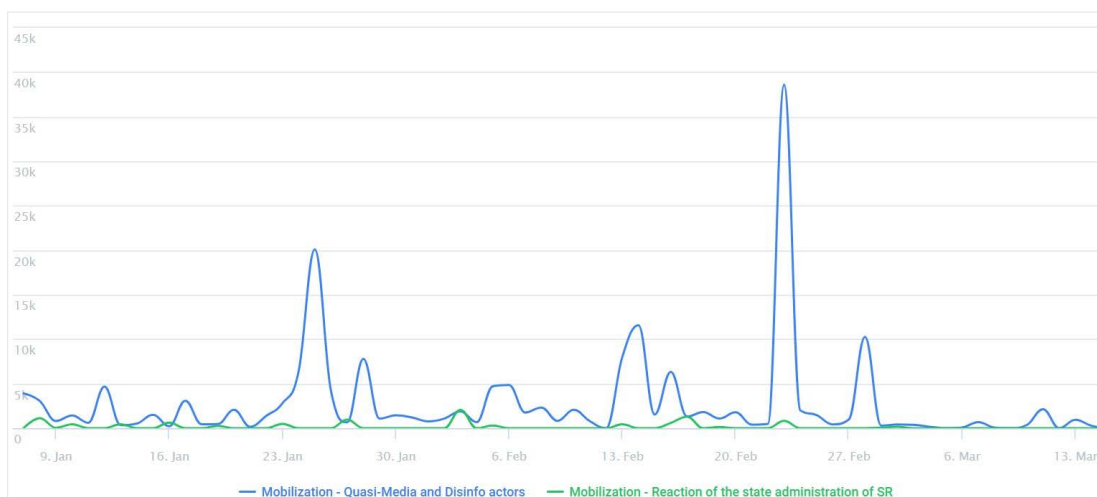
Before 2023: The number of applications for denial of service in the Armed Forces of the Slovak Republic does not exceed 2000 each year.



Reflection of the case in the information space:

The dissemination of the misleading report on the mobilization of Slovak men has seen many more interactions than the response of the Slovak administration. This was also due to the weak engagement of the state on this issue. In the two-month period since the disinformation started spreading, the ratio of posts was 1165:35 in favor of the quasi-media and disinformation actors. As a result, news of the alleged mobilization also received more than 5.1 million hits in Slovakia. The state administration's response was only less than 47,000.

65 Global24 Ltd. 2023. "Daj tú handru dole a neprovokuj ma! Kričali v Nitre na chlapca s ukrajinskou vlajkou." Nitra24.Sk. Dnes24.sk. February 27, 2023. <https://nitra.dnes24.sk/daj-tu-handru-dole-a-neprovokuj-ma-kricali-v-nitre-na-chlapca-s-ukrajinskou-vlajkou-430162>.



Interactions of the posts the spread of disinformation about mobilization and the response of the Slovak state administration

The data show that the disinformation about the mobilization of Slovak men for the war against Russia was spread not only by the quasi-media, but also by individual disinformation actors.

	Name	Content	Interactions	Reactions	Views
	CZ24.NEWS (cz24news)	45	4789	4789	150.2k
	KSB Správy (ksbspravy)	32	433	433	57.05k
	Dole králičou norou 17/17+ (1189116057)	30	59	59	98.77k
	Blog investigatívnej žurnalistiky (investigativnyblogSK)	28	2126	2126	70.23k
	Co neMÁTE vědět (coNemateVedet)	26	395	395	79k
	Miro Del (Miro_Del)	24	3230	3230	67.33k
	ZEM&VEK (zemavek)	24	6776	6776	164k

The sources that published the most posts about the alleged mobilization. (Data retrieved from Juno in May 2024.)

Rating:

This is a case of bad practice, where the lack of strategic communication on the topic of patriotism and defense of the homeland has significantly helped spread disinformation about the preparation of the Slovak population to be sent to fight in Ukraine. **This was manifested by bringing the issue into the real world**, by filing more than 40 000 notices of refusal to serve in the Slovak Armed Forces and by the massive organization of pro-Russian peace marches. Even before 2023, Slovakia was not sufficiently building citizens' awareness about the defense of the homeland and the benefits of NATO membership. Education of Slovak citizens in patriotism was and is partly carried out only by the Slovak Armed Forces, including through cooperation with the non-governmental sector.

The spread of disinformation about the mobilization took place at a time when a unit responsible for coordinating strategic communication was being created at the Government Office of the Slovak Republic. Also, the main conceptual material that would unify communication in the state

administration was still being prepared. Mistrust prevailed between institutions in this area and coordination was minimal.

The Slovak Police in particular responded to the published disinformation about the mobilization. Although the disinformation thematically fell under the Ministry of Defense of the Slovak Republic and this department already had an executive unit dealing with hybrid threats and strategic communication, the first independent reactions were published only in early February 2023. It was also problematic that the Minister of Defense communicated mainly through his political profile on social media.

Some political actors further developed the idea of preparing Slovak citizens for fighting in Ukraine and sought to gain political advantage by cynically scaring Slovak citizens.⁶⁶ **Slovak mainstream media took information from the state administration** and responsibly reported on the negative consequences of spreading disinformation in several articles.

After the September 2023 general election, there have been no positive changes in the strategic communications on patriotism, defense of the homeland and democratic values, or NATO membership. The current staffing of the unit of the Office of the Government of the Slovak Republic is responsible for coordinating strategic communication is considered insufficiently prepared to cover this issue.

CASE STUDY 3: Ministry of the Interior's Wall Campaign



Source: Ministry of Interior

Date:

Summer 2023 – present

66 Matúš Demiger. 2023. "Politici Smeru na tlačovej konferencii dali znovu najavo, že témou predvolebnej kampane bude strašenie mobilizáciou..." Denník N. Denník N. February 8, 2023. <https://dennikn.sk/minuta/3230048/>.

Summary:

In the summer of 2023, the Home Office launched an awareness campaign of up to 40 million people, which included presentations on municipal notice boards, posters on trains and other forms of offline campaigning. These "bulletin boards" explained various topics, including energy insecurity following Russia's invasion of Ukraine. The campaign was both praised and criticized in the public sphere. It was an original approach to communicating with citizens who, for example, do not normally use the internet and social networks. However, this makes the impact of the campaign difficult to measure and it is important that state institutions are able to evaluate the effectiveness of such activities.

The course of the case:

The initiative for information boards was born out of a request from the Ministry of the Interior to create a communication tool for citizens who do not use the Internet and live in an information vacuum, which represents about 30% of the population. Based on an internal sociological survey of the Ministry of the Interior, which confirmed the existence of this part of the population, the idea of bulletin boards was born. The whole process from idea to implementation took three quarters of a year, including a media tender and agreements with other actors, such as the presidents of coalition parties and associations of municipalities, to support the importance of this communication and not to hinder the implementation of the bulletin boards.

The content of the bulletin boards was selected on the basis of criteria aimed at the target group, which consists mainly of the lower middle class and the elderly, who are not interested in politics at all or only occasionally. Places for the placement of the bulletin boards were selected on the basis of a socio-demographic survey and were focused on local public transport, trains and public spaces where the target group most frequently moves.

After a test run in the Liberec region in the winter of 2022/2023, the campaign was expanded nationwide in the spring of 2023. The campaign included bulletin boards, banners and frames on trains, which proved to be the most effective way to reach the target group, as this form of communication was available in the area where the target group moves most frequently, while allowing for longer-term visual contact with the content. **The total cost of the campaign was CZK 20 million. A total of CZK 42 million was allocated, but it was not necessary to use the entire amount.**

The campaign is perceived as part of institutional communication and has no party political connotations. The campaign contains the logo of the state, but not the face of any politician, which underlines its neutral character.

The impact of the campaign is measured by surveys that gauge public awareness of the issues. Regular non-public surveys available to the Home Office show that the posters were well received in public spaces, leading to adjustments to the graphics based on feedback. The campaign continues to develop, for example, it now targets Ukrainians working in the Czech Republic. Experts assess the campaign positively and believe that with bigger budgets it could have an even bigger impact.

Timeline:

- After February 2022**
 - The Ministry of the Interior calls for the creation of an information channel for people who do not use the internet.
- 2022**
 - Sociological research by STEM shows that it makes sense to target around 30% of the population.
- 2022**
 - Content selection and criteria aimed at the lower middle class and older people watching specific TV programs.
- 2022**
 - Negotiations with the government, associations of towns and municipalities to support the project.
- Winter 2022/2023**
 - Test run of the campaign in the Liberec Region and agreement with the Governor on support.
- Spring 2023**
 - Expansion of the campaign across the country.
- 2023**
 - Placement of information materials in the form of bulletin boards, banners and frames on trains based on a socio-demographic survey.
- 2023**
 - Ongoing surveys monitor awareness of posters in public space and adjust the graphics according to feedback.
- 2023**
 - Continuation of the campaign with emphasis on information about Ukrainians working in the Czech Republic.
- 2023**
 - The total cost of the project is CZK 20 million, with the possibility of allocating up to CZK 42 million. An extension is being considered topics and increase the budget for greater impact.

Reflection of the case in the information space:

As the campaign itself was offline, it had very minimal impact online, with only a few dozen posts (29 posts from 25 different accounts). Given the low number of contributions, it is more interesting to look at specific individual accounts and the extent of their individual contributions. The top five posts with the most interactions came from disinformation sources - Aby bylo jasno (To be clear) and My občané 2 (We, the citizens 2) and politicians (Kateřina Konečná and Tomio Okamura). Only the sixth place was occupied by posts from the X-account of the Minister of the Interior Vít Rakušan (968 interactions). Although the total reach of his contributions was almost the same as that of Tomio Okamura (1121), it should be noted that while in the case of the Minister of the Interior the total was the sum of three contributions, in the case of Okamura it was only one. In comparison, the account with the highest reach (16,690 interactions) involved two posts from the disinformation Facebook page Aby bylo jasno.



Comparison of the engagement of individual accounts informing about the bulletin board campaign.

Rating:

The state's response was well targeted at a specific segment of the population (approximately 30% of the population) that does not use the internet and is often out of reach of mainstream information channels. The inclusion of opinion polling data in the planning of this campaign was crucial to effectively communicate with the target group, which includes the elderly and lower middle class. **The communication achieved wide coverage through the strategic placement of bulletin boards and banners on trains and local public transport, which helped** the public to be better informed about important issues. This may have led to an increase in overall awareness among the target group. After a successful test run in the Liberec region, the campaign was extended throughout the country. Ongoing surveys and adjustments to the graphics based on feedback increased the relevance and impact of the campaign. The total cost of the campaign amounted to CZK 20 million, with CZK 42 million allocated, indicating efficient management. The campaign featured the state logo but not the faces of politicians, underlining its neutral character and independence from political positions. The neutral presentation of the campaign without political faces probably increased its credibility among the public. People perceived the information as objective and independent of political interests. The tailoring of the campaign based on feedback and effective communication with the target group probably led to positive public acceptance of the campaign, which is crucial for the success of any information initiative.

The campaign had limited impact measurement, which made it difficult to accurately assess its impact on public opinion and specific changes in the behavior of the target group. **Although poster awareness/recognition surveys were carried out, there was insufficient clarity to measure the actual impact the campaign had on changing public opinion or target group behavior.** This limitation makes it difficult to assess the effectiveness of the campaign and its impact. The failure to use certain communication media, such as the planned use of town hall newspapers, limited the larger impact of the communication. With a larger budget, the campaign could have had a more substantial impact. Production constraints, such as the inability to use town hall sheets, limited the communication options. There is potential to expand the campaign and improve impact measurement, which would provide more accurate data on the campaign's effectiveness.

The communication campaign was a great tool to reach a specific sector of the public. However, this newly created channel remained isolated within this campaign planned and implemented by the Home Office. The use of this tool could have been maximized if the campaign had been cross-departmental and coordinated by either the Home Office or the Cabinet Office. This could have led to a broadening of the topics covered by the 'bulletin boards'.

CASE STUDY 4: Strategic Communication Associated with the Czech Munitions Initiative for Ukraine



Source: ČTK

Date:

2024

Progress of the case:

In the context of Ukraine's growing demand for artillery ammunition, the Czech government launched an inter-national campaign to raise funds to enable the purchase of 800,000 rounds of ammunition. This effort, led by Prime Minister Petr Fiala and President Petr Pavel, has received support from a number of EU and NATO countries. More than EUR 1.5 billion has been raised. The procurement process involves sourcing ammunition from non-European suppliers, which has helped to offset production constraints within the European Union.⁶⁷

The Czech government has been active in communicating the urgency of the situation and asking for international support. There was a visible effort to balance the transparency of the initiative with operational security and efforts to ensure that sensitive details were not leaked. President Pavel and Prime Minister Fiala stressed the importance of continued support for Ukraine and coordinated closely with allied countries.

Prime Minister Petr Fiala and President Petr Pavel played a key role in securing international support through meetings with NATO and EU leaders. These meetings often coincided with major events such as the Munich Security Conference and NATO summits to maximize visibility and impact.

The Czech government has regularly issued public statements on the progress and success of the initiative. These declarations were strategically timed to coincide with important milestones such

67 "Nejdůležitější česká mise v novodobých dějinách." 2024. Respekt.
<https://www.respekt.cz/tydenik/2024/16/nejdulezitejsi-ceska-mise-v-novodobych-dejinach>.

as securing the financial the awarding or signing of public procurement contracts, thus maintaining the momentum of information disclosure and public interest.⁶⁸

The main focus of the Czech government's communication was on balancing transparency and security of the initiative.⁶⁹ Regular updates were provided on progress, funding sources and procurement logistics. This can be seen as key in building trust not only with the public but also with allies and ensuring continued support from international partners.

The Czech initiative has been repeatedly praised and thanks to it the Czech Republic has created an image of a country that can initiate joint and effective solutions within the EU and NATO. In doing so, the Czech Republic has set a precedent for international cooperation in the field of military support and highlighted the need for robust supply chain management in defense logistics.

Timeline:

- February 2024** • Prime Minister Fiala announced the initiative at the European Council and it was subsequently published by Politico. The initiative was then spontaneously presented publicly by President Paul at the Munich Conference.
- March 2024** • Securing seed funding with significant contributions from Norway, Germany and other countries.
- April 2024** • Signing of contracts for the first batch of 180,000 rounds.
- May 2024** • Coordination with multiple countries to streamline procurement and supply logistics.
- June 2024** • First ammunition shipments expected to arrive in Ukraine.

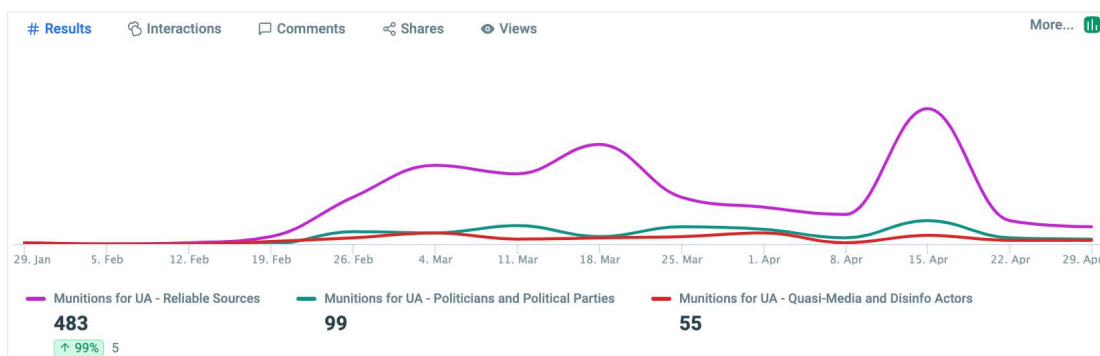
Reflection of the case in the information space:

In this case, the Czech information space, both in terms of the number of contributions and the interactions associated with them, was completely dominated by the mainstream media and the individual government politicians who led and supported the initiative. In particular, Prime Minister Petr Fiala and Defense Minister Jana Černošková. Among the actors with the biggest impact was again the Instagram account of the President of the Republic, who announced the initiative and actively communicated it. Unsurprisingly, his account had the largest reach, even though there were only two posts on the topic. The same success could be observed in the case of reporting on refugees from Ukraine.

Although communication about the Initiative was not necessarily always well thought out and specifically planned, it was quick and state and government communication channels were able to dominate the space. Given that the quasi-media and disinformation actors in this case exhibit a completely marginal reach, we can thus observe that they were not given sufficient space for an intense counter-pressure.

68 "Do české muniční iniciativy přispělo patnáct zemí přes 39 miliard korun, řekl Fiala." Fiala said. 2024. CT 24. <https://ct24.ceskatelevize.cz/clanek/domaci/na-schuzku-k-bezpecnostni-spolupraci-dorazi-do-prahy-i-ukrajinsky-premier-smyhal-349667>.

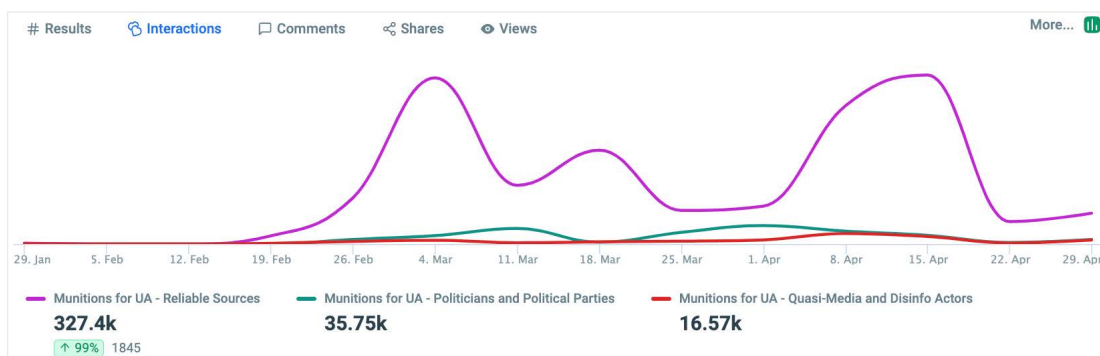
69 "The Ministry of Defense emphasizes the transparency of the Czech munitions initiative." 2024. Ministry of Defense of the Czech Republic. <https://mocr.army.cz/information-service/reporting/ministry-of-defence-places-emphasis-on-transparency-ceske-muni-iniativy-250574/>.



Comparison of the number of posts within the monitored groups reporting on the Czech Munitions Initiative.

Sources		Content		Content		Content	
Munitions for UA - Reliable Sources		Munitions for UA - Politicians and Political Parties		Munitions for UA - Quasi-Media and Disinfo Actors			
Name	Content	Name	Content	Name	Content		
Petr Pavel	2	Tomio Okamura - SPD	4	Jindřich Rajchl	1		
ČT24	44	Andrej Babiš	1	neCT24	7		
ČT24	28	ODS - Občanská...	21	Roman Kirsch	4		
dnesnaukrajine.cz	13	Zuzana Majerová	4	CZ24.NEWS	10		
Petr Fiala	9	Marek Ženíšek	5	InfoVojna	2		
Petr Pavel	3	ODS	18	Selský Rozum	15		

Comparison of the number of posts by individual accounts within the monitored groups reporting on the Czech Munitions Initiative.



Comparison of interactions of monitored groups reporting on the Czech Munitions Initiative.

Sources			Interactions		
Munitions for UA - Reliable Sources			Munitions for UA - Politicians and Political Parties		
Name		Interactions	Name		Interactions
Petr Pavel		50.17k	Tomio Okamura - SPD		8607
ČT24		37.75k	Andrej Babiš		3838
ČT24		28.54k	ODS - Občanská...		3483
dnesnaukrajine.cz		17.71k	Zuzana Majerová		2674
Petr Fiala		17.7k	Marek Ženíšek		2282
Petr Pavel		17.68k	ODS		1937
Munitions for UA - Quasi-Media and Disinfo Actors					
Name		Interactions			
Jindřich Rajchl		4258			
neCT24		2930			
Roman Kirsch		2633			
CZ24.NEWS		1919			
InfoVojna		1551			
Selský Rozum		1055			

Comparison of interactions of individual accounts within the monitored groups reporting on the Czech Munitions Initiative.

Rating:

In 2024, the Czech government launched a major international initiative to support Ukraine by raising funds for the purchase of artillery ammunition. This campaign, led by Prime Minister Petr Fiala and President Petr Pavel, was a significant step in strategic communication that had its strengths and weaknesses.

The Czech government successfully gained the **support of a number of EU and NATO countries**, which led to the collection of more than EUR 1.5 billion. Prime Minister Fiala and President Pavel played a key role in this process, and through personal meetings with the leaders of these countries, they were able to secure the necessary support. These meetings were strategically timed to maximize the visibility and impact of the initiative, for example during the Munich Security Conference and NATO summits.

The government regularly updated the public on the progress of the initiative through public statements timed to coincide with significant milestones. This approach helped maintain momentum and public interest, which is key to building trust not only among the public but also among allies.

The government has tried to balance the need for transparency with operational security so that sensitive details are not leaked to help the Russian Federation. This approach was important in securing the support and trust of international partners, which was critical to the success of the initiative.

Thanks to this initiative, the Czech Republic has created an **image of a country capable of initiating and managing effective inter-national cooperation** within the EU and NATO. This step highlighted the need for robust supply chain management in defense logistics and set a precedent for future international cooperation.

While communication was fast and efficient, some key announcements were not planned in advance, which could have led to a lack of coordination and potential misunderstandings. An example of this was President Paul's public announcement of the initiative at the Munich Conference, which was a spontaneous response to the Danish Prime Minister's speech and was not originally planned. Chaotic communication also took place at times regarding the resources obtained.⁷⁰

70 "Ministerstvo obrany klade důraz na transparentnost české muniční iniciativy." 2024. Deník N. <https://denikn.cz/1480141/cesko-rozjizdi-novou-municni-iniciativu-jak-bude-fungovat/?ref=tit>.

The strategic communication of the Czech government during the initiative to purchase ammunition for Ukraine had many positive aspects that contributed to its success. The key was gaining international support, effective communication and transparency, which helped build trust and maintain momentum. However, there were also weaknesses, particularly in the area of planning and coordination of communication, which could be improved in the future. Overall, this initiative has significantly strengthened the international image of the Czech Republic and demonstrated its ability to manage international cooperation effectively.

Summary:

The experiences of the Czech Republic and Slovakia in the field of strategic communication show several important similarities. Both countries have had to deal with changes in the security environment following the annexation of Crimea by the Russian Federation in 2014, which increased the risk of disinformation campaigns aimed at destabilizing society and undermining trust in democratic institutions and membership in international organizations. In response to these threats, Slovakia has decided to strengthen its strategic communication as a key tool to protect society.

In the Czech Republic, although government officials have long supported the importance of strategic communication rhetorically (but especially after Russia's full-scale invasion of Ukraine), in practice there is no concept or strategy in this area, and only partial departments in the power ministries are dedicated to communication. In both countries, senior government officials are often involved in strategic communication. Prime ministers, presidents and other senior politicians play a key role and can actively support initiatives to increase societal resilience.

One of the main differences between the countries is the way of financing and sustainability of strategic communication projects. Slovakia used to use mainly European funds to finance its activities, which led to problems with long-term sustainability after the end of these projects. In contrast, the Czech Republic finances campaigns from the state budget.

On the other hand, a common aspect remains the lack of coordination and involvement of several ministries in truly strategic communication campaigns. Coordination between institutions is often informal or non-existent and not all ministries are involved in the process.

RECOMMENDATIONS FOR CZECH POLITICAL AND STATE INSTITUTIONS

The following recommendations are divided into several areas:

1. **General recommendations** Valid for the area of hybrid threats, disinformation and strategic communication and generally aimed at strengthening the Czech state's resilience against foreign interference.
2. **Recommendations on the topic of hybrid threats and disinformation** This category has been combined for the purposes of the report, as disinformation falls under hybrid threats and most of the proposed solutions do not exclusively address disinformation.
3. **Recommendations on the topic of strategic communication.**

In each area, the recommendations are divided between timeframes:

1. **Short-term framework** - Measures that should be possible to implement within about 12 months.
2. **Long-term framework** - Measures likely to take more than 12 months to implement.

The measures are then prioritized within each timeframe.

GENERAL RECOMMENDATIONS

Short-term framework

Better implementation of strategies and oversight

The President of the Republic should establish an independent commission to oversee the implementation of the state strategies and action plans on hybrid and Influence, which have been adopted by the government. The Commission should be composed of experts not only from the government, but also from the academic and non-governmental sector. The role of this commission should be to continuously monitor the implementation of the single strategies and their action plans, evaluate progress, monitor the effectiveness of financial resources spent on implementation, and subsequently prepare regular reports on the status of implementation of these strategies. These reports would be submitted to the President of the Czech Republic, the Government of the Czech Republic, constitutional officials, and the relevant committees and commissions of the Parliament of the Czech Republic.

High priority

Creating Consensus regarding definitions basic concepts	There is a need to create inter-ministerial consensus on the understanding of the basic concepts of and terms, in particular: 'hybrid threat', 'disinformation', 'misinformation "malinformation", "influence", or others. In most cases these definitions already exist, within official European Union documents and NATO, or in specific ministries (in particular the Ministry of the Interior and the Ministry of Defense. If necessary, working groups composed of experts in law, security and information technology, who submitted it proposes selected definitions on which institutions across ministries can agree.	Medium Priority
--	---	-----------------

Long-term framework

Strengthening cooperation with the academic and non-governmental sectors	The Ministry of Education, the Ministry of the Interior and the Ministry of Defense, and possibly other ministries, should systematically support the academic sector and non-governmental organizations in research and practical (e.g. educational or awareness-raising) projects that substitute the role of the state in the field of hybrid threats, disinformation or strategic communication. Support should be provided through grant schemes, scholarships or the establishment of partnerships and the implementation of joint projects. Systematic support would not only develop the activities of the non-governmental and academic sectors but would also help to expand and develop know-how between the state and non-state sectors.	High priority
Definition of competences, responsibilities and boundaries	The Government of the Czech Republic should revise the Competence Act (69/1993 Coll.) in order to clearly define the powers and responsibilities of individual ministries and functions in the field of hybrid threats and strategic communication. In this way, it would not only be possible to provide these institutions with a specific and stable mandate, but also to anchor in law the extent to which political leaders can intervene in the strategic communication of the state.	High priority
Increasing public awareness and resilience	The Government Office, in cooperation with the relevant ministries, should continuously coordinate information and awareness-raising campaigns and sub-activities with the intention of strengthening the information resilience of the public and building mutual trust between the state and citizens and citizen resilience to information and hybrid threats in a transparent manner through appropriate communication channels.	High priority
Building media literacy	The Ministry of Education should include the issue of hybrid threats and in-formation literacy in the curriculum at all levels of education.	Medium Priority

HYBRID THREATS AND DISINFORMATION

Short-term framework

More consistent coordination and information exchange	The National Security Council already has an Expert Working Group on Hybrid Threats, whose members include all relevant institutions involved in countering hybrid threats. However, it meets minimally and does not carry out real coordination activities. The Government of the Czech Republic should require the active use of this working group for regular meetings, exchange of information and monitoring of the current status and developments in the field of hybrid threats, and actively use the outputs of this working group for further tasking and coordination of activities outside the working group. In addition to physical meetings, there should be a secure online platform for instant information exchange within the Expert Working Group.	High priority
Methodological guidelines and systematic training of the public administration	The Ministry of Defense, in cooperation with the Ministry of the Interior and the NÚKIB should develop methodological guidelines for identifying and responding to hybrid threats. This methodology should be accompanied by training programs and e-learning for government employees across departments, including those not primarily involved in hybrid threats. All civil servants should receive e-learning and, where appropriate, physical training and have the methodology guidance available.	High priority
Increase in financial and staff capacity to implement the legislation and strategies	The Ministry of Finance should increase the budget for law enforcement agencies, institutions involved in investment and countering hybrid threats and disinformation. It is necessary to increase not only the staffing in order to fulfil the tasks assigned by the state strategies and action plans and to effectively implement the adopted legislation (especially in the area of sanctions), but also the technical background and equipment for these institutions in order to make their work truly effective (especially analytical and monitoring tools focused on financial flows, information space or sentiment analysis).	High priority
Edit by and specifications of the Criminal Code	The Government and Parliament of the Czech Republic should submit an amendment to the Criminal Code that would include the facts of cooperation with a foreign power and specify the facts of espionage so that it would be possible to punish the export of sensitive information (not only classified information). The amendment should also allow the use of intelligence information from the Security Information Service as formal evidence in criminal proceedings.	High priority
Adoption of the Digital Economy Act	The Parliament of the Czech Republic should urgently adopt the Digital Economy Act, which will enable the implementation of the Digital Services Act (a European Union regulation), which the Czech Republic is currently not complying with and for which it faces sanctions. This Act will provide new rights for Czech Internet users in relation to online platforms and social networks and will strengthen the possibilities of defense against harmful and illegal content.	High priority

Long-term framework

More effective Implementation of the sanctions and investigation of their violations	The Government of the Czech Republic, the Ministry of Finance and the Ministry of Justice should make the registration of the real owners of companies and real estate more effective, so that it is possible to obtain complete and up-to-date data on owners. In addition, there is a need to strengthen the control mechanisms for financial transactions and tighten sanctions for non-compliance with the transparency rules. Limit the laundering of the proceeds of crime can be legislated against by the Anti-Money Laundering Act through so-called flow-through accounts. Lastly, the capacity of the Financial Analytical Office (FAO) should be strengthened to uncover ownership structures and more effectively implement sanctions.	High priority
Communication and media coverage of the hybrid threats	The Government Office, in cooperation with the relevant ministries, should regularly include in its strategic communication awareness-raising on hybrid threats, regularly inform the public about successfully detected hybrid operations and their consequences and proactively communicate with partners abroad.	Medium Priority
Legal regulation of website blocking	The Ministry of Justice, in cooperation with the Ministry of the Interior and the NÚKIB, should draw up a law that clearly defines the conditions and procedures for blocking websites spreading disinformation that threatens security of the state. The law should ensure transparency in the website blocking process, clearly defined and predictable conditions, safeguards to limit the measure, protection of freedom of speech, and the availability of judicial review.	Low Priority

STRATEGIC COMMUNICATION

Short-term framework

Creating conceptual document for strategic communication	The Government Office should coordinate the creation of a conceptual document for the strategic communication. A working group should be set up under the Government Office, composed of experts in security and communication, along with representatives from public administration, civil society, and academia, should consult the document. The resulting strategy should clearly define the purpose of strategic communication, its goals, responsibilities of individual ministries and institutions in its implementation, coordination mechanisms and procedures, as well as the boundaries between strategic and political communication. The concept should be public and should be actively introduced within the civil service and to those employees who are not primarily involved in strategic communication on a daily basis. The conception should involve the gradual building of communication channels that would be mutually complementary and coordinated. A key role in this process should be played by the government's newly created Strategic Communications Coordinator whose mandate should be enshrined in law.	High priority
---	--	---------------



Coordination and exchange of information between ministries	The Department of Strategic Communication at the Office of the Government should play the role of coordinator for strategic communication, which will regularly receive, and ensure the exchange of information from the various ministries. Beyond the regular coordination meetings of relevant actors, there should also be secure online platform for instant communication between the Government Office, the resorts, but also regional institutions and other relevant communication actors outside the center. On a regular basis, the Government Office should provide updates on the status and development of strategic communication to the Prime Minister and the Government	High priority
Methodological guidelines for strategic and crisis communication	Strategic Communication Department at the Government Office in cooperation with the Ministry of the Interior should develop standardized methodological guidelines for individual ministries for monitoring information threats and the procedure for crisis communication. This methodology should be made available to staff of all ministries, and regional and local governments, and staff involved in any form of communication should be trained on this methodology.	High priority
Formal cooperation with NGOs, influencers and private sector	Each ministry should compile an inventory of relevant NGOs and influencers who are relevant to the departmental agenda. These summaries should be also brought together by the Strategic Communications Department at the Office of the Government. A formal platform should be created for these actors to facilitate not only regular exchange of information, but especially concrete cooperation and coordination on campaigns. In a similar way, the strategic communication of the state and individual ministries should also involve the private sector and companies, which can be important communicators to their own clients and/or employees.	High priority
Increase in financial, technical and personnel capacities	The Government of the Czech Republic and the Ministry of Finance should go beyond the Department of Strategic Communication. Office of the Government should also ensure an increase in professional capacities in individual ministries, not only in existing departments or divisions dealing with strategic communication, but also in ministries where such capacities don't exist yet. There should be at least a small team in each individual ministry focused on strategic communication. At the same time, all ministries should be equipped with adequate tools for open source and social network analysis and have up-to-date public opinion surveys on relevant topics. The Ministry of Finance should also allocate sufficient funds from the state budget for communication campaigns and long-term building of communication channels, including advertising on social networks, in order to effectively promote factual information and refute disinformation. A special fund for crisis communication should also be created for cases of need, which could be used under specific pre-defined conditions to ensure that crisis communication comes in adequate form and in a timely manner.	High priority

Systematic training of officials	The Office of the Government in cooperation with the Ministry of the Interior, NÚKIB and non-governmental and academic sector should coordinate the creation of a training program and related e-learning focused on strategic communication officials in the public administration. This training and e-learning should be provided to all employees in public administration, including regional and local governments, and include not only the theoretical level of strategic communication, but also practical simulations and exercises.	High priority
---	--	----------------------

Long-term framework

Incorporating strategic communication into the preparation of key legislative and non-legislative decisions and measures	The Office of the Government should ensure that strategic communication is an integral part of the preparatory process for all key measures. Each ministry should be required to include a communication plan in the preparation of any significant decision or new policy. This process should be monitored and coordinated by the Department of Strategic Communication at the Office of the Government. When drafting these communication plans, individual ministries should leverage consultations and advice from strategic communication experts, both from within and outside the public administration. The preparation of communication plans should incorporate up-to-date opinion poll, and ministries should also be equipped to anticipate potential informational threats or disinformation that may arise on the given topics, as well as prepare potential state counter-responses.	High priority
Evaluating the impacts of strategic communication	The Office of the Government should coordinate the ongoing evaluation of the impacts of strategic communication using analytical tools, opinion polls, and focus groups (particularly for offline communication). It should ensure the measurement of results from long-term communication activities as well as individual major campaigns and adjust and reassess future planned activities based on these findings.	Medium Priority
The use and strengthening of the concept of modern patriotism	The Office of the Government, in collaboration with the Ministry of Education and the Ministry of Culture, should initiate programs focused on strengthening modern forms of patriotism. These programs should include educational activities on the significance of historical events, support cultural and sports events that foster national pride and awareness of Czech history and values, and create media campaigns promoting positive examples of patriotism and civic engagement.	Medium Priority

