BRATISLAVA INTERNATIONAL SCHOOL OF LIBERAL ARTS

How Strategic Narratives Created a Strategic Mess: The Lack of Securitization of Disinformation Operations in Slovakia

BACHELOR THESIS

Max Radó

Bratislava, 2022

BRATISLAVA INTERNATIONAL SCHOOL OF LIBERAL ARTS

How Strategic Narratives Created a Strategic Mess: The Lack of Securitization of Disinformation Operations in Slovakia

BACHELOR THESIS

Undergraduate Study Program : Liberal Arts

Study field: 3.1.6 Political Science

Bachelor Thesis Advisor : James Thomson

Qualification : Bachelor of Arts (BA)

Date of Submission : January 31, 2022

Date of Defence : May 17, 2022

Max Radó Bratislava, 2022

Declaration of Originality

I hereby declare that this bachelor thesis is the result of my own work and has not been published in part or in whole elsewhere. All literature used is acknowledged and cited in the reference list.

In Bratislava, January 15, 2022

Max Radó

Abstract

Author: Max Radó
Title: How Strategic Narratives Created a Strategic Mess
University: Bratislava International School of Liberal Arts
Thesis Advisor: James Thomson
Thesis Defence Committee: Prof. PhDr. František Novosád, CSc., doc. Samuel Abrahám, PhD., prof. PhDr. Iveta Radičová, PhD., Mgr. Dagmar Kusá, PhD., prof. Silvia Miháliková
Head of the Defence Committee: Prof. PhDr. František Novosád, CSc.
Place, year, and scope of the thesis: Bratislava, 2022, 49 pages (88565 characters)
Qualification: Bachelor of Arts (Bc.)

Keywords: disinformation, securitization theory, countering disinformation, Slovakia

This work aims to explore the Slovak government's responses to disinformation operations, as a part of hybrid warfare, by foreign powers such as the Russian Federation. It´s main premise is that this threat was, until very recently, insufficiently securitized. This is reflected both in the main strategic documents and speeches of high Slovak politicians. If the government fails to prevent the spread of such narratives, both local and foreign disinformation actors can target the domestic population freely in order to weaken social cohesiveness, decrease public trust towards domestic institutions and authorities, and to establish a group representing the actor's interests which can be further utilised for strategic and political purposes. In this thesis, the responses of the government towards hybrid threats are interpreted through the prism of the securitization process, as developed by the Copenhagen School. Similarly, the theory of Copenhagen School provides viable criteria through which it is possible to determine whether securitization was successful or not.

The results indicate that, because of the state's inaction, Slovakia became a fertile ground for disinformation, and thus the process of securitization might be needed to build sufficient countermeasures with haste. Although securitization is generally portrayed very negatively by scholars, this thesis advocates for a more positive notion of this phenomenon in the case of disinformation, as it can be an effective approach for establishing policies to counter the spread of strategic narratives of a hostile actor.

Abstrakt

Autor: Max Radó
Názov práce: Ako Strategické Naratívy Vytvorili Strategický Chaos
Univerzita: Bratislavská medzinárodná škola liberálnych štúdií
Školiteľ: James Thomson
Komisia pre obhajoby záverečných prác: Prof. PhDr. František Novosád, CSc., doc. Samuel Abrahám, PhD., prof. PhDr. Iveta Radičová, PhD., Mgr. Dagmar Kusá, PhD., prof. Silvia Miháliková
Predseda komisie: Prof. PhDr. František Novosád, CSc.
Miesto, rok a rozsah bakalárskej práce: Bratislava, 2022, strán (znakov)
Stupeň odbornej kvalifikácie: Bakalár (Bc.)

Kľúčové slová: dezinformácie, teória sekuritizácie, boj proti dezinformáciám, Slovensko

Cieľom tejto práce je preskúmať reakcie slovenskej vlády na dezinformačné operácie v rámci hybridnej vojny zo strany cudzích mocností, ako je Ruská federácia. Hlavná hypotéza práce je, že táto hrozba bola až donedávna nedostatočne sekuritizovaná. Odráža sa to ako v hlavných strategických dokumentoch, tak aj vo výrokoch slovenských politikov. Ak sa vláde nepodarí zabrániť šíreniu takýchto naratívov, domáci aj zahraniční dezinformační aktéri sa môžu slobodne zamerať na domáce obyvateľstvo, aby oslabili sociálnu súdržnosť, znížili dôveru verejnosti voči štátnym inštitúciám a autoritám alebo vytvorili skupinu ľudí zastupujúcu záujmy aktéra, ktorú môže ďalej využívať na strategické a politické účely. V tejto práci sú reakcie vlády na hybridné hrozby interpretované cez prizmu sekuritizačného procesu, ktorý uviedla Copenhagen School. Podobne, teória Kodanskej školy poskytuje základné kritériá, pomocou ktorých je možné určiť, či bola sekuritizácia úspešná alebo nie.

Výsledky naznačujú, že pre pasivitu štátu sa Slovensko stalo úrodnou pôdou pre dezinformácie, a preto môže byť potrebný proces sekuritizácie na rýchle vybudovanie dostatočných protiopatrení. Aj keď je sekuritizácia odborníkmi vo všeobecnosti vykresľovaná veľmi negatívne, táto práca sa zasadzuje za pozitívnejšie poňatie tohto fenoménu v prípade dezinformácií, keďže môže ísť o efektívny prístup k vytváraniu politík na boj proti šíreniu strategických naratívov nepriateľského aktéra.

Acknowledgments

I would like to express my deepest gratitude to my advisor James Thomson for his invaluable advice and patience while helping me with this thesis. Without his guidance and support, this thesis would not be possible.

Secondly, I would like to thank JUDr. Daniel Milo for his help in understanding the effect of disinformation on Slovak society. Interviews with experts like him proved to be more informative than the majority of the available academic texts on the topic.

Lastly, I would also like to thank my family and friends for their love and support throughout my studies.

Table of Contents

Introduction: Disinformation Operations as a Part of Hybrid Warfare

Hybrid warfare is an ongoing process in the international community whereby some members deliberately spread false information that promotes their own narratives, in order to destabilise the domestic political systems of their adversaries. The Russian state's coordinated dissemination of disinformation and propaganda is a key weapon in its arsenal. Slovakia, despite being a small, strategically insignificant country, has found itself the target of one such disinformation campaign, as Golianová and Kazharski (2020) note: “Russian-backed disinformation has clearly been identified as a national security issue in Slovakia" (p. 1).

The purpose of a disinformation campaign (sometimes referred to under the rubric “active measures”) is to undermine institutions that serve as sources of factual truth, such as government agencies or the news media. Disinformation scholar Rid (2020) states: “For liberal democracies in particular, disinformation represents a double threat: being at the receiving end of active measures will undermine democratic institutions and giving in to the temptation to design and deploy them will have the same result” (p. 18).

The phenomenon of weaponised disinformation campaigns in the 21st century started to gain the attention of the media, academia, politicians, and the general public after the annexation of Crimea by Russia in 2014 and the ensuing conflict in eastern Ukraine. Despite the abundance of evidence of Russia’s strategic use of disinformation within so-called hybrid warfare, both the political elite and general public frequently fail to acknowledge the real threat of disinformation operations and thus may not fully understand the ways in which a pro-Western government can and should respond to disinformation.

The primary premise of this paper is that there are threats that must be approached through the securitization process, which describes how societies construct security threats through discursive practises, establishing what is and is not a significant concern in the eyes of domestic society. This paper will examine if the Slovak government sees Russian disinformation as an existential threat, and if so, how it has decided to respond. Similarly, this paper will highlight whether this position has changed during different administrations from the beginning of the conflict in Ukraine in 2014 until the year 2021.

The most interesting aspect of this research is the position of Slovakia on the geopolitical spectrum, where it is internationally oriented to the West, as a member of both NATO and EU, while having a significant portion of its population positively oriented towards Russia and the regime of Vladimir Putin. This puts defence policy makers into an unfavourable position as they either do not proceed with securitization of Russian hybrid threats and risk disinformation campaign being successful or must publicly argue that Russia, which is portrayed by those inclined to pro-Russian perspectives as a “Slavic big brother”, is in fact a self-interested actor which pursues its own goals in Central Europe by feeding disinformation to the Slovak audience.

The thesis will examine the approaches proposed by securitizing actors in Slovakia, such as government agencies, non-governmental organizations, and think tanks, to tackle the danger of Russian disinformation. The work will present a contemporary issue as it has evolved by evaluating the process of securitization, or lack thereof, to determine whether these strategic measures have firmly established themselves inside Slovakia's informational domain.

Literature Review

No, It Is Not Propaganda

Historically, the use of disinformation as a tool belonged in the arsenal of states at the height of the Cold War. In the language of the KGB, the former secret intelligence agency of the Soviet Union, "Active Measures" stands for ideological subversion with the use of disinformation. It has been a practice of secret intelligence agencies for decades. While the Cold War is no longer officially in effect, the practice of orchestrating disinformation campaigns has not entirely disappeared.

On the contrary, with the advancement of technology which led directly to the internet and social media platforms, disinformation campaigns can now have an even greater influence on a much larger audience more quickly and oftentimes more consistently than in the past. This section will provide insight into what disinformation campaigns are and how they function; furthermore, it will introduce securitization as a strategy that can be used to counter disinformation; finally, it will discuss the types of responses states use to securitize disinformation campaigns. In order to clarify what the author means by disinformation, multiple similar terms as described by Derakhshan & Wardle (2018) can be found below.

Misinformation	**Disinformation**	**Propaganda**	**Mal-information**
Misinformation is information that is false, but the person who is disseminating it believes that it is true (or is indifferent to its possible falsity).	Disinformation is information that is false, and known to be false by the person disseminating it.	Propaganda is usually more overtly manipulative than disinformation, typically because it traffics in emotional rather than informational messaging.	Mal-information is information that is based on reality, but used to inflict harm on a person, organisation or country.

La Cour (2020), defines 3 ‘prototypes’ of disinformation disseminated by state actors, which are the disinformation story, a disinformation campaign and a disinformation operation. According to her definition, a disinformation campaign is a “coherent campaign spreading multiple false stories in a foreign country linked to a particular event” (p. 5). Moreover, false narratives within disinformation campaigns do not present one particular view or promote one narrative, as they frequently aim to confuse a specific audience about the circumstances and facts surrounding any specific event. According to Mahairas and Dvilyanski (2018) the actor creating a disinformation campaign will often utilise existing “wedge issues”, issues which polarise society into two groups. The process of operating a campaign begins by identifying these issues and creating a narrative which further sows discord. Thus, disinformation is spread in the target’s informational sphere by the use of blogs, articles or posts made on social media addressed to the general public. Mahairas & Dvilyanski (2018) argue that the goal of disinformation campaigns it is to “create discord and confusion, and amplify existing divisive issues in order to further expand the space separating the targeted audience; thereby, making reconciliation between any two sides of a divisive issue even more difficult to achieve” (p.25).

Similarly, Mareš and Mjelniková (2021) argue that disinformation is a real threat because of its substantial potential for [“disrupting democratic discourse and increasing or escalating tensions between various groups in the population, be they political, social, ethnic, or religious”] (p. 89). The outcome of a successful disinformation campaign would artificially increase the existing conflicts in the public discourse in order to destabilise the society. Because of the level of interconnectedness of today’s world, with constant flow of information through international channels, the threat of disinformation does not only concern one society targeted by another state, but the authority of truth in itself.

According to Rid (2020, as cited by Rauch, 2021), disinformation campaigns covertly and gradually assault against the liberal epistemic order, represented by institutions such as empirical science or investigative journalism which "prize facts over feelings, evidence over emotion, observations over opinion” (p. 17). If the campaign is successful, the authority of fact is destroyed and is substituted by emotion. Rid proposes that liberal democracies are especially vulnerable to disinformation campaigns as these operations erode trust in government institutions but also entice the victim to produce disinformation of their own. The severity of the threat from disinformation is determined by the strength of the democratic system, Rid argues: “the stronger and the more robust a democratic body politic, the more resistant to disinformation it will be and the more reluctant to deploy and optimize disinformation. Weakened democracies, in turn, succumb more easily to the temptations of active measures” (p. 18). Undoubtedly, Slovakia is not amongst the strongest democracies, which makes the threat of disinformation that much more severe and urgent.

Nevertheless, in order for the campaign to succeed, it first needs to penetrate the informational sphere of the desired group. On this, Sarts (2021) argues that a hostile actor must establish itself as a natural component of that environment as it helps to disguise these campaigns and achieves one of the essential criteria, to go undetected. As the majority of effective disinformation campaigns go undetected by society, many players use this strategy. Additionally, state actors might also go unnoticed by collaborating with local players who would benefit from such discourse. Sarts claims this strategy is successful because it is difficult to distinguish between a legitimate reaction by a local group to an issue in the public discourse and an attempt by a hostile power to exploit a vulnerability to weaken the society.

Because of the possible relationship between foreign powers and local organizations, Mareš and Mjelniková (2021) categorise actors based on their affiliation and the tactics they employ. While most disinformation campaigns are, according to the authors, organised by governmental actors and their agencies, others include the involvement of non-state, but pro-governmental forces. The chapter’s most significant contribution lies in the description of the Russian disinformation apparatus which employs both governmental and non-governmental bodies. They claim that at the top of the apparatus, there are secret intelligence agencies, such as the FSB, which are responsible for “prefabrication and the primary spread of propaganda messages and disinformation” (p.84). Based on the insight, it is clear to see the potential impact disinformation campaigns can have on a targeted audience.

Securitization Theory

As the main aim of this work is to analyse how the process of securitization of disinformation did not occur in Slovakia, it is absolutely imperative to define it as a concept. The theory of securitization by the Copenhagen School, represented by Buzan et al. (1998), lays a foundation for examining how security challenges emerge, how threats are presented, and what actors are involved in the process of securitization. The Copenhagen school suggests that security should be seen as a speech act, where the central issue is not if threats are objective or subjective, but the ways in which a certain issue can be socially constructed as a threat. Therefore, Buzan et al. introduce three categories of threats based on their significance. While the non-politicised issues are insignificant and are not a part of public discourse, the politicised issues are a part of government policy and require resources. The most severe threats have to be securitized as they are "presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure" (p. 24). The state elite decides which issue belongs to which group, as some issues can be elevated to a group with a higher priority. The process of the speech act consists of a securitization actor who asserts that a referent object is existentially threatened, thus the actor demands the right to take non-standard countermeasures to address the threat. In other words, the securitising actor legitimises the use of countermeasures by persuading an audience that breaking rules to address the threat is appropriate. As the audience has to accept the existence of a threat, the securitizing actor can employ tactics of deception, to inflate the threat by offering biased or false narratives convincing enough for the population to consent to extraordinary measures. However, the use of extra politics does not imply that successfully securitized issues would be militarized, on the contrary, many issues can be dealt with by desecuritizing them rather than securitizing them. Nonetheless, securitized issues will be reflected in a national security modus operandi. When it comes to the act of breaking the rules, in the case of information exchange between people, most of whom now communicate through social media, regulation of information channels, where false narratives are spread the most, by the government could prevent the spread of foreign disinformation. This work, however, does attempt to draw a line between successful securitization of disinformation and suppression of free speech and it leaves such a task to further research in the field.

The nature of the securitising agent has changed as they were usually associated with power and authority, such as an elected official or a member of the state security apparatus, whereas now an increasingly wide range of actors, such as think tanks and non-governmental organizations, may attempt to securitize specific challenges. However, the audience, whether it is the general public or other members of the political elite, can decide whether to accept the existence of the threat or not. According to Buzan et al. (1998), "A successful securitization thus has three components (or steps); existential threats, emergency action, and effects on interunit relations by breaking free of rules" (p. 26). The crucial component of the process of securitization is the audience, for if the audience is not approached and not convinced by the agent of securitization of the existence of a threat then securitization cannot happen.

	State actor	Non-state actor
Audience	Citizens	General public
Securitization move	Speech act : represented by statements of officials and defence policy paper	Speech act: publications and rapports which increase awareness of a threat
Tools of securitization	Government institutions and agencies (ministry of defence, secret service agencies)	Do not possess effective tools of securitization

Why Securitization is the Right Path to Take to Tackle Disinformation

Roe (2012) accurately summarises the debate surrounding the theory of securitization. While the Copenhagen School sees securitization as an act where a legitimate existential threat is constructed by the elite and requires means beyond standard democratic procedure, the opposition, represented by Aradau (2004), proposes that the act of securitization itself is inherently damaging to democracy as both the process and outcome of the act are fundamentally undemocratic. On this, Roe writes, "Securitization's negativeness, therefore, lies in its disruption or indeed complete abandonment of open and accountable government (p. 252). This alleged abandonment stems from the procedure of securitization that is generally perceived negatively because it possesses qualities of speed and silence, which are often qualities of authoritarian procedures dealing with threats, while the outcome significantly increases the power of the ruling elite. Furthermore, Aradau highlights the assumption that silence and speed characterize the kind of security politics the referent object wants. It is the consensus among the audience to choose whether they will consent to fast-tracked, exceptional measures or to rather have slow but democratic procedures where scrutiny is essential (p. 252).

Nevertheless, for Roe, the speed and silence of the process do not necessarily result in a lack of discourse to give the securitising actor permission to use countermeasures outside of his jurisdiction, as he writes, "While the legislative process is surely accelerated, a degree of scrutiny and oversight nevertheless remains" (p. 260). Securitization, for the Copenhagen School, symbolizes panic politics, a situation where the actor of securitization must act immediately, as the safety of the audience is in jeopardy. Under such circumstances, it is evident that the chance to discuss, for example, the morality of actions taken, is limited to a bare minimum. In principle, extraordinary politics means that standard procedures cannot be used since it may already be too late to respond with force. Bigo (2002, as cited by Roe, 2012) demonstrates how security experts, armed with privileged information, authoritatively characterize risks, as it is easier to exaggerate or aggravate existing threats embedded in the society in order to promote their own institutional goals, rather than responding to such threats out there. (p. 252). Additionally, through the security speech act, the actor of securitization can reorient relations with other entities, from friends to enemies and vice versa.

On the whole, Weaver (2011, as cited by Roe, 2012) claims that particular securitizations cannot be “positive or negative per se, rather, their quality depends on who else is involved, doing what” (p. 261). While in the academic debate securitization is seen generally as a negative process, this regards securitization as necessary to effectively counter foreign disinformation operations, which, as highlighted above, can have detrimental consequences on the security and well-being of a given state and its citizens.

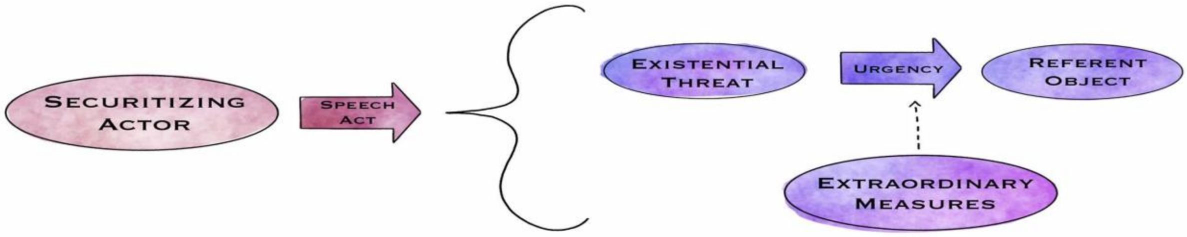
Securitization of Disinformation in Practice

Hellman & Wagnsson (2017) observe the responses of European countries to Russian information warfare. As Russia's information warfare and propaganda campaigns against European neighbors have intensified, Western democracies are forced to respond to hostile narratives in order to defend against the other's frame of interpretations and protect their own view of reality. The authors proceed to divide the responses to hostile narratives into two dimensions. While the first dimension splits responses according to the degree of engagement into engaging and disengaging, the second separates policies into those which target domestic or foreign audiences. By combining the dimensions of engagement and targeting, Hellman & Wagnsson develop four different models which states adopt in order to respond to hostile narratives. These strategic responses are confronting, blocking, naturalising or ignoring.

Confronting entails actively creating and projecting counter-narratives in response to a hostile narrative. Similarly, a blocking strategy also acknowledges the existence of a foreign narrative, but it sets up very strict countermeasures which enables the domestic state to control the flow of information, conflicting with the values of a free and democratic society. Naturalising is the act of projecting one's own narrative without directly contrasting it with those of the “other." Lastly, ignoring means to avoid engaging with foreign strategic narratives, or the “no-narrative strategy” (p. 10). This approach is less consistent and thus potentially weaker than the others, for it relies on people's ability to decode narratives, which may be too optimistic. Similarly, it could also lead to an over-reliance on the media as objective, independent actors who will protect democracy for the state.

Research Design and Methodology

To explore the securitization of disinformation in Slovakia, this thesis employs a single case study method. Yin (2009, as cited by Ridder (2012)) defines it as “an empirical enquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident” (p. 93). Methodologically, the thesis will follow the process of securitization as described by the Copenhagen School, identifying the specific criteria of the process which have to be necessarily met in order for securitization to be successful and applying it to Slovakia. As seen in the diagram below, inspired by the one of Özcan (2013), this is the clearest example of the securitization process.



The focus of the thesis is concerned with the securitizing actor's assessment of the severity and threat level of the issue of disinformation, the concrete policies put in place to combat disinformation, and the pace of the securitization process. Thus, the focus illustrates the phenomena of securitization, while assuming that the theory itself holds validity.

There is very little scholarly evidence on government responses to disinformation in general, let alone in the case of Slovakia, due to the recent occurrence of some of the cases under investigation. As a result, the thesis' analysis relies significantly on secondary sources. Traditional news sources are useful in relaying events to the reader and summarizing the initial disinformation activities. The thesis analyses statements by elected officials published documents by government agencies, think-tanks and non-governmental organizations which have conducted research on hybrid warfare and lastly, related policies and measures passed in Slovakia which will be used to measure the degree of securitization of disinformation. In terms of the analysis' time scope, the paper covers the years 2014, marked by the annexation of Crimea and subsequent conflict in the Donbas region of Ukraine, through 2021. As a result, the research comprises official strategy documents published since 2014, such as the Defence Strategy of Slovak Republic and reports of the Slovak Information Service (SIS, Slovakia’s main civilian intelligence agency).

In order to gain qualitative and relevant information about the subject, several in-depth structured and semi-structured interviews were conducted. The interviewees were selected based on their affiliation with securitising actors, such as the Slovak Ministry of Defence, but also specialists from NGOs, journalists investigating sources of disinformation and academics invested in the field.

The thesis concludes with an empirical analysis that incorporates the knowledge gathered via interpretive case study, as this is the most effective approach to contextualize the events. In this way, the thesis seeks to expand knowledge on the phenomena of disinformation particularly in a country like Slovakia with a rather complex relationship with Russia. Lastly, the thesis can also contribute to the knowledge of securitization of hybrid warfare such as disinformation campaigns.

Thesis Statement

The threat of disinformation campaigns were insufficiently securitized in Slovakia because of the inability of the government to set up effective countermeasures and its unwillingness to inform the general public about the existence of such a threat, which resulted in Slovakia becoming a “breeding ground for disinformation”.

Chapter 1 : A Strategic Tragedy

The Russian Federation launched an unexpected offensive on Crimea in 2014, employing both conventional and unconventional warfare tactics. Crimea, according to Galeotti (2015), was the ideal place to put Russia's new approach to warfare to the test, combining strategic narratives with covert military operations. The annexation was successful due to the Ukrainian government's mistreatment of the local population and the military's small, and to a large extent apathetic, presence on the peninsula. The setup for the seizure of Crimea included a disinformation campaign aimed at residents and Russian special forces infiltrating regional forces on both sides at the time. The success of this operation changed the security environment in Europe entirely as it showed how powerful a tool hybrid warfare is.

Traditionally, the most effective securitising actor was the government, as it possesses the means to successfully deter or destroy a given threat. Even though threats are now more abstract than physical in form, governments in functioning states still have a monopoly on violence and, via their agencies, can attack or defend their interests and more importantly, their sovereignty. Such actions are described in strategic policy papers which are published regularly to inform citizens of the procedures which protect national security. As disinformation operations are part of the arsenal of hybrid warfare, from the security standpoint, the government has to take measures that help protect against the successful deployment of such hybrid weapons.

The Slovak Republic's immediate reaction to the events in Ukraine was similar to that of its Western allies. The Slovak government openly criticized the Russian Federation's flagrant breach of international law and later joined EU sanctions. Even though one would expect a similar position to be reflected in Slovak strategic papers, quite the opposite is the case: they seem to demonstrate a more cautious approach to identifying Russia as an international aggressor. The first important document within the scope of this research is the White Paper on Defence of the Slovak Republic published in 2016, which acknowledges the evolving security environment, defined by the growing relevance of hybrid warfare.

According to the Ministry of Defence of the Slovak Republic in 2016, “Strategic-level propaganda along with specific operational methods which are today called 'hybrid means of conducting combat operations' represent a major security threat from the point of view of conducting conflicts in a changing security environment” (p. 34). The document predicts that hybrid warfare will influence the long-term security environment of Slovakia, but fails to mention any proposed plans by the government to reverse this trend. As such, the White Paper did highlight the possible threats to the population but it did not succeed in reassuring the reader that necessary steps were being taken to improve the defenses against said threats.

The year 2017 was marked by the creation of major strategic publications, the most significant of which was the Defense Strategy of the Slovak Republic. While the Strategy was weaker in terms of language, it finally included the threat posed by disinformation and foreign hostile activities to Slovakia. Nonetheless, the importance of this document in terms of securitization is controversial as it has never gone into effect. The attempted implementation of the Slovak Republic's new security strategy in 2017 was unsuccessful due to a lack of political consensus among members of the then governing coalition. While the Defence Strategy of 2017 is comparatively more critical of the Russian Federation than the White Paper published in 2016, as it describes the annexation of Crimea as an extremely worrying case of violation of the fundamental principles and standards of international law, it also maintains the importance of dialogue with Russia. Yet, the Defence Strategy makes no mention of military activities which were directly involved in the conflict and were directed from Moscow, only emphasizes the rise of hybrid activities and expects that the armed forces to be able to employ conventional means to counter hybrid threats. With regard to hybrid threats, the strategy acknowledges that the nature of armed conflicts is shifting from the use of conventional weapons to tools of hybrid warfare. More importantly, it highlights the possible consequences of tools of hybrid warfare on the general public, as the publication states,

> [Hybrid threats] polarize society, bring uncertainty, and thus undermine the legitimacy, credibility, and ability of state institutions and of democratic constitutional order to act, and thus have a negative impact on the realization of the security interests of the states exposed to them. Hybrid activities can also be aimed at weakening public support for the fulfillment of international obligations or to paralyse the reaction of the international community (Article 27, Author’s translation).

Furthermore, the Security Strategy proposes the course of action by which it will improve the state’s resilience to hybrid threats not only by developing appropriate domestic and international strategic communication facilities but also by strengthening the bilateral cooperation between international organizations and also relevant NGOs (Article 79). Unfortunately, the implementation of the revised strategy did not get enough support in the parliament, particularly because the Slovak National Party (SNS), a pro-Russian oriented party, refused to vote on the proposal. Anton Hrnko, a member of the party, offered an explanation on why they refused to support the new Security Strategy, saying, “There are things that are unacceptable to the SNS, because the SNS thinks that Slovakia has no enemies and does not need to produce enemies” (SME, 2018). This meant that the Security Strategy from 2005 was reintroduced. As a result, Slovakia’s defence strategy was highly outdated and did not possess a framework by which it could respond to advanced security challenges.

The implementation of the Concept for Combating Hybrid Threats in 2018 was a turning point in Slovak policy towards hybrid threats. It declares that the Slovak Republic, as a member of the European security environment, faces the same security challenges as other EU and NATO member states, and thus cannot disregard this type of threat. Furthermore, it emphasizes that a persistent disinformation effort is taking place on Slovak territory, often including foreign players and their agencies, propagating diverse narratives. According to the Concept, these disinformation campaigns often disseminate an over-simplified or false image of current issues which trouble the general public and claim that these issues stem from the membership status of both EU and NATO. If these efforts are successful, the state is weakened from within, the Concept states:

> [The effect of disinformation activities] may be reflected in society's increased distrust of representative democracy, a reduction in interest in participating in national or European elections, and thus weakening the legitimacy of elected political representations. The ultimate goal of such campaigns is to weaken the states and their policies, to weaken the EU from within, or even to provoke the departure of its members and thus damage its geopolitical position (p. 3, Author’s translation).

On the whole, the main objective of the Concept is to provide a platform for information cooperation and exchange among relevant departments so that hybrid threats may be efficiently identified and countered. The actions proposed within the Concept, however, were insufficient as Stolkay (2018) rightly points out, “Not only are our reactions delayed, but they are also not very original and even insufficient” (para. 2).

While not a strategic defence policy paper, the SIS Activity Report for 2019 serves as an example of a publication that contains threat assessments with the goal of raising public awareness about certain security challenges. In summary, the intelligence service details Russian hybrid actions against the Slovak population. Moreover, it identifies those domestic actors that are suspected of spreading strategic narratives to their audiences. As the report points out:

> The main disseminators of pro-Russian narratives in the Slovak Republic were pro-Russian civic organizations and groups on social networks, Russian news media, including their foreign branches, and the so-called alternative media. As in the previous period, Russian propaganda largely abused pro-Russian sympathizers, who, out of their own convictions, uncritically took over and spread these messages (para. 59, Author's translation).

Nevertheless, as the current government changed so did the approach towards hybrid warfare. After the political party Ordinary People and Independent Personalities (OĽaNO) defeated Direction (Smer) in the 2020 elections, ending Smer's eight-year stint in power, the geopolitical focus of the government shifted towards the EU and NATO. Furthermore, the newly established coalition also vowed to update the country's outdated strategic documents, such as the 2005 Security Strategy of the Slovak Republic.

In 2021, the government delivered on its promise and implemented a new Security Strategy of the Slovak Republic which reflected the current security environment. At first, the strategic document begins by emphasizing the European Union and NATO as cornerstones of Slovakia's security and defence. Among other new components, the altered strategic paper identifies the significant increase of disinformation narratives in Slovakia. Disinformation activities, according to Article 10 of the Security Strategy, can have a severe impact on the Slovak population by weakening the democratic political system and decision-making mechanisms. Additionally, the effect of such narratives might even "weaken citizens' trust in the democratic state and the rule of law and question the importance of NATO and EU membership" (Article 10, Author's translation). Equally important is the plan of action of the government to boost the general public's resilience to being susceptible to disinformation narratives, as described in the document:

> The spread of information to the population will contribute to the resilience of the population to misinformation and harmful propaganda from the external and internal environment and to their trust in public administration bodies and support for the Slovak Republic's membership in NATO and the EU (Article 64, Author's translation).

Despite Slovakia's recent developments, there are still significant issues with the securitization of Russian disinformation operations, as none of the documents analyzed above clearly declare such activities as a potential threat. As an illustration, the Concept of 2018 avoided naming the potential threat actors altogether. Nevertheless, there is great anticipation of a new strategic document called the Action Plan for Coordination of the Fight Against Hybrid Threats. After the document was presented to security experts at Globsec in June of 2021, Marian Majer, both the co-guarantor of the Hybrid Action Plan and the Deputy Defence Minister, highlighted the critical role of interdepartmental cooperation in this initiative, stating, "Countering hybrid threats is an issue not only for the Ministry of Defence or the other powerhouse ministries, but it is a complex challenge for the State and society as such" (Ministry of Defence of Slovak Republic, 2021).

While the exact details of this document have not yet been revealed at the time of this writing, in November 2021, Defence Minister Jaroslav Naď when revealed that they are working on a new action plan to coordinate the defense against hybrid threats, mentioned that the document includes "measures aimed at strengthening social resilience and combating disinformation, but also education and teaching of media literacy or critical thinking" (Aktuality, 2021). The experts who have been briefed about its contents, especially those dealing with disinformation and strategic communication, have voiced their approval of the draft of the Action Plan. Daniel Milo, was one of the experts who had the opportunity to study the document, and while he could not share any specifics, he said that,

> "[The Action Plan] aims to create a strategic framework and set up particular tasks for individual ministries. To chart away on increasing resilience towards hybrid threats and create a cross-departmental system coordination of activities, ranging from collection, analytical activities to developing additional policies and changes in the legislative. It is broad but it mentions concrete tasks for the ministries and state bodies" (Daniel Milo, online communication, November 2021).

Due to one of the prerequisites of successful securitization being the process of communicating the existence of a threat from the elite to the general public, and consequent the audience's acceptance of the threat, the defence papers from the period of 2016-2020 failed to identify Russia and its hybrid capabilities as a threat. Although the current government is taking steps in the right direction in terms of building institutionalised countermeasures and building the public's resilience to disinformation, the effect such communication might have on the population will depend on the level of trust towards government authorities and institutions.

As long as all these measures which are outlined in the Action Plan and other strategic documents are implemented, their result might be higher societal resilience to strategic narratives. Nevertheless, the obstacles in the path to successful securitization lie not only in the reversibility of the strategic documents by the next elected government in the future but also by the practice of current Slovak politicians and public officials who themselves spread disinformation on their social media in order to increase their influence.

Chapter 2: Sabotage out of Incompetence

Provided that successful completion of the securitization process implies audience acknowledgement of the threat, this chapter will review how the Slovak government attempted to frame hybrid warfare as an existential threat to the Slovak Republic by appealing to the citizens of Slovakia as the primary audience through state officials. While other, lesser authorities might have an impact on the process of securitization of hybrid warfare, when it comes to foreign policy and national security, one can argue that the authority of the prime minister increases the chances of a successful securitization in the respective fields. As primary sources, the study will use official statements made by Slovak politicians, and the Slovak mainstream media.

The prime minister of Slovakia is the highest-ranking official in the country, articulating discourse on a national but also a European level. As a result, the holder's position empowers them to make securitizing moves that might ultimately lead to securitization on both levels. When it comes to hybrid warfare and the threat it represents one can observe a pattern of behaviour by former prime ministers, namely Robert Fico and Peter Pellegrini, that has failed, by comparison with former president Andrej Kiska, in presenting the disinformation threat to the general public. While Kiska acted as a counterbalance to Fico's statements, as he publicly criticised Russia and its hybrid operations, his position as the president of Slovakia does not possess the executive power to create and implement new security measures, thus, it can hardly be recognised as a securitising move.

For this study, I gathered the original or translated quotes from politicians through a search engine by using the following combinations of keywords:

a) 'Prime minister of Slovakia on disinformation

b) 'Robert Fico on disinformation ,' the Slovak Prime Minister in 2014 (until May 2018);

c) 'Andrej Kiska on disinformation,' the former President of Slovak Republic from 2014 until 2019;

d) 'Peter Pellegrini on disinformation,' the Slovak Prime Minister who replaced Fico as Prime Minister in 2018 (until March 2020);

e) ‘Igor Matovič on disinformation, leader of OĽaNO, winner of March 2020 elections (until April 2021).

The search was also repeated in the Slovak language, (here the keywords were ‘dezinformácie’ plus the full name of the given Prime Minister). I considered the fact that defence policy and matters of security are not only informed by Prime Ministers, and matters related to national security are included in the discursive acts coming from Ministers, Presidents, and other actors which have high-enough position to also make them relevant.

2.1 The Political Discourse Regarding Hybrid Threats from 2014 to 2020

2.1.1 Robert Fico

Robert Fico, who was prime minister from 2012-2018, i.e. during and after the crisis in Ukraine, did not echo the rhetoric of Slovakia’s allies or condemn the Kremlin for its aggression and involvement in the conflict. Fico often relied on softer words about Russian policy, often using the phrase “violation of principles of international law” instead of “aggression” or “invasion” when publicly discussing events in Crimea (Dennik N, 2015). As an example, Gyárfášová and Mesežnikov (2015) observe that rhetoric about Russian aggression towards neighbouring Ukraine has been “absent in Fico’s observations” (p. 148). By his choice of words, Fico was communicating to Slovak citizens that there was no direct political and military involvement in Ukraine by the Kremlin and that Ukraine was suffering from an internal conflict among Ukrainians.

Furthermore, Fico characterised the Russian-Ukrainian conflict as “a global propaganda war”, in which the EU only listens to the “voice of Ukraine”, and that nobody is interested in “hearing the voice of the other side” (Pravda, 2014). Even though he even emphasised the presence of a propaganda war, one can infer that he deliberately failed to identify the actor which was actually disseminating disinformation through communication channels throughout the EU. After his party SMER-SD won the 2016 elections, the government programme mentioned a pledge to update strategic documents, and even though it was government approved, the updated Security and Defense Strategy was not submitted to the National Council of the Slovak Republic for approval. Meanwhile, not only did the former prime minister fail to condemn Russia’s actions and bolster the security of the state, he even portrayed Russia as a victim of propaganda. Researchers such as Gyárfášová and Mesežnikov assume that Russia was too important in both economic and strategic terms to Fico that any public statement critical of the

Kremlin could risk damaging such ties. As a result, Fico during his term, was a proponent of preserving friendly relations with Russia, despite his government's Interior Ministry publicly stating that “Slovakia, like other states in Central and Eastern Europe, has become the subject of information activities of the influential structures of the Russian Federation” (Šnídl, 2016).

Rechtík and Mareš (2021) see Fico’s approach as a pragmatic one, writing that his approach is characterised by “accentuating the importance of energy relations with Russia while under-emphasising threats which Russia poses to Slovakia’s national security” (p. 14). Nevertheless, it is hard to argue if the hypothetical economic costs of adopting a more critical approach to Russian hybrid activities were seen as too high by the decision-makers to protect the country and its people from new security challenges. Moreover, given the level of energy dependence on Russia, further aggravated by its position as a major transit country without any protection against Russian influence, Slovakia, because its government put economy above security, was put into a position where it became highly susceptible and vulnerable to Russian disinformation threats. On bringing awareness of the threat of disinformation operations by Fico's government, Milo said that it brought awareness only “To a limited extent, as the [Smer] government was quite different in geopolitical views, and these views manifested themselves in the policy papers, but also in terms of foreign policy as even in the height of Sergei Skripal's case Slovakia was among the few countries which did not deport Russian personnel” (Daniel Milo, online communication, November 2021).

Recently, as noted by Sitko (2021), Robert Fico has begun spreading disinformation on his own social media profiles in order to evoke negative emotions, which are spread more easily thanks to the algorithms used by platforms such as Facebook. Using this approach, Slovak politicians like Fico can get more exposure than they would get via traditional media outlets, resulting in more substantial political support.

2.1.2 Andrej Kiska

President Andrej Kiska (2014-2019), while prevented by his role from engaging in normal day-to-day politics, nevertheless actively countered the narrative of Robert Fico. The then president stated clearly that Slovakia should coordinate with NATO and EU, as highlighted in a speech in 2015, ”The illegal annexation of Crimea, the continuing war in Ukraine, the continuing occupation of South Ossetia and Abkhazia [separatist regions in Georgia sponsored by Russia], as well as the heavy disinformation campaign against our countries have ended our vision of a strategic partnership with Putin's Russia” (TASR, June 2015). Gyárfášová and Mesežnikov

(2015) write that despite Prime Minister Fico, who frequently advocated (and continues to advocate) for reducing or even eliminating sanctions against Russia, Kiska encouraged EU member states to maintain the imposed sanctions (p. 150). In July 2014, he spoke in favour of strengthening sanctions against Russia as a common EU response. Kiska also stressed the importance of united front of EU states when facing assertive actors such as Russia, "As far as our position towards Russia is concerned, it is extremely important that the EU preserves a united position so that Russia cannot take advantage of the differences between the states of the Union and break our internal unity" (Webnoviny, 2015).

On the topic of disinformation in hybrid warfare, Kiska observed in this context that there has been a growing information war in the form of misleading information and lies that are being spread by the media and by various actors on the internet at a time of the conflict in Ukraine. Slovakia's president said that, "I have no doubts about [Russia's involvement in Ukraine], and I believe that anyone with adequate information who hasn't succumbed to Russian propaganda can't have any doubts, either" (Daily News Monitor, Feb 2015, p. 3). On the whole, Kiska was unafraid to critique Russia because its image shifted from being an economic partner to a potential threat. Furthermore, he was aware of influence operations spreading various narratives containing disinformation and propaganda. The former president openly criticised the government's passivity during a press conference in 2017: "Information war is one of the serious threats to Slovakia, and unfortunately, the official units do very little, do almost nothing" (SME, 2017). He also added that Slovakia is "a target which does not defend itself", that the behaviour of competent officials was highly irresponsible, and that neighbouring countries within the Visegrad Group are doing more to protect their states and their people. Sadly, Kiska's approach was not adopted by other highest constitutional politicians at the time, thus, only a minor part of the general public was alerted to the existence of hybrid threats.

2.1.3 Andrej Danko

Another foreign policy actor among Slovak politicians has been Andrej Danko, the Speaker of the National Council of the Slovak Republic in 2016-20, who established and maintained close relations not only with representatives of the Russian Federation but specifically also with individuals sanctioned by the EU. Such relationships seemed to be mutually beneficial, since he could gain not only support from the pro-Russian oriented part of the population but also the personal prestige flowing from relations with representatives of the largest country in the world. The Russian Federation, in turn, had an ally in Danko in the form of the second highest constitutional official of a country that was a member of both the EU and NATO. By using this connection, the Kremlin established a channel through which it could disseminate strategic narratives which would be utilised to disseminate pan-Slavist narratives on a wide scale. Danko, in a joint statement in 2017, made alongside President Kiska and Prime Minister Fico, called for "steps that will increase the security of our citizens and the defence capacity of Slovakia, especially by means of implementing the updated Security Strategy, Defence Strategy, and Military Strategy of the Slovak Republic" (Office of the President, October 2017).

Nevertheless, even after such a public statement, his Slovak National Party (SNS) decided to block the updated security documents which meant weakening the ability of the Slovak Republic to respond to both conventional and hybrid threats. Danko's party was unwilling to support the implementation of the documents because of the characterisation of the Russian Federation as a security challenge to Slovakia. Unfortunately, the party solely focused on representation of Russia and missed the importance of establishing security measures targeting a wide variety of foreign actors. When Daniel Milo was asked about the SNS's sabotage, he stated that

> "The security strategy failed because Andrej Danko connected his political legacy to a great extent with building good relations with the Russian Federation. Obviously, having Russia mentioned as a security challenge would hurt these relations, so he vehemently opposed any such mention in official strategic documents. The security strategy then ended up in limbo because it was on one hand passed by the government but on the other hand not passed by the parliament, making the document not legally binding" (Daniel Milo, online communication, November 2021).

2.1.4 Peter Pellegrini

Although Peter Pellegrini was not prime minister for long enough (2018-20) to make extraordinary changes, he did inherit the issue of an outdated security policy from Robert Fico. Pellegrini, who was by then prime minister, stated that he considered the non-adoption of the new Security Strategy to be simply a technical problem. However, by simplifying the process, and more importantly, the importance of implementing such a fundamental strategic document, Pellegrini, similar to his predecessor, failed to push for the update of strategic documents which were much needed. Pellegrini simply left the task to a future government, stating: "The revised strategy papers will wait until a new government is formed after the February parliamentary elections" (SME, 2020).

It is worth pointing out that the Concept cannot be considered a high-profile document. As an amusing example of its relatively poor accessibility (and possibly low impact on the general public), we can mention an interpellation by an MP to ask whether any document for combating hybrid threats had been released – a year and a half after the publication of the Concept (National Council of the Slovak Republic 2019).

2.2 A fresh start in the fight against disinformation

The situation regarding securitization of hybrid threats, and particularly disinformation operations, changed after OĽaNO won the 2020 elections and formed a new government. In its programme manifesto, it showed an interest in finally updating the national security strategy by highlighting Slovakia's position alongside its western partners. While the previous government of Smer, SNS and Most-Híd practically overlooked the threats posed to the country by disinformation, the government of Igor Matovič (OĽaNO) decided to act, and to take real steps to deal more deeply with this issue. Even though Prime Minister Matovič did not directly mention the threat of disinformation, his government's programme manifesto at least mentioned the threat of disinformation and publicly pledged to take action. It states:

> "The spreading of disinformation and hoaxes endangers the development of a knowledge-based society ... The Government of the SR will prepare an action plan for coordinating the fight against hybrid threats and spreading of disinformation, and build adequate centralised capacities to carry it out" (Sirotnikova, 2020).

Not only this, but also the fact that the current government updated and successfully implemented the two main strategic documents, the Security Strategy and the Defence Strategy of Slovak Republic, made many experts within the field hopeful that something was finally being done to address the threat. The Ministries of Foreign Affairs, Defence, and Interior should be the major driving forces in the current government's fight against disinformation operations. Their knowledge should now be used to contribute to the creation of a broader understanding. Jaroslav Naď, the current Minister of Defence, believes that the cooperation between ministries was necessary because of the inactivity of the past government, about which he stated: "Disinformation, hoaxes, the fight against propaganda are all part of a package called strategic communication, and there was zero effort to deal with it in the past" (Aktuality, 2020, author's translation). In the same statement, Naď also declared that the ministries will take “fundamental steps to suppress disinformation as one of the hybrid threats that exists here” (Aktuality, 2020, Author's translation). As such, disinformation operations were portrayed as a threat to the target audience by a member of a political elite, yet no proposed plan of action, which would be considered outside the normal political realm, was announced at that time. Nevertheless, it is understandable that a call for popular approval for an action against disinformation that would require diligent threat assessment which, as was highlighted by the Minister of Defence, was non-existent until he took over.

When asked about the performance of the current government, Daniel Milo replied that it set off in the right direction, towards being “more open, and directly mentioning foreign interference, including disinformation, in public speeches and statements”. More specifically, the statements of Foreign Affairs Minister Ivan Korčok, and Defence Minister Jaroslav Naď serve as examples of official’s more critical stance towards Russia. Additionally, there is also Veronika Remišová, the head of the newly established Ministry of Investment, Regional Development and Informatization, who also included her department in the government's effort to boost public resilience, saying in a public statement, “We will support the activities aimed at combating disinformation. We are witnessing this phenomenon gaining momentum in recent years and it is important that we teach children, students and the public how to access information, how to verify resources, especially in the digital world of the Internet and social networks” (Ministry of Investment, Regional Development and Informatization, 2021).

On the other hand, Tomáš Kriššák, an expert on information threats from Gerulata Technologies, believes that the current government displays a similar attitude towards securitization of disinformation compared to its predecessors. According to their website, Gerulata Technologies is a technology company specializing in developing software for STRATCOM (Strategic Communications) and OSINT (Open Source Intelligence). The company is now cooperating with the current Slovak government. Its goal is to improve the strategic communications among individual ministries, making it easier for the citizens to understand the message the government wants to relay without confusion, making it harder for disinformation actors to spin government narratives to their favour.

The absence of any political will to securitize disinformation is, according to Kriššák, one of the key aspects of why little to nothing was and is being done to counter them. As he said in an interview, “Even if there was a political will 10 years ago, which in my opinion is unthinkable because of the political climate, then there is simply a critical lack of people who are oriented in the topic". As an example, Kriššák revealed that "The Ministry of Education was not present at any of the meetings where topics such as disinformation were addressed, because they do not have a single person who could do anything on this topic. And education is the complete basis for creating resistance to disinformation and similar information threats" (Tomáš Kriššák, online communication, December 2021). Another reason which might explain the passivity of high-ranking politicians, both past and present, is the fact that fighting against disinformation does not result in higher public support, as Kriššák states :

> "For politicians, this is a difficult topic because they can not gain any capital from it, so it is hard to turn this topic around so that people will give them more support, it will only appeal to a politician who understands the topic and knows the implications of disinformation on a society" (Tomáš Kriššák, online communication, December 2021).

Furthermore, the effort to deal with disinformation by the current government is, according to Milo, also highlighted in the key strategic documents. In these documents, the use of language is the most important tool in policymaking, especially in the case of securitization, where attributing the meaning of a threat to an object is a crucial step for the actor of securitization to be given special privileges and power outside his jurisdiction. On the specific words used in strategic documents and public speeches, for example when Russia is called a "security challenge" and not a "threat", Milo stated that these are often "nuances, and what is important is that these issues are being addressed at all" (Daniel Milo, online communication, November 2021). The only concern, shared amongst the experts Milo and Kriššák, is that after the next elections, these efforts might be reversed by the next government which might be of a different composition with dissimilar geopolitical orientations.

When the first wave of COVID-19 hit Slovakia, disinformation actors had been active for years, with only non-governmental activists and information and security specialists countering their narratives and bearing the majority of the burden. These civil and non-governmental organizations could only use their platforms to spread awareness of the threat to the general public, but as they do not possess any extensive resources and tools to securitize hybrid threats, this burden falls to the state. Yet, since state actors were passive in their role, no systematic protection against disinformation operations, whether local or foreign, was constructed.

The damaging consequences of disinformation were finally tangible during the COVID-19 pandemic, when the health of the general public was at risk from medical disinformation spreading conspiracy narratives about the origin of the virus, COVID testing, and the contents of vaccines. Slovak disinformation experts warned at the beginning of the pandemic that false COVID-related narratives and influence campaigns would definitely be spread, putting extra pressure on the government's effort to persuade people about the benefits of getting vaccinated or even tested. This was confirmed also by a spokesperson for the Ministry of Defence who stated, "The pandemic has reinforced the disinformation narratives, so the Defence Ministry has intensified its strategic communications, whether on social networks or in the field. We also think exchanging information and experiences in the area of combatting hybrid threats and disinformation with our partners is essential" (Sirotnikova, 2020). For disinformation actors, the pandemic presented a great opportunity to increase their audience and with it, their influence.

This notion was confirmed by Daniel Milo, who said: "If you have a population that is prodded to distrust public officials or even to rebel against restrictive measures, you have basically achieved your strategic goal because the society is vulnerable, unstable, and any outside or even internal actor could utilise such a situation for their benefit" (Daniel Milo, online communication, August 2021). Kriššák also mentioned that what the government should have done in the first place was to "depoliticise the COVID-19 pandemic, it should not have been a subject of many press conferences coming from politicians, namely former prime minister Matovič. As a result, these politicised press conferences totally devalued trust in scientists and doctors." Nonetheless, there is an opportunity to learn from the poor management of strategic communication by "setting up processes that will not be subsequently cancelled or changed by other policy forces, and set up proper strategic communication processes, build technical-analytical capacities, and communication capacities" (Tomáš Kriššák, online communication, December 2021).

Since the approach of the former political leaders had left Slovakia's national security weak, unreflective of the current security environment, and open to several security challenges, such as vulnerability to Russian influence and disinformation threats, a much needed overhaul of the Security Strategy was needed. This much-needed change of approach came with the new government elected in 2020, which pledged to combat disinformation and hybrid threats as highlighted in the government's programme. For the Copenhagen School (Buzan et al.,1998) a securitising speech act essentially means "by saying the words, something is done" (p. 26).

The question remains, what does it mean when no one is saying anything? In this case, the public discourse directed by the prime ministers of Slovakia since 2014 until the most recent government was devoid of any mention of a threat, as there were no public statements regarding the threat of disinformation as a part of hybrid warfare, or what countermeasures were being built by the most relevant authorities.

Chapter 3 : How the Russian “Lie Machines” Create “Bear Huggers”

The term “lie machines” is used by Howard (2020) to characterise the nature of Russian disinformation campaigns, consisting of various automated parts such as bots, artificially created profiles on social media. Although the Russian disinformation “machine” has not been able to win the hearts and minds of the whole population of Slovakia, it has managed to enchant at least a portion of them, ensuring that these people are filled with negative emotions, such as confusion or frustration, towards their own values and public institutions. As Milo (2020) puts it, some Slovaks belong to the group of “bear huggers”, meaning people who express positive emotions and support towards Russia and its policies and dismiss any potential threat coming from their “big brother” (p. 9). The term “bear huggers” comes from this publication, and while it might be interpreted as a harsh criticism of pro-Kremlin oriented individuals and groups in Slovakia, it correctly captures the positive attitudes of a relatively significant part of the Slovak population.

The evidence of the effectiveness of the Russian disinformation campaign can be found by analysing public opinion polls on security related issues, done by Globsec. This work will utilise the relevant data collected from Globsec Trends throughout the period between 2018 and 2021 and analyse it in order to show how the Slovak audience was influenced by foreign disinformation actors in combination with local entities that helped spread false narratives. Pro-Russian narratives are a significant instrument in shaping public opinion in this region, and they are adequately supported, as will be demonstrated in this chapter.

The Copenhagen School’s theory implies that the audience, to which the securitising actor addresses the speech act, is inherently passive in the process of securitization, and their sole role in the process is to decide whether to acknowledge the existence of a threat or not. On this, Côté (2016) states that this view clashes directly with the empirical evidence of securitization processes. According to Côté, the evidence suggests that unlike what is stated in the theoretical literature, audiences, according to empirical evidence, are actually an active component of the process, as they can challenge the securitizing actor’s presentation of the threat, force the actor to suggest a new or modified security narrative or force the complete abandonment of the actor’s attempt at pursuing securitization (p. 6). The audience can also hold the securitising actor accountable for pursuing extraordinary measures without their consent and subsequently punish them by voting them out of office in the next elections. On the other hand, in some cases, the audience demands extraordinary measures from the competent actors, intensifying the urgency of the need to securitize a given threat.

According to Floyd (2016), the securitizing move might be interpreted in two ways. First, as a warning to an aggressor as the target of security actions, and then as a pledge to safeguard the referent object (p. 12). Moreover, there is a group of relevant security influencers, which, while not having the capacity to legitimise new security measures by themselves, can influence the communication and other interactions between the securitising actor and the audience. This distinction generates two unique audiences that can be addressed by securitizing moves in a single instance. As a result, academic research on the role and potential of audiences in securitization processes suggests that many audiences may exist within a single process, and that audiences frequently have various levels of power and influence, resulting in diverse consequences on securitization results.

Furthermore, Floyd (2016) proposes that revised theories of securitization would discard the outdated concept of audience acceptance, and instead put emphasis on security action. This security action can take the shape either of a specific policy change or "a change of behaviour by a relevant actor" (p. 8). What is more, Floyd proposes six possible scenarios of securitization based on empirical evidence, where the audience is often a relevant component in the process. His fifth scenario best reflects the attitude of the Slovak audience when it comes to the threat of disinformation, as it illustrates what might happen if the referent object (the audience) rejects the pledge of protection. This rejection then results in either “we are perfectly safe and not threatened at all or we may be threatened but we don’t think that you [the would-be securitizing actor] are the right actor to protect us” (p. 14).

Sarts (2021) argues that in order to conduct an influence campaign, a hostile actor must establish itself as a natural component of that environment. It helps to disguise these campaigns and achieve one of the essential criteria, going undetected. The majority of effective disinformation campaigns go unnoticed by society, and many players use this strategy. Additionally, foreign state agents might also go unnoticed by collaborating with local players who would benefit from such discourse. This strategy is successful because it is difficult to distinguish between a legitimate local group's reaction to an issue in the public discourse and an attempt by a hostile power to exploit a vulnerability in a given society to serve its interests.

Sarts (2021) also provides a detailed analysis of state actors that use disinformation as a part of influence campaigns, explaining how these actors exploit social weaknesses to disrupt a country's social cohesion, by using military and diplomatic means, "in conjunction with information space activities to achieve desired effects" (p. 23) . Although many of the tools used in hostile campaigns were developed during the height of the Cold War, there is a newer emphasis on exploiting opportunities created by the digital environment, such as organised trolling as a fundamental part of hostile social media campaigns or using automated bots to spread a given narrative to as many people as quickly as possible.

3.1 The "Hijacking" of Local Cultural Institutions by the Russian Lie Machines

Golianová and Kazharski (2020) in their article provide a valuable insight into how Slovak cultural institutions and local organisations have been hijacked for the purpose of spreading pro-Kremlin narratives which often contain disinformation. The disinformation campaign first identifies a major cleavage in society and constructs a narrative which supports the foreign policy of Russia while also benefiting domestic actors which build their influence more efficiently. In Slovakia the narratives these actors disseminate often target Western organisations like NATO or the European Union, of which Slovak Republic is a member, and provide an oversimplified image of incompetent evil overlords to the Slovak audience. On the other hand, it actively portrays Russia as a "desirable model and attainable alternative to Western liberal democracies". Furthermore, these narratives are not considered to be disinformation in and of themselves, but often contain disinformation. The article's biggest contribution is twofold. On one hand, it identifies local actors, such as the Russian-Slovak Society or The League of Anti-Fascist Fighters, who disseminate pro-Kremlin narratives often containing disinformation, and points out that these actors have been active within Slovakia for a quite a long time now.

For the purpose of gaining greater insight into the local disinformation actors, an interview with Kazharski was conducted. On the whole, Kazharski sees the situation in Slovakia as a "decentralised effort with many actors at play, with really bizarre marriages like the Slovak Anti-Fascist Union and fans of the wartime Slovak State" (Aliaksei Kazharski, online communication, August 2021). The reason why these two groups are subscribing and further spreading similar, if not identical, narratives might be because the message of one local disinformation actor can often align with the content of a different actor, as the practice of disseminating disinformation does not have a single doctrine. On the contrary, it is very organic and these actors are experimenting with their content, as some are using the leftover nostalgia of the Soviet Union, while others are using the fascist Slovak State.

Furthermore, there appears to be a symbiotic relationship between them, if not a degree of cooperation, as Kazharski noted: “They gravitate, they socialise, they support each other, there was an attack launched at us by members of the Russian-Slovak Society, which served as an example of the solidarity between these pro-Kremlin disinformation actors.” While it could not have been possible to prove for certain that the disinformation operations on a local level in Slovakia are being run from the Kremlin, Kazharski said he “would not be surprised if there was outside coordination” (Aliaksei Kazharski, online communication, August 2021).

As most disinformation narratives aim to promote the success of Kremlin's policies and simultaneously dismiss any criticism towards Russia, according to Kazharski, pro-Kremlin disinformation actors adopt a strategy to “counter and undermine criticism by relativising whataboutism: if someone says something critical about Kremlin, these actors can quickly point to the West and its imperfect policies. There is no truth in this world, only different narratives, and there is no moral truth. Confusion in the cognitive sense and relativisation in the normative sense is planted into the minds of the audience targeted by disinformation, conditioning them into believing that there is no benchmark and everybody is evil” (Aliaksei Kazharski, online communication, August 2021).

However, without the consensus between disinformation actors on what objective reality is, there are many inconsistencies within the narratives these actors are disseminating. One shared component of the majority of disinformation is the portrayal of the “West” as an enemy, nevertheless, even in this framework there are ideological narratives which might contradict the narratives of other actors. According to Kazharski, inconsistencies can be found even in the strategic narratives spread by state-funded television network Russia Today (RT), “Something which would not happen during communism, where the party had one consistent ideological line” (Aliaksei Kazharski, online communication, August 2021). Even though Dr. Kazharski is from an academic background and is not directly connected with policy-making, when asked about possible countermeasures or approaches which would help against the influence of strategic narratives, he replied:

> “Blocking disinformation is a hard path to take in this day and age, and if you cannot block it you have to engage with it, that would include fact-checking activities, and you have to launch a counter-narrative. If you have a disinformation campaign showing that the EU is evil, then you have to launch a public campaign showing the benefits which Slovakia enjoys as a member of the EU” (Aliaksei Kazharski, online communication, August 2021).

3.2 GLOBSEC Trends

3.2.1 GLOBSEC Trends 2018

The year 2018 in Slovakia was marked by unprecedented belief in conspiracy theories and disinformation narratives in comparison with other countries of the Visegrad Four. Globsec Trends for the year 2018 found that the majority of Slovaks (53%) believe in conspiracy theories. The research found that Slovakia is the only country in Central Europe where the majority of respondents believe that world events are decided by hidden organisations seeking to establish a totalitarian world system rather than by publicly elected authorities. Anti-Semitic conspiracy theories are likewise supported by the majority of Slovaks (p. 30). While 68% of Slovaks aged 18-24 years encountered disinformation on social media, only 9% of social media users report it (p. 11). On this Daniel Milo, one of the leading experts on disinformation in Slovakia and co-author of Globsec Trends, said in an interview, “If you have a population which is prone to believe in conspiracy theories then disinformation can have a more severe impact” (Daniel Milo, online communication, August 2021). As was mentioned above, Slovak social media users are encountering disinformation, and a significant part of these users are prone to believe false narratives, disinformation actors can use these factors to set up operations to shift public opinion on strategic matters such as membership in NATO.

A particularly disturbing finding comes with the question whether neutrality would provide better security than NATO membership. When it comes to the topic of NATO membership, Pro-Kremlin narratives achieved a major achievement in 2018, when almost half of Slovak respondents of Globsec Trends (47%) replied that they would prefer Slovakia being neutral than being a member of NATO. According to Šuplata (2018) this is one of the primary narratives intended at weakening public support for NATO membership (p. 9). What's more, in the same year, Slovaks showed the strongest sympathy for Putin and his policies, continuing a long-standing trend of being the most pro-Russian country in V4. This favouritism was also reflected: 50% of Slovaks reject Russian military presence in Ukraine, while one third does not believe that the conflict in Ukraine continues due to the presence of Russian forces on the ground (Globsec Trends, 2018, p. 29).

As Klingová & Hajdu (2018) observes, disinformation narratives were frequently taken up and promoted by various far-right local extremist organizations and political parties; unfortunately, since then this practice also penetrated into the mainstream political core in Slovakia. Furthermore, owing to linguistic and cultural closeness, a free flow of disinformation narratives between various Czech and Slovak sources was recognized (p. 40). Moreover, Klingová & Hajdu highlight in their report possible warning signs of existing symbiosis between disinformation outlets and political elite of Slovakia, where the politicians defend the credibility of information gained from said sources, which might signal to their audience that it is a source of legitimate information same as mainstream or even investigative media (p. 40). Klingová (2019) further develops the influence of the marriage between politicians and disinformation actors in the eyes of regular citizens. In her work, she shows yet another category where Slovakia is an outlier, namely, the phenomenon where there is a direct correlation between the belief in conspiracy theories and higher education levels (para. 7). While there are many independent and dependent variables at play, such as the degree of media literacy of an individual, that might have influence over why this phenomenon exists, one of the explanations offered by the author herself, is that "Slovaks believe all the messages that their political representatives spread" (para. 8). The ordinary people are then exposed to disinformation not only from foreign and local disinformation outlets but also from their own elected officials, from which they do not expect to be deceived.

3.2.2 GLOBSEC Trends 2019

In the successive year, Slovak respondents of Globsec Trends 2019 maintained their views, and the trend of being among the most pro-Russian countries in the Visegrad Four continued. Here the authors attributed the endurance of the trend to the notion of pan-Slavism and anti-

American sentiment (p.29). Slovaks, among other societies belonging to "bear huggers", have strong historical, cultural, and ethnic links with Russia, which creates favourable views and a strong sympathy for the Kremlin and its policies. One of the most significant historical and ethnic links is the concept pan-Slavism, which advocates the union of all Slavs organised into one political body ruled by Russia. Golianová and Kazharski (2020) discuss that pan-Slavism has a strategic place within disinformation narratives because “Slovak pan-Slavists tend to see Russia as the natural ‘core’ of the Slavic world and ignore the actual conflicts and divisions between individual Slavic nations” (p. 9). On the other hand, Anti-Americanism, while being a newer concept than pan-Slavism, is already deeply rooted in Slovakia, a consequence of 40 years of communist propaganda paired with deeply established pro-Russian sympathies. This attitude is sustained by current disinformation operations and narratives, resulting in 41% of Slovaks believing the US, not Russia, constitutes a significant threat to their nation, by far the most in the area (Globsec Trends 2019, p. 11).

3.2.3 GLOBSEC Trends 2020

Russia has managed to project its desired image into the consciousness of the Slovak audience. It has done so by using the legacy of communism amplified by its current "lie machines" of media influence. As Kandrík & Jevčák (2018) rightly point out, Kremlin is taking a substantial risk of backlash when it comes to narratives working with the shared communist past, as in case of Slovakia, it evokes not merely nostalgia but also “negative memories of occupation” (p. 3). There are safer options for the Kremlin's lie machine to take, for example the conservative nature of Slovak society or the country's heavy dependency on Russian resources, such as oil and gas. Nonetheless, the Slovak audience seems to continue to subscribe to the two most common narratives of disinformation outlets, first being that Russia is a Slavic brother, and second, that Russia is a military superpower wrongfully vilified by the West. Specifically, 78% of respondents think that, “Russia is my country’s traditional Slavic sister/brother nation” and 50% of respondents replied saying, “Western countries often unjustly accuse Russia of unlawful or fraudulent behaviour” (p. 39). Furthermore, the victimisation narrative, which lays the responsibility for all wrongdoings is fully on the shoulders of the West and NATO, finds a receptive audience and growing acceptance in Russophile countries like Slovakia. Similarly, the idea that they have a shared Slavic origin with Russia is also popular among the general public.

Based on one of the most recent and insightful articles on the image of Russia in Slovakia, written by Milo (2021), it can be argued that Slovak audience in the securitization process would, with high probability, not accept the Russian disinformation operations as a threat because a majority of the population would still not regard Russia as a security challenge. One of the most significant findings of this study was that 56% of participants responded that they do not feel threatened by Russia. As Milo claims, most respondents justify their beliefs by stating that their country is “too small to pose a threat to Russia or that Slavic links and heritage will discourage Moscow from engaging in hostile acts" (p. 6). In short, the combination of these factors makes a powerful narrative about Russia being an outcast, wrongfully convicted of transgression, allowing the genuine perpetrators, embodied by Western superpowers and organizations, to evade accountability. This story is then disseminated through communication networks and social media in order to sabotage efforts to fully Westernize the country. If the majority of people in the region do not perceive Russia as a threat, successful securitization will be impossible, as acceptance of an existential threat is the most basic prerequisite, as set out by the Copenhagen School.

Conclusion: Small Steps for a Government, One Giant Leap for Slovakia

Securitization, even according to those in the Copenhagen School who framed the concept, is perceived negatively, as a mechanism by which security needs are used as a pretext by state actors to acquire more power, or the freedom to act with less accountability, which has the same result. Nonetheless, it can be argued that securitization can fulfil a useful role when it comes to addressing certain threats, in part, because it allows the state to identify a genuine threat that might otherwise be dismissed or ignored. Disinformation is one such threat. Securitization is justified in this case because the state lacks other effective responses and, without securitization, the security of the state might genuinely be undermined.

Disinformation is designed to disrupt the objective reality of an individual and, if enough people are influenced, to make coexistence in a shared society extremely difficult. The degree of harm is only determined by the willingness of actors to securitize disinformation, and by the susceptibility of the general public to disinformation. As such, the author believes that disinformation represents a threat sufficient to justify the use of the securitization act by the securitization actor. While the countermeasures created by the government can be effective, the processes by which they are created are time-costly, and with the former governments of Slovakia neglecting to develop security measures towards these threats, time is of the essence. As such, the act of securitization as applied in this work provides a path in which a securitising actor has to possess power outside of normal bounds to counter hybrid threats promptly. Nevertheless, future researchers will need to determine what security measures are ‘out of bounds' when it comes to the threat of disinformation.

Widespread, but institutionally ignored, strategic narratives that target specific groups of people, using social media platforms and their algorithms as brokers, can result in the erosion of established values and a regression in democracy. The security risk which lies in disinformation operations was heavily underestimated: a consequence of either a poor assessment of, or complete ignorance of, the threat. The government's inactivity meant that the presence of foreign influence operations was not properly communicated, despite NGOs, think tanks, and traditional media outlets releasing publications providing evidence that these operations are not only real but very active. Nonetheless, non-governmental agents do not possess the same apparatus as the government to successfully securitize a given liability. This is reflected in strategic documents published by the Ministry of Defence, and in public statements by politicians before 2020, both of which used vague language while describing hybrid warfare and were hesitant to identify Russia as an aggressive actor possessing these instruments or their possible deployment on Slovak territory.

In the first chapter, the strategic documents of the Slovak Republic were reviewed from the period marked by the start of the conflict in Ukraine in 2014 and ending with the ongoing COVID-19 pandemic in 2021. This analysis showed that the perception of the threat of disinformation operations changed only in 2020, when a new government took over. The passivity of the previous governments towards hybrid threats, stemming from their geopolitical preferences, resulted in Slovakia having no institutionalised measures which would actively increase the public's resilience or in having security measures that possessed highly exploitable weaknesses. While the approach of the current government was praised initially, experts within the field remain cautious, as the result of the next election will dictate whether Slovakia continues to build up security measures against hybrid warfare or reverts back to the state it was before 2020. Both of these scenarios are possible since strategic documents can be altered with the coming of a new government. Thus, it remains to be seen to what extent these measures will last in the future.

As was shown in the second chapter, there was no political will to increase security regarding hybrid threats by the political elite until very recently. One exception is the former President of Slovak Republic, Andrej Kiska, who took the threat of hybrid tools of warfare from the side of Russia seriously, and even though his office does not possess the power necessary to evoke the securitization act, as dictated by the Slovak Constitution, he used his office to bring attention to the issue. The same cannot be said about other high politicians such as Robert Fico or Andrej Danko, whose personal geopolitical attitudes, which are not consistent with the geopolitical affiliation of the Slovak Republic, led them to adopt a stance of wilful ignorance towards the threat presented by hybrid warfare. Even with the coming of the new government, there remains comparably little political will to regulate social media networks, which are used to spread disinformation and conspiracy narratives but are also the main channels for political advertising, and thus indispensable to politicians. Therefore, the political elites of Slovakia are largely unwilling to regulate social media as their support to a significant degree depends on them. Furthermore, the topic of regulation does not generate much political interest, much less support.

The third chapter provided evidence of how successful disinformation actors are within

Slovakia. Based on a combination of its history, unconvincing political communication, and fragile democratic heritage, Slovakia has become fertile ground for Russia-centric, pan-Slavist disinformation narratives. As a result, Slovaks are more prone to trusting disinformation than their neighbours in the V4. Thus, even if the securitizing actor did call for the building of defences against the threat of Russian hybrid warfare, a significant part of the population would rebel against such measures, not because of the fact that the actor doing the securitization would get more power, but because they believe that Russia would never threaten another Slavic nation, much less Slovakia.

To improve the resilience of its people towards disinformation, it is vital for Slovakia to improve the strategic communication channels that connect government and citizens. Failing to implement effective countermeasures against disinformation, even by the use of securitization, may have even worse consequences than giving a state securitization actor more power. Nevertheless, for that, it is imperative to increase the general public’s awareness of the threat. As was shown in this thesis, with Slovaks being one of the strongest supporters of Russia among Central European countries, both on the political and individual level, we can observe that pro-Kremlin disinformation operations have succeeded at sowing confusion and anti-West narratives to weaken public support for typically Western organisations, such as NATO. Slovakia needs to significantly step up its fight against hybrid threats.

This can be done by adopting an approach in which the government would actively seek reliable ways to boost resilience against disinformation among the entire population and not just focus on protecting individual ministries or other government agencies. They could do this by reforming the education curriculum to include media literacy, and finally, by pushing for regulation of the social networks that operate within Slovakia. There is a chance to reverse the damage done by passive actors in the past, and change Slovakia from a “breeding ground of disinformation” to a more secure environment in which pluralist democracy and freedom of speech is less easily abused for sinister intentions, and instead might thrive.

Resumé

Cieľom tejto práce je preskúmať reakcie slovenskej vlády na dezinformačné operácie v rámci hybridnej vojny zo strany cudzích mocností, ako je Ruská federácia. Práca kladie dôraz na dezinformácie práve preto, že ako informačné hrozby môžu byť nasadené do informačnej sféry akéhokoľvek štátu, hlavne v čase globálnych sociálnych sietí. Táto práca pracuje s hypotézou, že hrozba dezinformácii nebola až donedávna prioritou vlády Slovenskej republiky a taktiež nebol uskutočnený ani pokus sekuritizovať túto hrozbu.

Prehľad literatúry v prvom rade definuje pojem dezinformácia v kontraste s často zameniteľnými pojmami ako misinformácie alebo propaganda. V jazyku KGB (bývalej tajnej spravodajskej služby Sovietskeho zväzu) dezinformácie znamenajú ideologickú subverziu daného obyvateľstva s cieľom oslabiť sociálnu súdržnosť a následne vytvoriť skupinu ľudí zastupujúcu záujmy aktéra. Ten môže ďalej využiť polarizovanú spoločnosť na rôzne strategické a politické účely.

Okrem prehľadu o tom, čo sú to dezinformačné kampane a ako fungujú, táto časť taktiež uvedie sekuritizáciu ako stratégiu, ktorú možno použiť na boj proti dezinformáciám ako o jednom z typov reakcií štátov voči tejto hrozbe. Práve pri použití procesu sekuritizácie je možné rýchlo vytvoriť bezpečnostné opatrenia, ktoré sú miestami až zúfalo potrebné.

V prvej kapitole boli zhodnotené strategické dokumenty SR z obdobia poznačeného začiatkom konfliktu na Ukrajine v roku 2014 a končiac prebiehajúcou pandémiou COVID-19 v roku 2021. Táto analýza ukázala, že vnímanie dezinformácii ako hrozby sa zmenilo až v roku 2020, keď nastúpila nová vláda, ktorá hneď obnovila strategické dokumenty aby zahŕňali aj hybridné hrozby ako dezinformácie. Zatiaľ čo prístup súčasnej vlády bol spočiatku veľmi optimisticky hodnotený, odborníci v tejto oblasti zostávajú opatrní, pretože výsledok najbližších volieb určí, či bude Slovensko pokračovať v budovaní bezpečnostných opatrení proti nástrojom hybridnej vojny, alebo sa vráti do stavu pred rokom 2020. Tieto scenáre sú možné, keďže strategické dokumenty sa môžu s príchodom novej vlády zmeniť.

Ako sa ukázalo v druhej kapitole, politická elita až donedávna nemala politickú vôľu zvýšiť bezpečnosť ohľadom dezinformácii. Vysoko-postavení politici ako Robert Fico či Andrej Danko zámerne ignorovali prezentovanú hrozbu zo strany Ruska vďaka svojím osobným

geopolitické postojom. Výnimkou je bývalý prezident SR Andrej Kiska, ktorý bral hrozbu hybridných nástrojov vedenia vojny zo strany Ruska vážne, a hoci jeho úrad nedisponuje potrebnou právomocou na vyvolanie sekuritizačného aktu. Niektorí experti stále tvrdia, že aj po nástupe novej vlády zostáva malá politická vôľa regulovať sociálne siete, ktoré sa využívajú na šírenie dezinformácií a konšpiračných naratívov, no zároveň sú aj hlavnými kanálmi politickej reklamy, a preto sú pre politikov nevyhnutné. Politické elity Slovenska preto nie sú vo veľkej miere ochotné regulovať sociálne médiá, ako jeden z možných výstupov sekuritizácie, keďže ich politická podpora do značnej miery závisí od ich propagácie na sociálnych médiách. Okrem toho, samotná téma regulácie nevyvoláva veľký politický záujem, čo by znamenalo o to menšiu verejnú podporu.

Tretia kapitola priniesla dôkazy o tom, akí úspešní sú dezinformační aktéri na Slovensku. Na základe kombinácie svojej histórie, nepresvedčivej politickej komunikácie a krehkého demokratického dedičstva sa Slovensko stalo úrodnou pôdou pre rusko-centrické panslavistické dezinformačné naratívy. V dôsledku toho sú Slováci náchylnejší veriť konšpiračným teóriám a dezinformáciam ako ich susedia vo V4. Ak by teda sekuritizačný aktér skutočne vyzval na vybudovanie obrany proti hrozbe ruskej hybridnej vojny, značná časť obyvateľstva by sa proti takýmto opatreniam vzbúrila, nie preto, že by aktér, ktorý vykonáva sekuritizáciu, získal väčšiu moc, ale preto, že veria, že Rusko by nikdy neohrozilo iný slovanský národ, tým menej Slovensko.

Výsledky naznačujú, že pre pasivitu štátu sa Slovensko stalo úrodnou pôdou pre dezinformácie, a preto môže byť potrebný proces sekuritizácie na rýchle vybudovanie dostatočných protiopatrení. Aj keď je sekuritizácia odborníkmi vo všeobecnosti vykresľovaná veľmi negatívne, táto práca sa zasadzuje za pozitívnejšie poňatie tohto fenoménu v prípade dezinformácií, keďže môže ísť o efektívny prístup k vytváraniu politík na boj proti šíreniu strategických naratívov nepriateľského aktéra. Pasivita predchádzajúcich vlád voči hybridným hrozbám, vyplývajúca z ich geopolitických preferencií, viedla k tomu, že Slovensko nemá inštitucionalizované opatrenia, ktoré by aktívne zvyšovali odolnosť verejnosti, alebo bezpečnostné opatrenia s vysoko zneužiteľnými slabinami.

References

Aradau, C., (2004). Security and the democratic scene. *Journal of International Relations and Development, p.*388–413.

Buzan, B., Wæver, O., De Wilde, J., (1998). *Security: A new framework for analysis*. London: Lynne Rienner Publishers.

Cerny, D. (2014). *Na Ukrajine Ide O Propagandistickú vojnu, tvrdí Fico*. Pravda.sk. Retrieved from https://spravy.pravda.sk/domace/clanok/329117-na-ukrajine-ide-o-propagandisticku-vojnu-tvrdi-fico/

Cuprik, R. (2019). *Disinformation Hunter: Slovakia is in a hybrid war*. spectator.sme.sk. Retrieved from https://spectator.sme.sk/c/22216183/disinformation-hunter-slovakia-is-in-a-hybrid-war-blbec-online-website-facebook.html?ref=av-center

Defence Strategy of the Slovak Republic (2021), Assessed from https://www.vlada.gov.sk/data/files/8049_obranna-strategia-sr-2021.pdf

Derakhshan, H., & Wardle, C. (2018). Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information. In *Journalism, 'Fake News' and Disinformation* (pp. 43-54). UNESCO. Accessed from https://en.unesco.org/sites/default/files/f._jfnd_handbook_module_2.pdf

Fabok, M. (2020, April 8). *Korcok: Fight Against Fake News Can't Fall to Foreign Ministry Alone*. Retrieved from https://newsnow.tasr.sk/foreign/korcok-fight-against-fake-news-cant-fall-to-foreign-ministry-alone/

Galeotti, M. (2016). *'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't*. E-International Relations. Retrieved from https://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/

Golianová,V. & Kazharski, A. (2020), '*The Unsolid'. The RUSI Journal,* DOI: 10.1080/03071847.2020.1796521

Gregor M., Mlejnková P. (2021). *Challenging Online Propaganda and Disinformation in the 21st Century: Political Campaigning and Communication*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-58624-9_2

Hajdu et al. (2020) *Globsec Trends 2020*, GLOBSEC Policy Institute, available at: https://www.globsec.org/publications/globsec- trends-2020/

Hajdu, D., Klingová, K. & Milo, D. (2018), GLOBSEC Trends 2018, GLOBSEC, available at: https://www.globsec.org/wp-content/ uploads/2018/05/GLOBSEC-Trends-2018.pdf

Hellman, M. & Wagnsson, C. (2017) *How can European states respond to Russian information warfare? An analytical framework*, European Security, 26:2, 153-170, DOI: 10.1080/09662839.2017.1294162

Howard, P. (2020). *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots,* *Junk News Operations, and Political Operatives*. New Haven: Yale University Press. https://doi.org/10.12987/9780300252415-002

Kandrík, M., & Jevčák, M. (2018). *Unprepared and vulnerable: The resilience of the Slovak republic to foreign, foremost Kremlin-led disinformation campaigns*. Retrieved from https://www.stratpol.sk/wp-content/uploads/2018/06/PP-DRI-Final.pdf

Klingová, K. (2019). *Which Slovaks Believe in Conspiracy Theories?* Retrieved from https://www.globsec.org/2019/02/27/which-slovaks-believe-in-conspiracy-theories/

la Cour, C. (2020). *Theorising digital disinformation in international relations*. *Int Polit* 57**,** 704–723. https://doi.org/10.1057/s41311-020-00215-x

Mahairas, A., & Dvilyanski, M. (2018). Disinformation – Дезинформация (Dezinformatsiya). *The Cyber Defense Review*, *3*(3), 21–28. https://www.jstor.org/stable/26554993

Merriam-Webster. (n.d.). Disinformation. In *Merriam-Webster.com dictionary*. Accessed from https://www.merriam-webster.com/dictionary/disinformation

Milo, D. & Klingová, K. (2017). *The vulnerability index: Subversive Russian influence in Central Europe*. Globsec Policy Institute.

Milo, D. (2021). *The image of Russia in Central & Eastern Europe and the Western Balkans Russia: Mighty Slavic Brother or Hungry Bear Next-door?* Retrieved from https://www.globsec.org/wp-content/uploads/2021/04/Image-of-Russia-Mighty-Slavic-Brother-or-Hungry-Bear-Nextdoor.pdf

Milo, D., Klingová, K. & Hajdu, D. (2019), *GLOBSEC Trends 2019,* GLOBSEC Policy Institute, available at: https://www.globsec.org/publications/globsec-trends-2019/

The Ministry of Defence of the Slovak Republic. (2021). *MOD presents action plan for coordination of fight against hybrid threats to experts at Globsec*. Retrieved from https://www.mosr.sk/49526-en/rezort-obrany-predstavil-expertom-na-globsecu-akcny-plan-koordinacie-boja-proti-hybridnym-hrozbam/

Ministry of Investments, Regional Development and Informatization of Slovak Republic. (2021). *Ministerka Remišová: Boj proti dezinformáciám a informačnú gramotnosť podporíme novou výzvou v hodnote 120-tisíc eur*.Retrieved from https://www.mirri.gov.sk/aktuality/digitalna-agenda/ministerka-remisova-boj-proti-dezinformaciam-a-informacnu-gramotnost-podporime-novou-vyzvou-v-hodnote-120-tisic-eur/

Nemr, C., & Gangware, W. (2019). *Weapons of mass distraction: Foreign state-sponsored disinformation in the digital age*. Park Advisors.

Office of the President of the Slovak Republic. (2017). *Declaration by the President, Speaker and Prime Minister on the EU and NATO*. Retrieved from https://www.prezident.sk/en/article/vyhlasenie-prezidenta-predsedu-narodnej-rady-a-predsedu-vlady-k-eu-a-nato/

Özcan, S. (2013). *Securitization of energy through the lenses of Copenhagen School*. *West East*

Journal of Social Sciences. Vol.2. No.2; Paper prepared for the 2013 Orlando International Conference, 21-23 March, 2013, West East Institute, Orlando/USA.

Rauch, J. (2021). *The Constitution of Knowledge: A Defense of Truth*. Brookings Institution Press. http://www.jstor.org/stable/10.7864/j.ctv13qfw2t

Rechtik, M., & Mareš, M. (2021). *Russian Disinformation Threat*: Comparative case study of Czech and Slovak approaches 1. Journal of Comparative Politics, 14(1), 4-19.

Rid, T., (2020), *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux. ISBN: 9780374287269

Ridder, H.-G. (2012). [Review of *Case Study Research. Design and Methods 4th ed.*, by R. K. Yin]. *Zeitschrift Für Personalforschung/German Journal of Research in Human Resource Management*, *26*(1), 93–95. http://www.jstor.org/stable/23279888

Roe, P. (2012). *Is securitization a 'negative' concept? Revisiting the normative debate over normal versus extraordinary politics*. Security Dialogue, 43(3), 249–266. https://doi.org/10.1177/0967010612443723

Sarts, J. (2021) *Disinformation as a Threat to National Security*. In: Jayakumar S., Ang B., Anwar N.D. (Eds.) *Disinformation and Fake News* (pp. 23-33). Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-15-5876-4_2

Sirotnikova, M. G. (2020). *Pandemic pushes Slovakia to finally target disinformation*. *Balkan Insight*. Retrieved from https://balkaninsight.com/2020/10/20/pandemic-pushes-slovakia-to-finally-target-disinformation/

SITA. (2015). *Rusko Stratilo dôveru, Kiska Vyzval úniu K Upevneniu Sankcií*. Webnoviny.sk. Retrieved from https://www.webnoviny.sk/rusko-stratilo-doveru-kiska-vyzval-uniu-k-upevneniu-sankcii/

SITA. (2017). *Kiska: Slovensko v Boji Proti hybridným hrozbám Nerobí Takmer nič*. Retrieved from https://domov.sme.sk/c/20484726/kiska-slovensko-v-boji-proti-hybridnym-hrozbam-nerobi-takmer-nic.html

SITA. (2020). *Strategické Dokumenty Počkajú na Novú vládu, postoj SNS UŽ Pellegrini Komentovať Nechce*. SME. Retrieved from https://domov.sme.sk/c/22293394/pellegrini-strategicke-dokumenty-pockaju-na-novu-vladu.html

Sitko, A. (2021,. *Fico má nového spojenca - dezinformačnú scénu*. Antipropaganda.sk. Retrieved from http://antipropaganda.sk/fico-ma-noveho-spojenca-dezinformacnu-scenu/

Slovak Information Service, 'Správa o činnosti SIS za rok 2019' ['Activity Report 2019'], (2020), Accessed from http://www.sis.gov.sk/ pre-vas/sprava-o-cinnosti.html

SME.sk (2018) *The ruling coalition puts Slovakia in jeopardy, opposition says*. The Slovak Spectator. Retrieved from https://spectator.sme.sk/c/20972289/the-ruling-coalition-puts-slovakia-in-jeopardy-opposition-says.html

SME.sk. (2019). *Slovakia still unable to react to current security threats*. The Slovak Spectator.

Retrieved from https://spectator.sme.sk/c/22220592/slovakia-is-unable-to-react-to-hybrid-threats-globsec-report.html

Struhárik, F. (2020). *Štát Predstavil Svoj Prvý Plán na Boj proti hoaxom. Remišová má pripraviť nástroj na ich monitoring*. Denník N. Retrieved from https://dennikn.sk/2128471/stat-predstavil-svoj-prvy-plan-na-boj-proti-hoaxom-remisova-ma-pripravit-nastroj-na-ich-monitoring/

Szekeres, E. (2021). *Slovakia grapples with the 'big business' of disinformation*. Balkan Insight. Retrieved from https://balkaninsight.com/2021/08/05/slovakia-grapples-with-the-big-business-of-disinformation/

Šnídl, V. (2017). *Štát prvýkrát priznal, že ruská propaganda útočí na prozápadné smerovanie slovenska*. Denník N. Retrieved from https://dennikn.sk/481082/stat-prvykrat-priznal-ze-ruska-propaganda-utoci-prozapadne-smerovanie-slovenska/

Šnídl, V. (2018). *Danko Prinútil koalíciu stiahnuť Strategické Dokumenty, Ktoré Označujú Rusko Za Hrozbu*. Denník N. Retrieved from https://dennikn.sk/1308036/danko-prinutil-koaliciu-stiahnut-strategicke-dokumenty-ktore-oznacuju-rusko-za-hrozbu/

Šuplata, M. & Nič, M., (2016). *Russia's Information War in Central Europe*. GLOBSEC Policy Institute.

TASR. (2015). *Prezident: Musíme Byť pripravení Na roky nestability*. TERAZ.sk. Retrieved from https://www.teraz.sk/slovensko/prezident-kiska-globsec-prihovor/141585-clanok.html?utm_source=teraz&utm_medium=organic&utm_campaign=click&utm_content=.%253Bsearch

TASR. (2021). *Parliament Passes Slovakia's First New Security Strategy in 16 Years*. Retrieved from https://newsnow.tasr.sk/policy/parliament-passes-slovakias-first-new-security-strategy-in-16-years/

Tóda, M. (2015). *Fico v Moskve Zabudol Na Vojnu na Ukrajine AJ Krym*. Denník N. Retrieved from https://dennikn.sk/127916/fico-v-moskve-zabudol-na-vojnu-na-ukrajine-aj-krym/