Adapt

Security Academy

YOUTH ON SECURITY

Security Academy Essays

This publication is supported by the Ministry of Defence of the Slovak Republic and Friedrich-Ebert-Stiftung in Bratislava. The authors of each essay are solely responsible for the content of their contribution to this publication. Opinions expressed in this publication do not purport to reflect the opinions or views of Adapt Institute or donors of this publication.

Adapt Security Academy - Youth on Security
March 2023

ABOUT PUBLICATION

You are about to read the collection of essays written by young aspiring professionals, who have spent the last five months attending the Security Academy. Security Academy is an educational project of the Adapt Institute and the European Values Center for Security Policy. It has been implemented from October 2022 to March 2023 under the auspices of the Minister of Defence of the Slovak Republic Jaroslav Naď and in cooperation with Friedrich Ebert Foundation Office in Slovakia. Apart from attending regular online lectures led by distinguished experts in defence and security policy, the twelve students have also taken part in study trips to gain first-hand experience in working in security related fields. Additionally, they have been assigned their very own mentor, under which supervision they have been gaining knowledge on particular topics of their interest. Essays included in this publication are the outcome of this mentoring program.

This project would not have been possible without the kind support of the aforementioned partners, to whom the Adapt Institute expresses honest gratitude. Additionally, many thanks to all of the lecturers and mentors, who have dedicated their precious time and shared their know-how and many years of experience with our students. Last but not least, it is important to take a moment to appreciate the students of this year's Academy. For the future of democracy, it is crucial that the young generation is involved and engaged in relevant educational activities and is aware of the challenges that are now threatening our democratic values and system as such. Security and prosperity go hand in hand. Therefore Adapt believes that involving these young people and opening the door to Slovak security and defence community for them will contribute to their professional lives as well as to Slovakia priorities in general.

TABLE OF CONTENTS

THE ROLE OF WESTERN POWERS AND THE UNITED NATIONS IN RESOLVING THE SYRIAN CONFLICT

Ančinová Annamária, expert consultant: Židuliaková Daša

EXECUTIVE SUMMARY

The conflict in Syria is a proxy war, with various powers pursuing regional interests. This essay will analyze the ongoing civil war in Syria and explore the reasons behind the international community's inability to take forceful action. The Western powers and the UN are considered to be key stakeholders in maintaining peace, stability, and democracy. Many states have become involved in this national conflict, yet the hostilities continue and have had disastrous humanitarian, economic and other severe consequences.

INTRODUCTION

In March 2023, Syria will enter its 12th year of civil war. This essay will argue why the international community seems to be at an impasse on Syria and why the United Nations Security Council has not adopted any forceful resolution yet. Firstly, we will explain all the geopolitical reasons for this long-lasting conflict and the interest of the international community. Secondly, we draw on the role of the United Nations Security Council. Furthermore, the question stays if the international norm called Responsibility to Protect[1] should be used and under what circumstances. Finally, we provide a summary, recommendations, and results of the issue investigation.

The uprisings in Daraa and Damascus erupted in March 2011, quickly resulting in a conflict of global dimension. The conflict in Syria represents one of the major conflicts since the Cold War. Syria has been in a proxy war since its outbreak. It is a war in which two or more powers use third parties

[1] The Responsibility to Protect or R2P is a global political commitment adopted by the United Nations at the 2005 World Summit to address the concerns of preventing war crimes, ethnic cleansing, genocide, and crimes against humanity.

to confront each other and advance their regional interests. Russia, the United States, Iran, Turkey, China, and Saudi Arabia are either trying to become a regional power and gain a leading role over the country or are attempting to keep their distance while being cautious that any foreign movement in the region does not gain influence over the post-Assad establishment. Ultimately, the Syrian conflict has had terrible humanitarian repercussions, affecting millions and causing great human misery. Other regional and international effects of the conflict include the emigration of refugees, heightened hostility between regional countries, and the development of extremist ideas. Almost 12 million Syrians still need food aid due to the conflict's widespread food insecurity. The destruction of infrastructure, livestock, and crops has limited production, delivery, and access to food (IFCR 2021).

The Syrian conflict has caused the largest refugee crisis since World War II. According to the latest World Bank data, 21 million people have been displaced in Syria's 12 years of conflict. This number represents half the total population, including internally displaced persons and refugees. Since the conflict began, the country's GDP has fallen by more than half, and the social and economic consequences of the conflict have been steadily growing (World Bank 2022).

The international community found itself in a political deadlock where it could not resolve the crisis in Syria, and many international actors continue to claim the failure of the UN Security Council. It is interesting to study this case, as it has shown the limits of the United Nations Security Council (UNSC).

UN SECURITY COUNCIL PARALYSIS

The paralysis in the UNSC is perhaps most easily explained by looking at the example of two opposing members of the UNSC - the United States and the Russian Federation. As a result of their divergent interests and views, they cannot reach a solution. Both countries are members of the Permanent Five (P5) of the UNSC. Therefore, they have the power of veto (Philips 2018). Their inability to solve this crisis satisfactorily leads to a stalemate. However, what are their differences, and why is there no unified approach?

Let’s draw on the reasons why Russia is vetoing the UNSC resolutions. Firstly, there are plans to build a gas pipeline between Qatar and Europe across Syria and Turkey. In 2009, Qatar drafted plans to build a gas pipeline from Doha to Istanbul. Due to its geographical position, Syria has both gas and oil reserves. The country has a crucial geographic position in supplying gas to Europe without Russian interference. Thus, if this pipeline connection were established, Europe's dependence on Russian gas supplies would be reduced. Meanwhile, even China is keeping a low profile in this conflict. However, Russia takes a firm stance in supporting Syrian President Bashar al-Assad. Secondly, it is crucial to mention that Russian policy in Syria is influenced by events in Libya. Russia is concerned that Syria will become a second Libya, where they agree with the resolutions to protect the population, yet they see the regime being overthrown. The Russians fear that allowing the resolution calling for sanctions to pass will lead to the overthrow of the regime and increase Western influence in the region (Allison 2013).

PRESSURE ON WESTERN POWERS

On the other hand, the US has completely different interests in Syria. The US was initially supportive of the opposition against president Assad. However, after the involvement of groups designated by the US as terrorists, such as ISIS, Washington withdrew its support for the opposition. Furthermore, the US has repeatedly expressed its criticism of the actions taken by Assad against the population. Yet why should the US speak out against the regime in Syria when it is a sovereign state? According to Weiler's theory, Washington has sought regime change in Syria since 2009 for geopolitical reasons and its gas supplies (Weiler 2014).

Another important stakeholder is undoubtedly the European Union. Syria is a key factor of regional stability for the European Union, as it is a transit country between Europe and the Middle East. In addition, before the conflict, the European Union and Syria had agreements that were beneficial to both sides. In terms of trade, the two political actors were close. In 2010, the EU was the largest trading partner of Syria. Within this trade, it is important to note that Syria mainly depends on the EU for its oil exports, which accounts for almost all of Syria's exports to the EU (92.1%), particularly to Germany, Italy, and France (Tejero 2022).

The influx of refugees in 2015 pressured economies, infrastructure, natural resources, security forces, and policies within the European Union states. In cooperation with United Nations agencies, European Union governments have ensured the provision of humanitarian assistance and the maintenance of stability. The European Union has provided most of the humanitarian costs by dealing with a significant part of the refugee crisis. according to the European Commission, since the start of the civil war, the European Union has committed more than €27,4 billion. The disproportionate and unexpected burden of the wave of refugees on states has raised security issues and risks for the EU (European Commission 2022).

Former EU member state, the United Kingdom, has been a major ally of the US in counter-terrorism strategies since the global war on terror began immediately after the attacks of September 11, 2001. The UK Government has contributed its forces to the North American pursuit of bin Laden and the fight against the Taliban in Afghanistan. The fight against non-state military actors who use terrorism as a tactic is a very important issue that needs to be addressed to protect and guarantee the interests of the United Kingdom (Government of the United Kingdom 2018).

France is directly involved in the fight against jihadist groups in North Africa, particularly in Mali, where it is working against the al-Qaeda branch AQIM. The French government recognizes that these jihadist groups are a threat not only to African or Middle Eastern security but also to European security. In fact, combating this threat is a priority of the French government's foreign policy, and achieving this objective guarantees France's presence in these regions.

Luxembourg's counter-terrorism strategy is entirely consistent with the position of the European Union. This strategy recognizes the importance of international cooperation and is continuously adapting to evolving threats and challenges. The EU believes in the use of coercive measures as the best way to combat potential threats (Committee of Ministers Bureau 2002). Luxembourg is concerned about the expansion of non-state military actors around the world, particularly in the Middle East. It pays particular attention to the actions undertaken by extremist jihadist groups. Luxembourg has

paid particular attention to the proliferation of the use of chemical weapons by these groups (Stewart and Salisbury 2016).

The Syrian conflict seems to be at an impasse without any winner. UN member states give the UNSC the primary responsibility for maintaining international peace and security under the UN Charter. In exercising this responsibility, the UNSC must act by the purposes and principles of the United Nations, despite the severity and industrial scale of the serious crimes under international law committed in Syria. The involvement of international stakeholders through the UN-led Geneva Conventions has not been successful due to paralysis in the UNSC, and neither has the Russian-led Astana process helped. While many blame the inactivity of the Western powers or the UN, approximately 90% of the Syrian civilian population lives in poverty and has no access to energy, and about 13 million Syrians in total are forcibly displaced, which is more than half of the country's population (Philips 2022).

At the outset of the Syrian conflict, the UNSC continuously dealt with events in Libya. Consequently, the events in Syria were discussed for the first time in April 2011 during the session held on the Israeli-Palestinian negotiations (Security Council, 6524th Meeting, 27 April 2011). Another important session concerning the situation in Syria was held in August 2011, when delegates expressed their concern about the situation in the country. Even at this early stage, the US and some European states stated in the media that they were calling on Assad and his regime to end the violence against the protesters. This statement was not released due to a lack of support from all UNSC members. The resolution against the Syrian regime's violence was never voted on because it was assumed that Russia and China would block it in the UNSC. Thus, even at the beginning of the conflict, we recognize a division in the UNSC between the Western countries and Russia and China. A deadlock was created and unresolved for another four months (Security Council, 6598th Meeting, 3 August 2011). Moreover, since the beginning of the uprising in Syria in March 2011, Russia and China have vetoed 17 draft UN Security Council resolutions, resulting in several failed UNSC attempts (UK Government 2022).

POTENTIAL AND SUCCESSFUL SOLUTIONS BASED ON INTERNATIONAL LAW

According to the director of the Middle East and North Africa Program at the International Commission of Jurists, Said Benarbia, seven appropriate steps exist to resolve the crisis. The first one should be the renewal of the mandate of the Organization for the Prohibition of Chemical Weapons (OPCW) under Resolution 2235 of 2015. Secondly, it is important to establish an independent UN investigation mechanism to identify the international law subjects that have perpetrated, organized, sponsored, or participated in using chemical weapons in Syria. Thirdly, requiring all relevant parties to provide prompt and safe access to sites where chemical attacks are supposed to be investigated under the OPCW. The fourth step should be resuming the passage of humanitarian aid through the Bab al-Salam, Bab al-Hawa, and Al Yarubiyah border crossings. Another key step is to forward the situation in Syria since March 2011 to the Prosecutor of the International Criminal Court (ICC). The sixth step is to ensure that all parties immediately cease all air strikes and military flights. And the last one should be the decision, under Chapter VII of the UN Charter, that the Syrian authorities (a) cease military movements towards the civil population, (b) terminate all use of heavy weapons in the civil population centres (Benarbia 2021).

ACHIEVEMENTS OF THE INTERNATIONAL COMMUNITY

The most successful resolution adopted by the UN Security Council has been so far considered to be the UNSCR 2254, which was unanimously adopted on December 18, 2015. This resolution outlines a roadmap for Syria's political transition and calls for a political ceasefire and settlement. The EU strongly supports a political solution through an inclusive and meaningful transition in line with UNSCR 2254 and the Geneva Convention. However, even in 2022, no real progress has been made in implementing resolution 2254 (Security Council, 7588th Meeting, 18 December 2015).

Before we analyze the cause of the failure of the peace and security plan in Syria, we should be aware of the phase of the conflict in Syria. According to the hourglass model, there are approximately nine stages of conflict, and each stage has a way of resolving it. These stages are – difference, contradiction, polarization, violence, war, ceasefire, agreement, normalization, and reconciliation (Ramsbotham et al. 2011). Nevertheless, no

alternative would force the Syrian regime to disarm its forces. Violence and oppression have occurred in Syria because the government has attacked civilians with tanks, gunfire, and chemical weapons, which international law prohibits. Those are the fundamental issues that ought to be tackled. Syria is a country that receives military foreign aid from some nations, such as Russia, Belarus, Iran, and North Korea (Human Rights First 2013).

Initial reflections suggest that the easiest solution is to stop the violence and oppression in Syria by disarming the Syrian military and the other combatants. Foreign intervention by peacekeepers is needed in the country to prevent the abuse of military technology. Implementing a foreign intervention in Syria is difficult as Russia regularly blocks resolutions on humanitarian intervention.
However, the international community has repeatedly called for the use of the so-called R2P or Responsibility to Protect. The R2P is a norm under which state sovereignty is not an absolute right and a state that has either failed to protect its citizens from mass atrocities or has participated in genocide or other crimes against its population (Evans 2008).
The concept of R2P is based on three pillars:

1. Responsibility to prevent
2. Responsibility to react
3. Responsibility to rebuild

Under the first pillar, a sovereign state must protect its citizens from mass atrocities. To fulfil this duty, the government of a sovereign state must establish the rule of law and address the political needs of its population by creating institutions for the separation of powers and establishing an independent judicial system. If the government is either unwilling or unable to protect its citizens, the international community must take action to stop mass atrocities. Before using military force, the international community must use all non-military measures, such as financial sanctions or arms embargoes. When all these measures fail to stop mass atrocities, the international community may consider taking military action as a last option (Global Centre for the Responsibility to Protect 2021).

More generally, R2P clearly indicates that state sovereignty is no longer absolute but depends on responsible behaviour. If a government violates

international law and if it permits atrocities or commits abuses, the Security Council may or may not act depending on the political interests of the P5 members (Murray and McKay 2014).

The UN can only operate based on the will of its member states. If the international community were inactive, it would not create international ad hoc bodies, tribunals, and mechanisms to investigate violations of international law. One of these mechanisms is the International, Impartial, and Independent Mechanism (IIIM 2017). The IIIM was established by General Assembly resolution71/248(2016), adopted by 105 votes, with 52 against and 15 abstentions. IIIM is an ad hoc mechanism established to ensure the criminal accountability of individuals who have committed violations of international humanitarian law and international human rights law in Syria. The mechanism is mandated to collect, consolidate, preserve, and analyze evidence of violations of international law to prepare files on such violations and abuses for future criminal proceedings. The information and evidence are confidential, and they are provided only to the judicial authorities (IIIM 2017).

The failure of peacebuilding in Syria is because Syria continues to have the ability to commit atrocities against civilians through foreign supporters who have an interest in the country. These foreign supporters have also allowed the civil war to become an international conflict. The atrocities committed by the Assad regime have led to the imposition of economic sanctions by Western countries to restrict Syria's access to the financial market as pressure on the regime. However, these sanctions did not affect Syria, as Syria's external lenders could still financially support the government (Ministère de l'Europe et des Affaires Étrangères 2020). While some experts believe that economic sanctions can be an effective foreign policy tool in certain circumstances, a growing body of opinion sees them as largely ineffective and potentially harmful. Policymakers and academics will undoubtedly continue to debate the use of sanctions as they try to understand the nuances and limitations of this contentious strategy. Sanctions may trigger retaliation from the targeted regime or harm trade ties and other forms of economic cooperation. The unintended repercussions, according to critics, can diminish the overall effectiveness of sanctions and cause long-term harm to all parties. Sanctions may result in a

shortage of necessities like food and medication - this argument became evident almost immediately in the case of Syria (Berlin 2022).

The UN then adopted ten draft resolutions on Syria in September 2014. The United States unanimously adopted a draft on combating foreign fighters in Syria and Iraq. The draft envisaged preventing terrorists from travelling to the region and punishing those who provided them with weapons and logistical support (UN Digital Library S/2014/695). Philips criticizes the international community for the lack of will to improve the lives of civilians and for failing to prevent a permanent division of Syria. The most important lesson from the tragedy in Syria is that a new era of multipolarity has begun, one that will be marked by competitive power politics that have contributed to the suffering of millions of innocent people in Syria (Philips 2022).

Consequently, we can see that different international interests have brought the UNSC to an impasse on Syria. Since the Syrian conflict is so complicated, would it not be best to leave it alone and let them fight independently?

Based on research on the issue and lessons learned from the past, we argue that, despite several failures since its establishment, the UN is still beneficial in providing states with cooperation in resolving conflicts and maintaining peace and security internationally. Firstly, if the international community were to ignore the problems in Syria completely, it would lead to even greater crimes against humanity and more serious problems in the region than before. Unfortunately, refugees have proved to be a problem for neighbouring countries, and in 2015, this also caused a crisis in the European Union. If no action is taken, their numbers will only increase. Secondly, this conflict could spread across its borders and destabilize the entire region. In particular, the nearby Israeli-Palestinian conflict could create a major war if it escalates through contact with the Syrian conflict. Thirdly, if the international community does nothing about this conflict, it will effectively bankrupt the idea of R2P. And the UN and the Western powers are not yet ready to give up on the idea, given that the first real implementation of the concept was in Libya. Although a better future for Syria is not yet within reach, there are glimmers of hope (Lynch 2017).

The US and EU have imposed diplomatic and economic sanctions, albeit not all are considered useful. Studying the issue has made it clear that the division among the members of the Security Council and their inability to reach a consensus on the measures needed to stop the Syrian crisis is reminiscent of the issue of the United Nations. The UN has encountered enormous problems over the years, particularly in adopting and enforcing resolutions. The lack of consensus between permanent members, the veto problem, the absence of a unified political agenda to carry out advocacy, and the strategic calculations of the major powers in the UNSC. Overall, China's decision to work with Russia to veto UN Security Council resolutions against Syria demonstrated their shared determination to restrain US unilateralism on global governance issues (Puess 2022).

SUMMARY

In conclusion, we assess that the potential solution would be a reform of the UNSC. Considering Western powers such as the EU, we argue that the EU does not support the Assad regime or the militant groups. Furthermore, the EU is not even taking the lead and simply follows the US administration's lead. Colonial powers of the past, such as France, do not have the influence or the assets to intervene in the conflict permanently. However, following the outbreak of Russian aggression against sovereign Ukraine, the voices of the Syrian opposition have been raised, criticizing the EU for double standards. Nevertheless, the most important stakeholders are the US and Russia, as members of P5. Adopting resolutions and their enforcement will be difficult as long as the five permanent members retain veto power and political alliances forged largely based on compelling national interests. That is why major reform is needed, in particular, the enlargement of the Security Council to include Germany and Japan, which have once again become world economic powers, as well as Africa and Latin America, which are renowned for their ability to maintain regional peace and security. This will facilitate cooperation between Member States to achieve a broad consensus for Security Council enforcement actions. Expanding the number of members of the Council could help to strengthen its authority and regulate the veto power, enabling the adoption of a resolution and the possibility of its implementation. Regardless of whether the Security Council is reformed to include additional permanent members or whether the veto is reconsidered, the adoption of resolutions is conditional on the

unanimity of the permanent members. This required unanimity has rarely occurred since the UN was founded. Therefore, unanimity among Council members is necessary to ensure the rapid adoption of resolutions on international peace and security issues.

REFERENCES

Berlin, M. P. 2022. "The Effect of Sanctions". Accessed 22.02.2023. https://freepolicybriefs.org/2022/05/10/effects-economic-sanctions/.

Evans, G. 2008. *The Responsibility to Protect: Ending Mass Atrocity Crimes Once And For All.* Brookings Institution Press. 349 pages. EISBN 978-0-8157-0180-4.

European Commission. 2023. "European Civil Protection and Humanitarian Aid Operations: Syria". Accessed 30.01.2023. https://civil-protection-humanitarian-aid.ec.europa.eu/where/middle-east/syria_en.

Global Centre for Responsibility to Protect. 2021. "What is R2P?! Accessed 30.01.2023 https://www.globalr2p.org/publications/the-responsibility-to-protect-a-background-briefing/.

Government of United Kingdom. 2018. "The United Kingdom's strategy for countering terrorism". Accessed 30.01.2023. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.

Government of United Kingdom, CROKER, R.. 2022. "Russia's justification for using its veto on Syria is pure fiction". Accessed 30.01.2023. https://www.gov.uk/government/speeches/russias-justification-for-using-its-veto-on-syria-is-pure-fiction.

Human Rights First. 2013. "Enablers of the Syrian Conflict-how targeting third parties can slow the atrocities in Syria". Accessed 30. 01. 2023. https://ciaotest.cc.columbia.edu/wps/hrf/0032068/f_0032068_26056.pdf.

IFCR. 2021. "Syria crisis: 10 years on, humanitarian situation is worse than ever". Accessed 22.02.2023. https://www.ifrc.org/press-release/syria-crisis-10-years-humanitarian-situation-worse-ever.

IIIM. 2017. "At a Glance". Accessed 30.01.2023. https://iiim.un.org/who-we-are/at-a-glance/.

International Affairs: Allison, R. 2013. “Russia and Syria: explaining alignment with a regime crisis”. Accessed 30.01.2023. https://academic.oup.com/ia/article/89/4/795/2417157.

Middle East Eye: Philips, C. 2022. “Why the West need a radical rethink on Syria”. Accessed 30. 01. 2023. https://www.middleeasteye.net/opinion/syria-war-conflict-radical-rethink-needs-why.

Ministère de l’Europe et des Affaires Étrangères. 2020. “Les sanctions européennes : un instrument de lutte contre la répression en Syrie Accessed 30.01.2023. https://www.diplomatie.gouv.fr/fr/dossiers-pays/syrie/les-sanctions-europeennes-un-instrument-de-lutte-contre-la-repression-en-syrie/.

Murray, R.W., McKay, A.. 2014. “Into the Eleventh Hour”. Accessed 30.01.2023. https://www.e-ir.info/publication/into-the-eleventh-hour-r2p-syria-and-humanitarianism-in-crisis/.

Benarbia, S.. 2021. “Syria and the UN Security Council: A Decade of Abysmal Failures”. Accessed 30.01.2023. http://opiniojuris.org/2021/04/28/syria-and-the-un-security-council-a-decade-of-abysmal-failures/.

Stuart, I.J., Salisbury, D.. 2016. “Non-State Actors as Proliferators: Preventing their Involvement”. Accessed 30.01.2023. https://strategictraderesearch.org/wp-content/uploads/2017/09/Non-State-Actors-as-Proliferators-Preventing-their-Involvement.pdf.

UN Digital Library. 2014. “UNSC S/2014/695”. Accessed 30.01.2023. https://digitallibrary.un.org/record/779957.

United Nations Security Council. 2011. “6524th Meeting 27 April 2011”. Accessed 30.01.2023. https://digitallibrary.un.org/record/702233.

United Nations Security Council. 2011. “6598th Meeting 3 August 2011”. Accessed 30.01.2023. https://digitallibrary.un.org/record/708352.

United Nations Security Council. 2015. "7588th Meeting 18 December 2015". Accessed 30.01.2023. http://unscr.com/en/resolutions/doc/2254.

Tejero, M.. 2022. "The role of the EU in the Syrian conflict and the hunt for a new strategy". Accessed 30.01.2023. https://www.unav.edu/web/global-affairs/the-role-of-the-eu-in-the-syrian-conflict-and-the-hunt-for-a-new-strategy.

The World Bank. 2023. "The World Bank in Syrian Arab Republic". Accessed 30.01.2023. https://www.worldbank.org/en/country/syria/overview.

Weiler, A.Y. 2014. "Pipeline Predicament: The Ukraine-Syria-Russia-US gas nexus". Accessed 30.01.2023. https://efile.fara.gov/docs/6845-Informational-Materials-20201116-44.pdf.

ECONOMIC ASPECTS OF THE MODERNIZATION OF THE ARMED FORCES OF THE SLOVAK REPUBLIC AND THE POSITION OF THE SLOVAK DEFENCE INDUSTRY

Atalovič Peter, expert consultant: Škultéty Štefan

EXECUTIVE SUMMARY

The Slovak defence industry (SDI) has been at the periphery of the political scene's interests since 1989. Thirty years of neglect have led to the decline of this sector, which suffers from inadequate state support in terms of defence spending and investment, a lack of human capital, and deficiencies in the legislation. To improve the position of the SDI, the state must ensure an adequate level of expenditure, equivalent to at least 2% of GDP. In terms of state-owned enterprises (SOE), increased funding would provide opportunities to increase production, stabilize staff, and promote their products. Additionally, we recommend legislative changes to make international trade processes more predictable. These suggested changes are necessary for the survival of the SDI in the current global competition.

INTRODUCTION

On January 1, 2023, Slovakia commemorated its 30th anniversary. During this period, the Army of the Slovak Republic, and later the Armed Forces of the Slovak Republic (AF SR), fulfilled their tasks as stipulated in the Constitution of the Slovak Republic. These tasks primarily include securing sovereignty, territorial integrity, and protecting citizens.

To continue fulfilling these tasks, a modernization process has begun. The modernization of the AF SR is a long-term process that presents many challenges. Therefore, political will is crucial to this effort in the coming years. The ongoing Russian aggression against Ukraine has a significant impact on the current security environment. It has not only affected the modernization of the AF SR but also the issue of increasing the defence capabilities of our partners.

According to the Ministry of Defence of the Slovak Republic's (MOD SR 2016, 6-7) White Paper on the defence of the Slovak Republic, increasing the readiness and war-fighting ability of the AF SR is dependent on human resources and military hardware. The Government of the Slovak Republic (GOV SR 2021, 32) has also made the same commitment in its Program Statement for the period 2021-2024. This essay abstains from discussing the purchase of military equipment from abroad and military personnel and training. Instead, the aim is to focus on the domestic capacities of the defence industry. The aforementioned documents highlight the need to involve the Slovak defence industry in the modernization process. Therefore, this essay will analyze its position and potential challenges in global competition. Additionally, specific recommendations will be provided to the authorities to assist the SDI.

BACKGROUND AND CONTEXT

The defence industry in Slovakia has a long-standing tradition. However, the common perception that this industry's roots are solely based on the era of socialist Czechoslovakia, during which a wide range of military equipment was produced in Slovak enterprises, is not entirely accurate. In fact, the industry's beginning dates back to the time of the Austro-Hungarian Empire.

During the period of the First Czechoslovak Republic, the country established a strong and competitive defence industry, which ranked among the top world exporters. In 1934 and 1935, Czechoslovakia was the world's largest weapons exporter, with a share of 27% and 24.4%, respectively (Čechák et al. 1993, 34). This demonstrates that even small countries are capable of developing a globally significant defence industry. The most critical factors are the level of technology and skilled workforce, which enable fast, high-quality production and economies of scale. With this in mind, it is easy to understand the political significance of Czechoslovakia in Hitler's plan to conquer Europe.

Following the Second World War, Czechoslovakia became part of the Eastern bloc in 1948. This new reality led to changes in the defence industry to meet the needs of Warsaw Pact countries. The remaining production was exported to other socialist or Arab countries. Between 1970 and 1989, 70% of

the country's production was exported, representing 7-10% of the nation's exports (Mesároš, 1996, 207). Throughout the entire communist era, the country maintained a positive trade balance in military production. Despite the overall trade position of Czechoslovakia worsening since 1948, the country managed to maintain its position among the top 10 exporters of military equipment in the 1980s.

During that particular period, a portion of the production capacities was relocated to Slovakia. Some examples of territorial diversification within the defence industry included Trenčín, Dubnica nad Váhom, Martin and Detva, Hriňová, and Liptovský Mikuláš. By the end of the 1980s, the majority of production in the defence industry had shifted to Slovakia, with approximately two-thirds of employees, totalling around 45,000 people, working for the Slovak Defence Industry (SDI). The primary products manufactured by Slovak factories were tanks, armoured personnel carriers, artillery, and large-calibre munitions. The share of the defence industry in the total industrial production of Slovakia was 6% (Ivánek 2002, 133). This share was larger than in the Czech part of the federation.

Following the Velvet Revolution and the dissolution of the bipolar world, the Czechoslovak defence industry, along with other sectors, was unable to maintain its position. The traditional trade partners of Czechoslovakia were undergoing socio-economic changes, which resulted in a reduction in military capacities and cuts in defence spending. This situation also affected the newly formed Czechoslovak and later Slovak army. The conversion of defence industries to civil production resulted in significant unemployment and created many economic problems.

In response to the changing market conditions, the Slovak Defence Industry (SDI) had to adapt. The authorities mandated that military production be reduced by more than 90% (Ivánek 1994, 132). In the subsequent section, our attention will shift to the period after 1993 and the present situation in the SDI, which has been significantly influenced by the ongoing conflict in Ukraine. This situation has presented an opportunity for the SDI to adjust and respond to emerging challenges.

ANALYSIS

As previously noted, the defence industry experienced a significant decline in the 1990s. Following the partition of the Czech and Slovak Federative Republic, the two newly formed states adopted distinct approaches to their respective defence industries. Generally speaking, the Czech Defence Industry (CDI) has maintained a more integrated structure, is privately owned, and has been more successful in its export endeavours (Chovančík 2018, 274).

To assist the Slovak Defence Industry (SDI), the Security and Defence Industry Association of the Slovak Republic (SDIA SR) was established in 2000. Its objective is to promote and safeguard the interests of its members, support the promotion of their products, enhance their export capabilities, and assist them in participating in the industrial structure of EU and NATO countries. According to SDIA SR, the association comprises 58 members, and their total turnover amounts to 1.2 billion EUR (SDIA SR 2022, 4).

Even though just a few of its members are state-owned (SOE), these enterprises (Letecké opravovne Trenčín (LOTN) and DMD Group, which consists of Konštrukta Defence, ZVS Holding, ZTS Špeciál) are responsible for a considerable part of the production. Together they make up more than 10% of the turnover of all SDIA SR members, thus the state still keeps its position in SDI. As far as the production structure is concerned, these enterprises focus on the production of heavy weapons and munitions. The rest of the enterprises are private owned. However, the majority of them are small enterprises that struggle to compete globally. A positive example of a private-owned enterprise is Aliter Technologies which provides solutions for NATO in the field of information and communication technology. The existence of private- and SOE means that states could not use the same measures to improve their position. However, some measures could be applied and influence both types of enterprises, such as legislative changes. As stated in the introduction, the current process of modernization of AF SR and the ongoing conflict in Ukraine provide an impetus for SDI. To enhance the position of the SDI, it will be necessary to expand production, which may present certain challenges. In the following paragraphs, we will outline our views regarding the SDI's production capabilities.

Recent developments indicate that the government is committed to fulfilling its obligations as outlined in the Long-term development plan of the Ministry of Defence with a prospect until 2035. The plan mandates the SDI's participation in major acquisition projects at a minimum level of 30% (MOD SR 2022, 14). In August 2022, Slovakia and Finland signed an agreement confirming the purchase of 76 Patria AMVXP 8x8 armoured combat vehicles. The acquisition is scheduled to be completed by 2027 and, according to the Slovak Minister of Defence, will allow the participation of over 40 Slovak companies, producing more than 40% of the contract's value (MOD SR 2022). The MOD SR has also outlined additional projects to be carried out until 2035.

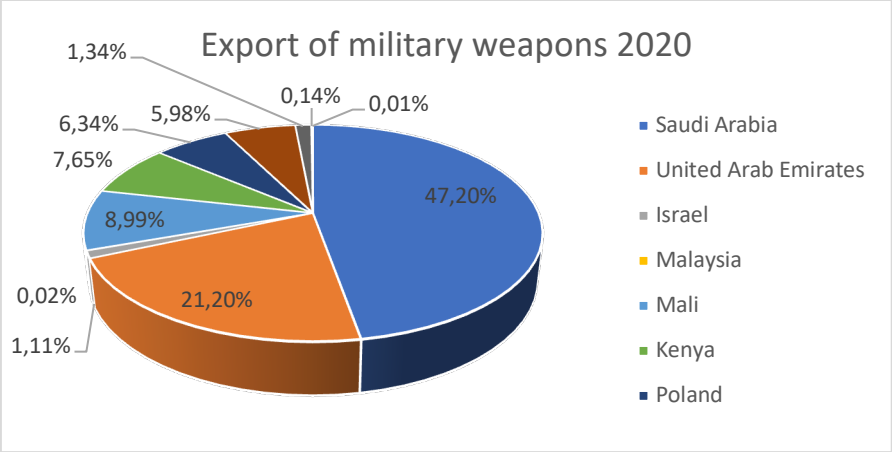
The current trend toward diversification of customers for SDI is positive; however, it is important to note that it still heavily relies on projects carried out for the MOD SR. This overreliance is particularly noticeable in the annual reports of the SOEs within the industry, which state that they primarily focus on MOD SR projects. For instance, Letecké opravovne Trenčín reported that in 2021, the MOD SR accounted for 72% of its total turnover (LOTN 2022, 19). To expand its customer base and increase sales abroad, SDI needs to undertake diplomatic efforts and promote its products at trade shows, such as the International Defence Exhibition Bratislava, which was held in May 2022.

Despite promotional efforts made in the past years, the territorial structure of its exports has remained largely unchanged, with a focus on the Middle East and Africa. These regions can be characterized as unstable, and they include countries with a history of indebtedness in military trade. Therefore, it would be appropriate for SDI to diversify the direction of its foreign trade. Graph 1 shows the territorial structure of the export of military weapons in 2020. Data show that no more than 15% is exported to the EU and NATO countries. With a few exceptions, this trend characterizes the trade of SDI. Even if the share was higher in several years, it was usually because of the Czech Republic. However, this traditional partnership seems to be in decline as the Ministry of Defence of the Czech Republic (MOD CR) procured 52 French self-propelled howitzers CAESAR in September 2021 and 10 additional in December 2022 in the total amount of 425€ million, instead of

Slovak self-propelled autonomous artillery system ZUZANA 2 (MOD CR 2022).

We may conclude that despite Slovakia's membership in the EU and NATO for over 15 years, the global defence market remains highly competitive and closed to SDI. Representatives from SDI have confirmed this current state of the global defence market, indicating that despite producing high-quality products, western countries do not allow SDI to enter their supply chains, instead choosing to support their enterprises. This trend is also reflected in the analysis of the top 100 arms-producing and military services companies in 2021 conducted by the Stockholm International Peace Research Institute (SIPRI). Only one company from states that entered Euro-Atlantic structures after 1999 made it onto the list - the Polish PGZ, which ranks 76th (SIPRI 2022, 10).

Graph 1



Source: The Observatory of Economic Complexity

Given the aforementioned factors, it is crucial to establish favourable conditions for FDI in SDI. Since 1998, Slovakia has successfully attracted FDI and developed a highly significant automotive industry. However, due to the unique nature of this industry, the government may not be inclined to promote FDI inflows. Apart from Czechoslovak group investments, Slovak enterprises largely rely on themselves. Besides FDI, government investments may influence the position of SOE. The question remains whether there is a political will to allocate more funds to SOE. As a result of this disadvantage, SDI faces challenges in expanding its production capabilities.

At this moment, another source of investment seems to be on the horizon. NATO allies discuss the possible renewal of production of 122mm and 152mm artillery munitions which are used by howitzers of the Soviet era and still dominate the battlefield in Ukraine. In this regard, cities Dubnica nad Váhom and Snina were mentioned. This production could be financed by NATO (Yar 2022). Even though this investment could help SDI, it is not a long-lasting systematic solution. Eventually, the war will end and SDI will continue to face strong competition.

In addition to investments, human capital plays an important role in the development of SDI. SDIA SR members employ a total of 11,000 people. The state does not have a direct impact on the employment policy of private-owned enterprises. Because of that, we will focus on SOE. According to annual reports of four SOE, they employed 780 people at the end of 2021. It corresponds to approximately 7% of SDIA SR employees. Table 1 shows the number of employees in SOE. Interannually, the aggregate number does not show a significant increase. We assume that the number will rise in the next years as DMD Group announced the creation of another 250 job positions (Aktuality 2023).

Table 1 Number of employees in SOE

Year	LOTN	Konštrukta-Defence	ZVS Holding	ZTS Špeciál
2021	302	139	212	127
2020	315	132	272	121

Source: Annual reports of LOTN, Konštrukta-Defence, ZVS Holding, ZTS Špeciál

At first sight, it seems that obtaining a workforce is not a problem. The unemployment rate in December 2021 was 6.76%. A year later it was only 5.90% which represents 160,204 people. Taking into consideration the territorial diversity of SDI enterprises (the majority of them operate in the western part of the country) and the fact that unemployment is more significant in the eastern part of Slovakia, it may be a problem to find people who are qualified for this kind of work whether for state or private-owned

enterprises. Table 2 shows the structure of unemployment in Slovakia in December 2022.

Table 2 Unemployment Slovakia in December 2022

Region	Unemployed	Region's share of total unemployment in %
Bratislava	11,805	3.24
Trnava	10,352	3.60
Nitra	13,236	3.85
Trenčín	10,751	3.69
Žilina	16,319	4.63
Banská Bystrica	26,733	8.48
Košice	32,064	8.69
Prešov	38,944	9.98

Source: Central Office of Labour Social Affairs and Family

Regarding the availability of a workforce, another problem for SDI is the automotive industry. Without hesitation, it is the most important sector for the Slovak economy making up 12% of the GDP and employing 164,000 people directly and other 81,000 indirectly (SARIO 2022, 2). But from the SDI point of view, it absorbs a large number of people skilled for work in the defence industry.

In SOE, the problem to recruit new people may be more severe due to low wages. Out of four SOE, two of them (LOTN and ZVS Holding) have published salary data, which show that neither enterprise pays an average wage that matches the national average wage (€1211/month) or the industry average wage (€1271/month). In general, SOE face problems with attracting a workforce.

Moreover, SOE even provide the age structure of its employees. LOTN states that 188 out of its 302 employees are over 50 years old (LOTN 2022, 7). ZTS Špeciál emphasizes that the average age of its employees is 49.1 years (ZTS 2022, 4). Based on the data provided during a personal interview with the management of DMD, the average age of an employee in Konštrukta-Defence is 46.1 years. The workforce is getting older. These findings together

with lower salaries in SOE will negatively influence the future capability to be part of the modernization of the AF SR and part of the other supply chains.

As mentioned in the previous paragraphs, SOE struggle to recruit new employees. Acquiring a new workforce from other industrial sectors is not an appropriate strategy because other engineering companies are often suppliers for defence enterprises which may have a negative impact on access to manufacturing inputs. For this reason, education of the new workforce seems to be a better approach to stabilising the staff. At the level of tertiary education, Slovakia currently has 32 technical faculties and 18,000 students in engineering-related fields. Besides that, it provides education in more than 260 technical vocational secondary schools, currently with 31,700 students (SARIO 2022, 9).

According to the representatives of SOE, some steps were already taken, such as a dual-education system. Data shows that this system is relatively new in this sector. ZTS Špeciál provides a dual education system in collaboration with the Secondary vocational technical school in Dubnica nad Váhom since the school year 2017/2018. The enterprise started with 2 students. In 2021, 12 students were enrolled (ZTS 2022, 4). In the current school year, 6 students participate in this program. Konštrukta-Defence does not even use the dual education system.

Cooperation with universities is also just beginning even though a positive trend can already be seen. In October 2022, DMD Group signed a Memorandum of cooperation with the University of Alexander Dubček in Trenčín (DMD Group 2022).

The position of any sector depends on the legislation of the country. The specific nature of the defence industry also means specific legal regulation. In Slovakia, trade in the defence industry is subject to Act no. 392/2011 Coll. on trade in defence industry products and amendments to certain laws. The Ministry of Economy of the Slovak Republic (MOE SR) carries out the control of this act. This act requires all entities that want to carry out trading and intermediary activities with defence industry products to obtain a permit. According to Act no. 392/2011 Coll, § 5 to obtain a permit it requires

fulfilment of certain conditions and a positive statement of the Ministry of Defence of the Slovak Republic (MOD SR), Ministry of Foreign and European Affairs of the Slovak Republic (MFEA SR), Ministry of Interior of the Slovak Republic (MOI SR), National Security Authority (NSA) and Slovak Information Service (SIS). Table 3 shows issued and rejected permits to trade with products of the defence industry in the last 10 years.

Table 3 Permits to trade with products of the defence industry

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Approved	20	31	21	28	34	24	35	25	36	29
Rejected	0	0	1	1	0	0	0	0	0	2

Source: Annual reports on trade in products of the defence industry

Besides the permit, foreign trade activities outside the EU require an export or import licence. As we have already shown, trade outside the EU is of great importance for SDI and makes up the majority of foreign trade in this sector. This document allows an enterprise to carry out a particular deal. Issuing an export or import requires a statement of the same bodies (MOD SR, MFEA SR, MOI SR, NSA, and SIS). Except for the MFA SR, the statements of the authorities are only of a recommendatory nature (Act no. 392/2011 Coll, § 17). Thus, the MFEA SR has the sole power to reject any trade contract. Table 4 shows issued and rejected export licences in the last 10 years.

Table 4 Export licences

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Approved	208	100	112	108	129	120	126	95	89	121
Rejected	0	0	0	1	11	3	3	2	0	0

Source: Annual reports on trade in products of the defence industry

The most recent legislative change related to the defence industry was the change of the licence fee. Previously enterprises had to pay for issuing the licence regardless of whether they received the licence. The fee, which was set at 0.2% of the contract, could be substantial and in the case of large

contracts, it could amount to tens of thousands of euros. Enterprises factored this cost into their pricing strategy, which had a negative impact on competitiveness and dissuaded some from participating in international trade with defence industry products. Effective as of September 1, 2022, Act no. 249/2022 Coll. has capped the maximum license fee at 2000€. This change should substantially improve the position of SDI enterprises, both private- and state-owned. However, the exact results of this change, such as the number of issued licenses, will be visible in the coming years.

The specific production portfolio of the defence industry creates another problem for enterprises. Because of the company policies of financial institutions, they refuse to provide tools of trade finance for SDI companies, which often exclude enterprises from international trade, not to mention the fact that trade is oriented towards countries where tools of trade finance, such as Letters of Credit (LoC) is commonly used (for the territorial structure of SDI export see the text above). Due to the lack of tools, the Export-Import Bank of the Slovak Republic (EXIMBANKA SR) introduced in October 2022 a new Export LoC to facilitate the needs of SDI. As the new tool came into being very recently, its impact cannot be evaluated yet.

RECOMMENDATIONS

In the previous part of this essay, we analysed the current position of SDI. We defined SDI in terms of membership in SDIA SR and emphasized the importance of SDI in the process of modernization of the AF SR. Nevertheless, we argued that SDI needs to be export-oriented. Subsequently, we took a closer look at the territorial structure of export, investments, human capital, and legislation. Based on these points, we recommend several measures which may have a positive influence on SDI.

Expenditures. Defence expenditures are the most critical factor that influences almost all other measures. During the 2014 Wales summit, leaders of NATO countries pledged to spend 2% of their GDP on defence, with 20% of that expenditure allocated to new equipment. However, at present, only one-third of NATO members meet this obligation. Slovakia is expected to reach the 2% GDP defence spending threshold for the first time in 2023, which equates to 2.45 billion euros (Trend 2022). It is worth noting, however, that the commitment was accepted before the full-scale Russian war in Ukraine. Given that Russia considers Slovakia an enemy state, this

situation should be reflected in defence expenditures. Therefore, we recommend adopting a law that establishes the minimum amount of defence spending at 2% of GDP. Recently, the Government of the Czech Republic submitted a bill with the same provision to parliament. Legally regulating this obligation will compel any future government to invest in defence. Coupled with the commitment to involve SDI in the modernization of the AF SR, this measure will ensure continuity and stability for defence enterprises and, as a result, enhance their position.

Investments. Secondly, the government should review its investment policy. The current demand for defence industry products and the insufficient capacity of SOE often results in order rejections or delays. Thus, providing favourable loan options would benefit SOEs and help them increase their production capacities. Regarding FDI, Slovakia should clarify its position on the involvement of foreign investors in its defence industry. If so, for instance, DMD Group could offer land and premises for sale and rent in Dubnica nad Váhom. This may not align with the goal of attracting investments to the eastern region of Slovakia, however, it could support the existing supply chains and provide an advantage to the already established enterprises.

Human capital. The question of human capital appears to be a complex issue for SDI and is directly interconnected with investments and expenditures. It is not possible to increase production without machines, as well as a skilled workforce. The age structure of SOE indicates that they will not be able to operate in ten years without additional measures, nor will they be able to increase production. Without increasing wages to at least the average level in the industry, the position of SOE will deteriorate. The task for SDI is to deepen dual-system education, thus involving more schools and students. Table 5 identifies possible secondary schools for cooperation in a dual-education system with SOE.

Table 5 Possible partner for dual-education system.

School	Address
Secondary vocational school	Pod Sokolicami 14, 911 01 Trenčín
Aviation-technical secondary vocational school	Legionárska 160, 911 04 Trenčín
Mechanical engineering secondary school	Športovcov 341/2, 017 49 Považská Bystrica
Secondary technical school	Bzinská 11, 915 01 Nové Mesto nad Váhom
Secondary technical school	Obrancov mieru 343/1 018 40 Dubnica nad Váhom

We have identified shortcomings in the acquisition of university-educated personnel. Therefore, we recommend expanding cooperation with other universities based on the model of cooperation with the University of Alexander Dubček. In this regard, we see potential collaboration with several faculties of the University of Žilina and the Faculty of Materials Science and Technology at the Slovak University of Technology in Trnava. Enterprises could offer internships to students, providing them with an opportunity to acquire skills and knowledge that could be useful in future collaborations. Additionally, the curriculum at these faculties should be updated to include specific subjects related to the defence industry, such as ballistics, which are usually absent from curricula. By including defence-related subjects, universities can raise awareness of this sector. However, the dual-education system will not make a difference if enterprises do not offer students attractive salary packages and other benefits. If they fail to meet the conditions, dual education and internship opportunities will serve only as the preparation of the workforce for the private sector a thus will fail to strengthen the position of SDI in the long term.

Promotion. In our analysis, we have examined the export of the SDI and have concluded that the territorial structure of exports cannot be easily altered, with markets in Africa and the Middle East remaining crucial. Despite this, SDI must remain proactive in promoting its products to maximize its market reach. Our recommendation is to encourage as many SDI enterprises as possible to participate in trade shows. To achieve this, the state could facilitate SDI's participation by partially or fully reimbursing

entrance fees for the enterprises. This would reduce costs for enterprises, allowing even small businesses to participate in trade shows.

Legislation. In addition to the necessity of making 2% of GDP on defence a legally binding obligation through a law, there is also an opportunity to reform Act no. 392/2011 Coll. on trade in defence industry products. In our analysis, we have emphasized the crucial role of the MFEA SR in granting export or import licenses. According to § 42 of Act no. 392/2011 Coll., a decision to reject an application for an export or import license only states that it is due to the foreign policy or security interests of the Slovak Republic. We believe that such legislation is insufficient. Therefore, we recommend an additional task for the MFEA to provide recommendations in the form of a report for SDI enterprises to either proceed or not proceed with contracts with partners in specific countries. This could be done at least once every six months. By doing this, we could create a more predictable environment for SDI. The enterprise would have a better understanding of whether or not to initiate negotiations with certain partners, thus saving costs and time and potentially reducing the number of rejected applications.

CONCLUSION

The defence industry is a traditional sector of the Slovak economy and it has undergone fluctuations over several decades. The collapse of the communist regime in 1989 and the subsequent conversion of military production to civilian purposes represented a significant milestone in the development of the sector, with lasting implications to the present day. The period following 1989 was characterized by a lack of interest in the SDI and national defence in general, influenced by pacifist government policies. The repercussions of this approach have become more apparent since February 24, 2022, and have exposed vulnerabilities in Slovakia's security posture.

In the essay, we tried to cover specific aspects of doing business in the defence industry. Firstly, we described the territorial structure of SDI export, which did not change much and does not even have a perspective to change in the upcoming years. Secondly, we emphasized the resistance of SDI to FDI and the impact of this approach. Thirdly, we discussed the importance of human capital in SDI. A sufficient number of qualified employees is the biggest challenge for Slovakia. If the country fails in this case, it will lead to the destruction of SDI with all its negative impacts on the

modernization of the AF SR, thus influencing the defence of Slovakia. Moreover, it will lead to socioeconomic problems. Fourthly, we analysed Slovak legislation related to the trade with military products.

In conclusion, Slovakia still has much to accomplish in the realm of the defence industry. Even though SDI enterprises are not lacking orders, the war in Ukraine cannot be used as a justification for not improving this sector. To assist SDI both domestically and abroad, we have proposed several measures. However, these recommendations necessitate the political leadership's willingness, a systematic long-term oriented approach, and interinstitutional cooperation between ministries and other interested stakeholders.

REFERENCES

Aktuality.sk. 2023. “Zbrojárska spoločnosť DMD Group ivestuje tento rok milióny eur do modernizácie”. Last modified January 26. Accessed 30.01.2023. https://www.aktuality.sk/clanok/QFgAMVG/zbrojarska-spolocnost-dmd-group-investuje-tento-rok-miliony-eur-do-modernizacie/.

Čechák, Oldřich., et. al. 1993. Zbrojní výroba - konverze - obranyschopnost. 1. ed. Praha: Magnet-Press.

Central Office of Labour Social Affairs and Family. 2022. “Nezamestnanosť - mesačné štatistiky 2022”. Accessed 26.01.2023. https://www.upsvr.gov.sk/statistiky/nezamestnanost-mesacne-statistiky/2022.html?lang=sk&page_id=1153450.

Chovančík, Martin. 2018. “Defense Industrialization in Small Countries: Policies in Czechia and Slovakia” Comparative Strategy, no. 4 (August): 272-85. Accessed 26.12.2022. https://doi.org/10.1080/01495933.2018.1497321.

DMD Group. 2022. “DMD Group a Trenčianska univerzita prehĺbia spoluprácu”. Last modified October 4. Accessed 06.01.2022. https://www.dmdgroup.sk/novinky/dmd-group-a-trencianska-univerzita-prehlbia-spolupracu/.

Government of the Slovak Republic. 2021. Program Statement of the Government for the period 2021-2024.

Ivánek, Ladislav. 1994. “Economic Problems of the Conversion of the Arms Industry” Perspectives, no. 3: 131–39.

Ivánek, Ladislav. 2002. “Ekonomické aspekty konverze české (československé) zbrojní výroby.” Obrana a strategie, no. 1: 133–38. Accessed 25.12.2022. https://www.obranaastrategie.cz/cs/archiv/rocnik-2002/1-2002/ekonomicke-aspekty-konverze-ceske-ceskoslovenske-zbrojni-vyroby.html.

Konštrukta - Defence. 2022. Annual Report 2021. Accessed 03.01.2023. https://www.registeruz.sk/cruz-public/domain/accountingentity/show/401675.

Letecké opravovne Trenčín. 2022. Annual Report 2021. Accessed 29.12.2022. https://www.registeruz.sk/cruz-public/domain/accountingentity/show/127533.

Mesároš, Oldřich. 1996. "Vývoj zbrojního průmyslu v Československu v letech 1945–1992." Acta Oeconomica Pragensia: vědecký sborník Vysoké školy ekonomické v Praze, no. 3: 201–16.

Ministry of Defence of the Slovak Republic. 2016. White Paper on Defence of the Slovak Republic 2016.

Ministry of Defence of the Slovak Republic. 2022. "Slovensko a Fínsko podpísali medzivládnu dohodu o akvizícií bojových obrnených vozidiel 8x8". Last modified August 30, Accessed 29.12.2022. https://www.mosr.sk/51903-sk/slovensko-a-finsko-podpisali-medzivladnu-dohodu-o-akvizicii-bojovych-obrnenych-vozidiel-8x8/.

Ministry of Defence of the Slovak Republic. 2022. Long-term development plan of the resort of Ministry of Defence with a prospect until 2035.

Security and Defence Industry Association of the Slovak Republic. 2022. "Security & Defence Technologies Catalogue" Accessed 27.12.2022. https://www.zbop.sk/files/2022/04/zbop-katalog-2022.pdf.

Slovak Investment and Trade Development Agency. 2022. Automotive Sector in Slovakia.

Slovak Investment and Trade Development Agency. 2022. Machinery & Equipment Industry in Slovakia.

Stockholm International Peace Research Institute. "The SIPRI Top 100 Arms-Producing and Military Services Companies, 2021". Accessed 31.12.2022.

https://www.sipri.org/publications/sipri-top-100-arms-producing-and-military-services-companies-2021.

The Observatory of Economic Complexity. “Where does Slovakia export Military Weapons to? (2020)”. Accessed 31.12.2022. https://oec.world/en/visualize/tree_map/hs92/export/svk/all/199301/2020/

Trend. 2022. “Naď dúfa, že rozpočet bude schválený. Fungovanie v provizóriu si nevie predstaviť”. Last modified December 3. Accessed 10.01.2023. https://www.trend.sk/spravy/dufa-rozpocet-bude-schvaleny-fungovanie-rozpoctovom-provizoriu-nevie-predstavit.

Yar, Lucia. 2022. “V Aliancii sa diskutuje o možnosti vyrábať na Slovensku muníciu pre Ukrajinu”. Euractiv, December 29. Accessed 01.01.2023. https://euractiv.sk/section/obrana-a-zahranicie/news/v-aliancii-sa-diskutuje-o-moznosti-vyrabat-na-slovensku-municiu-pre-ukrajinu/?fbclid=IwAR0HCGwlCeWNlnInBMnd2_qfSXALymHBO6VhroiE0HP_m04YfLRnQUe9Iic.

ZTS Špeciál. 2022. Annual Report. 2021. Accessed 03.01.2023. https://www.registeruz.sk/cruz-public/domain/financialreport/show/8020905

ZVS Holding. 2022. Annual Report 2021. Accessed 03.01.2023. https://www.registeruz.sk/cruz-public/domain/accountingentity/show/388962.

INTELLIGENCE AGENCIES IN THE INFORMATION AGE & THE APPLICABILITY OF OSINT

Bognár Juraj, expert consultant: Kulik Juraj

EXECUTIVE SUMMARY AND RECOMMENDATIONS

- All relevant institutions or units should be able to better utilize the potential of OSINT.
- Put more emphasis on the use of OSINT in the security domain of the state.
- Allocate more financial assets to HR to motivate highly qualified analysts to join the security forces, as well as to provide an ever-increasing budget for the acquisition of more high-tech systems.
- There is a need to emphasize precision in recognizing misinformation or disinformation in big data.
- We can observe that intelligence agencies are changing their attitude toward leaking important information that would have remained classified in the past, but in the information age, the posture toward keeping classified information is ever-changing.
- The overwhelming majority of intelligence products in the 2020s consists of approximately 80% of OSINT.
- The direct impact of the exploitation of OSINT can be observed throughout the entire duration of the Russo-Ukrainian War.
- The symbiosis between OSINT and GEOINT is undeniable.

INTRODUCTION TO INTELLIGENCE AGENCIES & OSINT

Intelligence agencies (hereafter IAs) play a crucial role in the security and foreign policy of modern states. It consists of "mainly secret activities – targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning threats and opportunities" (Gill and Phythian 2018, 5). They are also responsible for providing information and intelligence to policymakers and other government officials to conduct informed decision-making and protect national interests.

Zeman (2008) presents a more complex definition: “Intelligence is a deliberate and systematic human activity that involves all phases of the covert acquisition and processing of classified or latent information from an adversary or opponent, and its subsequent transmission to an authorised recipient. Its purpose is to answer pertinent questions and/or obtain early warning necessary to plan and execute future actions. Intelligence activities include those to protect proprietary classified information. It may also include covert preemptive and proactive interventions in an adversary's environment.”

The modern era has seen an increase in IAs, with almost every country having some form of intelligence-gathering organisation. These agencies can be divided into two main categories: civilian agencies, which operate under the jurisdiction of a country's government and are responsible for intelligence-gathering within the country's borders (not always the case, e.g. Slovak Information Service); and military agencies, which are responsible for intelligence-gathering in support of military operations and defence of the state.

Overall, IAs play a crucial role in the security and foreign policy of modern states. While their activities have sometimes been controversial, intelligence gathering is a necessary function in a complex and rapidly changing world. As such, IAs will continue to be an important part of the modern landscape.

One of the key challenges IAs are facing today is the rapid pace of technological change and the proliferation of new forms of communication. This has led to the development of new forms of intelligence gathering, such as open-source intelligence (OSINT) or cyber intelligence, which involves the collection and analysis of publicly available digital data and communications.

IAs are also facing challenges in terms of the complexity of the global security environment. The rise of non-state actors, such as terrorist organisations, private military companies, and transnational criminal networks, has made intelligence gathering more difficult. Additionally, the rise of global challenges, such as climate change and pandemics, has

increased the need for IAs to gather and analyse information from a wide range of sources.

One of the main functions of IAs is to provide policymakers and other government officials with timely and accurate information and analysis. This can include political, economic, military, and other types of intelligence, depending on the specific needs of the agency and its stakeholders.

In addition to traditional forms of intelligence-gathering, such as human intelligence and signals intelligence, modern IAs also rely on advanced analytical techniques, such as data mining and machine learning, to process and interpret large volumes of data.

INTELLIGENCE GATHERING METHODS

Intelligence gathering is the process of collecting and analysing information, and intelligence to inform decision-making and protect national interests. Intelligence-gathering methods can be divided into two main categories: human intelligence (HUMINT) and technical intelligence (TECHINT). (Michálek et al. 2013, 132)

HUMINT, according to Tóthová and Bališová (2009, 53) refers to intelligence-gathering methods that rely on human sources, such as undercover agents, informants, and defectors. HUMINT can be a valuable source of information, but it is also subject to certain limitations and biases, such as the possibility of unreliable or biased sources and the difficulty of verifying the accuracy of the information.

TECHINT refers to intelligence-gathering methods that rely on technical means, such as signals intelligence (SIGINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT). Michálek et al. (2013, 142-144) argue TECHINT can provide a wealth of information; however, it is also subject to limitations, such as the need for specialised equipment and the potential for interference or evasion by adversaries.

In addition to HUMINT and TECHINT, modern IAs also rely on a range of other intelligence-gathering methods, including open-source intelligence

(OSINT) and cyber intelligence. OSINT involves the collection and analysis of publicly available information, such as media reports and social media. On the other hand, cyber intelligence uses the collection and analysis of digital data and communications (Michálek et al. 2013, 146).

The quick rate of technical progress and the proliferation of new communication methods are two of the biggest issues IAs are currently confronting, which has led to the development of new forms of intelligence gathering, for instance, cyber intelligence. This has also raised ethical and policy questions, regarding the appropriate balance between security, privacy, and the potential for bias in the algorithms and data used by these technologies.

OSINT is a valuable source of information, as it can be accessed by anyone with an internet connection. However, it is also subject to certain limitations, due to the possibility of false or misleading information and the need to verify the accuracy and reliability of these sources. It refers to the practice of collecting, analysing, and disseminating information that is legally obtained from publicly available sources. This can include anything from news articles and social media posts to public records and government documents. IAs use OSINT to gather information about individuals, organisations, and events of interest. It is a valuable tool because it allows them to gather information from a wide variety of sources quickly and inexpensively. Nevertheless, it is important to note that OSINT should be used in conjunction with other intelligence-gathering methods, as it is only one piece of the puzzle.

Overall, IAs use a range of intelligence-gathering methods to gather and analyse information and intelligence. These methods have different strengths and limitations. Therefore, IAs must choose the most appropriate methods based on the specific needs and objectives of their mission. Additionally, IAs must also consider the ethical and policy implications of their intelligence-gathering activities, including the balance between security and privacy.

THE ROLE OF OSINT IN INTELLIGENCE GATHERING

In general, IAs strive to keep their activities and sources of information confidential to protect national security and maintain their effectiveness. However, there are instances when IAs may choose to release information to the public or leak information to the media. Releasing or leaking information to the public can be a way for IAs to shape public opinion or achieve certain policy objectives. For example, an intelligence agency may release information about a foreign threat in order to justify military action or to rally public support for a particular policy. As stated above, it is extremely rare for IAs to leak information to the media or to release information to the public, but with the ever-changing security environment around us, they can choose to do so. Notably, the first major leak of information coming from IAs occurred a few months before the Russo-Ukrainian war officially started, in October 2021 to be precise. It is possible that IAs from various NATO countries have gathered and analysed information about the intentions of the Russian Federation to invade Ukraine and some pieces of this particular information have been leaked to the media or made public.

There are also instances where IAs may release or leak information in response to public pressure or in order to correct misinformation. For example, an intelligence agency may release information in order to clarify its activities or to correct inaccurate reporting by the media.

The utilisation of OSINT is a crucial factor for intelligence services in the 21st century to be able to provide precise intelligence material for decision-making bodies (Pokorný et al. 2021, 286). OSINT represents up to 80% of the creation cycle of intelligence products nowadays, according to many sources. The biggest obstacle with the use of OSINT information is the fact that it is not always possible to effectively verify or analyse the information obtained, because of the lack of credible sources. This reality, especially in current times, is also evident in the lack of qualified personnel who can process the information quickly and efficiently into intelligence products (Laml, n.d. Práca s informáciami – posun od „need to know“ k „need to share“). Therefore, when analysing OSINT information, it is necessary to use other credible sources, such as academic texts, studies by NGOs, etc. Largely, in addition to OSINT, GEOINT information is also verified through the

creation of geo-sectors and subsequent geolocation. Then it is possible to verify the location of a target. OSINT also develops the ability to work in a space with information overload, to quickly and efficiently search for relevant data in a mass of unstructured information. This is an activity that cannot be accomplished by human effort alone. The term big data is used for this type of data.

OSINT USE DURING THE RUSSO-UKRAINIAN WAR

We have witnessed many uses of OSINT during this particular conflict with many independent sources using its full potential, for example, to help the Ukrainian civilian population with precise information on the location of Russian forces. Even some hours before the full-fledged invasion started, OSINT researchers from the Middlebury Institute of International Studies used Google Maps to track potential Russian military forces massed on the Ukrainian border. Specifically, on a road leading from the city of Belgorod, since there appeared to be a "traffic jam" in the app. Hours before, a young graduate spotted a military convoy on high-resolution images, which he obtained from a commercial satellite. All this OSINT activity began when Russian civilians posted TikTok videos in which we could clearly recognize BUK SAM launchers and other military hardware (Aldhous and Miller 2022).

As the British-based news journal The Economist (2023) suggests, the Russo-Ukrainian war gave OSINT a new breath. In the past, OSINT was not the primary source of information, but it was just a supporting element to the whole piece of intelligence-gathering methods. Nowadays, we see a clear change in the approach to using OSINT as a genuine method of gathering intelligence. Even the general public can analyse the open-source information, which is "thrown" around the internet. Based on that precise analysis, we can create an intelligence product, basically a classified document. The other methods of gathering information briefly mentioned at the beginning of this essay, namely HUMINT, SIGINT and GEOINT, are just a piece of the whole puzzle, which is being composed by OSINT in the 21st century. The whole preparation process of the Armed Forces of the Russian Federation to invade Ukraine could have been seen openly on social networks by millions if not billions of people around the world. During the whole war, we are witnessing a mass of information, which comes directly from the line of contact between both armies. This information is being

recorded on mobile phones of the soldiers or even civilians; we see images of tank battles acquired from drones, satellite imagery or other means. Thanks to commercial satellite imagery, many analysts can see the state of the Russian military airport runways, which are being targeted or even the status of stockpiles of Russian missiles or military hardware. It is estimated that the war in Ukraine has produced more of these sources of information than was produced during the entirety of the Syrian civil war. However, there is a downside to all of this, and it is the fact that this sheer amount of OSINT can produce more of a "fog of war" than the lack of information (The Economist 2023).

Another lesson from Ukraine is that IAs should give more weight to open-source data and the means to obtain and interpret it. The ultimate lesson for everyone, even government institutions, should be that it is hard for anyone to hide their "secrets" in the modern era. Spies will continue to struggle with hiding digital clues while creating plausible cover stories; we have been witnessing this problem for some time. Soldiers, too, must learn to operate in some form of a panopticon. A quick example of this is the fact that to survive, they will have to hide their radio emissions in the ambient electromagnetic noise. Recently, Russia and its soldiers paid a heavy price for carelessly using mobile phones near the frontlines, which attracted deadly accurate missile attacks.

CONCLUSION

In this essay, I explained the current status of IAs, their key challenges, and aspects of gathering information. Furthermore, I explained what OSINT is, why it is a core gathering method in the Intelligence Cycle and its use for civilian experts. It is important to say that humankind has learned not only the acquisition of information over the years but also the means of intelligence and the identification of channels for secret information. Through publicly available sources without infringing on the law, all the world's services have accessed them in recognisable ways. Often, official publications, exhibitions, advertising conferences, and ordinary people have provided missing information that complements the acquired knowledge through intelligence.

The OSINT functions properly at all levels of intelligence activities in almost every subject area, so there are many actors that use it not only for military issues but also in the private sector. Effective information retrieval using Open Source Intelligence has found its application at strategic, operational and tactical levels. In the age of technological development, the use of OSINT offers many new opportunities for IAs.

Open-source intelligence was considered of little value as an intelligence discipline until the advent of the Internet and modern communication and information-sharing applications. Failure to accept the real value of Open Source Intelligence mostly corresponded to an a priori attitude that an intelligence product could only be derived from covert information sources while working with publicly available data was considered less valuable and less interesting for intelligence activities. However, in today's changing security environment, where traditional threats are becoming more diverse and changing in their configuration, and in particular where the collection of secret data has become a lengthy, expensive and complex process, intelligence services began creating open-source intelligence knowledge. Moreover, this collection discipline has proven to be an invaluable source of knowledge outside of state activities and has therefore been fully assimilated into other spheres of public life. Furthermore, intelligence, including open-source intelligence, is no longer a function of the state alone. The collection, analytical processing and production of relevant and actionable intelligence are now typical of both state and non-state actors. In the future, however, the sheer volume of unstructured data, which will require ever more sophisticated software to collect and sort, will challenge OSINT. Because it is the largest source of information of all the intelligence disciplines, a great deal of effort will be required to extract quality and timely information from a considerable number of sources to produce actionable intelligence. At the same time, it must be pointed out that the public space is an area for spreading influence, propaganda and a variety of interests (hybrid warfare), which is why the checking of information has to be the main feature of work when dealing with the publicly available content.

In Slovakia, in my opinion, we need to develop the capabilities and capacities of various analytical units, which would be under the responsibility of

ministries or other state bodies, regarding the importance of using OSINT. Of course, it should be noted that a number of such analytical units have already been set up. There are already 14 such units in individual ministries, established under the project 'Building and developing the capacity of analytical units in selected central government bodies', the methodology for which was completed in 2020. Unfortunately, it is not possible to verify from available sources, which, if any, of these units use OSINT in their analyses.

However, there is an inter-ministerial organisational unit in Slovakia that is unique, the NBAC - National Security Analytical Centre. The complexity of the preparation of this unique project was also because the NBAC brings together, at the national level a number of entities competent in various security and defence-oriented fields. Representatives of the Slovak Information Service, the Military Intelligence, the Police, the Criminal Office of the Financial Administration, the Ministry of Foreign and European Affairs of the Slovak Republic, the National Security Authority, the General Staff of the Armed Forces of the Slovak Republic and the Office of the Government of the Slovak Republic work together on a secondment basis. Other participating state entities provide information support to the NBAC. Information products processed by the NBAC analytical unit are provided to all participating state bodies and institutions and, where relevant, to other entities under the jurisdiction of the state bodies for the purpose of decision-making and taking security measures. (Slovak Information Service)

The projected model of the central analytical service enables direct contact and flexible communication between the NBAC and the different entities. This has increased the potential to obtain more rapidly all available knowledge about a potential threat, and by concentrating it in one place, it has also enabled not only a more comprehensive analytical assessment of the potential threat but also a more timely delivery of such a product to relevant external recipients who are responsible at the national level for preventing unlawful activity or threats.

In particular, our intelligence services should have access to the best capabilities in this area. I think that it should be relatively easy to get individuals working with open source information into the intelligence system, as the information they have at their disposal at an early stage is

unclassified, which means that they could start working without security clearance, which would be processed in the meantime. This approach could save a lot of time. It would be a welcome change, as I can say that in the conditions of the Slovak Republic, we have very few developed capabilities in the field of OSINT.

Another option would be to establish a Centre of Excellence for OSINT in the Slovak Republic, which would carry out scientific and research activities in the field of OSINT, focusing in particular on proven methods and tools applicable to this type of collection, analysis, evaluation and interpretation of information, and also provide support, training and sharing of best practices to other state authorities in this area. In the Slovak Republic, we do not have such a centre established, yet.

REFERENCES

Aldhous, Peter, and Christopher Miller. 2022. “TikTok, Satellite Images, Flight Trackers Reveal Russia's Attack On Ukraine.” BuzzFeed News. Accessed 24.01.2023. https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social.

Gill, Peter, and Mark Phythian. 2018. *Intelligence in an Insecure World*. Third ed. Cambridge: Polity Press. ISBN 978-0745652795

Laml, Roman. n.d. “Spravodajstvo 21. storočia.” Asociácia bývalých spravodajských dôstojníkov, n.d., https://www.absd.sk/spravodajstvo_21_storocia. Accessed 22 January 2023.

Michálek, Luděk, Ladislav Pokorný, Jozef Stieranka, and Michal Marko. 2013. *Zpravodajství a zpravodajské služby*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. 132, 142-144, 146. ISBN 978-80-7380-428-2.

Pokorný, Ladislav, Michal Marko, Adrián Vaško, Jozef Stieranka, and Luděk Michálek. 2021. *Zpravodajské služby a zpravodajská činnost*. Praha: Wolters Kluwer ČR, 286. ISBN 978-80-7598-725-9.

Slovak Information Service. “O nás | Národné bezpečnostné analytické centrum.” Slovenská informačná služba. Accessed 14 February 2023. https://www.sis.gov.sk/o-nas/nbac.html.

The Economist. 2023. “How spies, soldiers and the public should use open-source intelligence.” Accessed 18.01.2023. https://www.economist.com/leaders/2023/01/18/how-spies-soldiers-and-the-public-should-use-open-source-intelligence.

Tóthová, Marcela, and Kristína Bališová. 2009. “Ľudský faktor v spravodajských službách - Machiavelistický typ osobnosti a jeho vhodnosť na pozíciu v spravodajských službách.” Asociácia bývalých spravodajských dôstojníkov. Accessed 22.01.2023. https://www.absd.sk/sympozium_ludsky_faktor_v_spravodajskych_sluzbach.

Zeman, Petr. 2008. “Co je zpravodajství.” Asociácia bývalých spravodajských dôstojníkov. Accessed 22.01.2023. https://www.absd.sk/co_je_zpravodajstvi#_ftn1.

THE LEGAL LIMITS OF BLOCKING DISINFORMATION FROM A NATIONAL AND EUROPEAN PERSPECTIVE

Černák Timotej, expert consultant: Kulik Juraj

EXECUTIVE SUMMARY

This analysis examines the legal implications of the Slovak Republic's efforts to combat Russian influence and the spread of disinformation through so-called alternative media. In response to this troubling phenomenon and the situation in Ukraine, the National Council has issued an Act allowing the National Security Authority to block access to these websites. This analysis also provides an exploration of the legality of these actions under current legislation and regulations from national and European perspectives.

Slovak legal framework does not define terms such as disinformation, serious disinformation, or hybrid threat. This creates a certain degree of legal uncertainty that needs to be dealt with in application practice. The current legislation encounters some logical ambiguities (tasks and responsibilities of state authorities) caused by the speed of the legislative process by which the amendment to the Cybersecurity Act was adopted. In the future, blocking the entire website may be considered a violation of Article 10 of the European Convention on Human Rights. The European Court of Human Rights underlines the proportionality of blocking measures so that not the entire website is blocked, but a specific article.

Considering the current political situation, the future of blocking is unclear, as the proposed amendment has not been adopted by the National Council. However, a future intervention of the Supreme Administrative Court of the Slovak Republic in the decision-making process in the adoption of blocking measures is expected. The analysis is based on the legal framework in force as of 28th February 2023.

INTRODUCTION

Back in the days of ancient China, the great Chinese strategist Sun Tzu (2010) said: "Fighting and conquering in all our battles is not supreme excellence, supreme excellence is to break the enemy's resistance without fighting," emphasizing the importance of hybrid activities.

Today, modern conflict does not take place on the classical battlefield. Advances in science and technology have created a new environment – cyberspace. NATO also refers to this as the so-called fifth operational domain (NATO 2022a). Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations (NATO 2022b). The problem with this new perception of reality in Slovakia is the relative unpreparedness of legislation to respond to hybrid threats.

The ongoing military conflict in Ukraine is fundamentally affecting life in the entire European geopolitical sphere, and Slovakia is no exception. The beginnings of this conflict were also accompanied by the Russian state apparatus trying to influence the internal political processes in European countries. One of the key issues this aggression has caused in Slovakia is the spread of disinformation, which disrupts the stability of the nation, especially the fragmentation of public opinion. In the early days of the conflict, the Slovak government adopted a legislative aid package to help Ukraine. Inter alia the possibility to block disinformation websites has been introduced into the Slovak legal framework. This essay examines the legal implications of the Slovak Republic’s efforts to combat Russian influence and the spread of disinformation through so-called alternative media. This analysis will provide an exploration of the legality of these actions under current legislation and regulations from a national and European perspective.

After a few months of using this tool, we have a good opportunity to look back and discuss how effective the current measures are, and how they can be improved. In this essay, we are going to examine the legal conditions and limits of this institute.

The essay is divided into two parts. In the first part, we will look at the current legislation and how it has worked so far. We will also look at what

kind of interference with the fundamental rights and freedoms of citizens the blocking itself represents. The second part of this essay is devoted to possible future de lege ferenda proposals.

DISINFORMATION AS A LEGAL TERM

What is disinformation? Disinformation is an indefinite legal term in the Slovak legal framework. And we are highlighting that. On the other hand, the National Security Analytical Centre (NBAC), which is an organizational structure of the Slovak Information Service (SIS), defines disinformation as information that is verifiably false, misleading, or manipulatively presented information, which is intentionally created, presented, and disseminated with the clear intent to deceive or mislead, to cause some harm, or to secure profit (e.g., economic, or political). Disinformation often contains an obviously true element, which adds to its credibility and may make it more difficult to detect. Disinformation does not include unintentional errors in reporting, satire, and parody, nor does it include news and commentary favouring one side that is clearly labelled as such (SIS 2020).

We can conclude that disinformation is false or misleading information that is spread deliberately to deceive or influence people. It is often spread through social media, websites, and other digital platforms. We distinguish disinformation from misinformation, which is false or inaccurate information that is spread unintentionally or without malicious intent. This may be the case where individuals spread information in good faith on social media without knowing that it is false (SIS 2020). In other words, intent is the main distinguishing criterion between these terms.

Although the NBAC has created a hybrid threat glossary that encompasses this concept, the legal definition of disinformation in the Slovak legal framework remains unclear. This creates a degree of legal uncertainty and leads to a lack of clarity on how to effectively combat the spread of false and misleading information in Slovakia. This fact causes some serious problems in application practice, which we need to respond to in the future. As soon as possible.

NATIONAL LEGISLATION AND LEGAL LIMITS OF BLOCKING

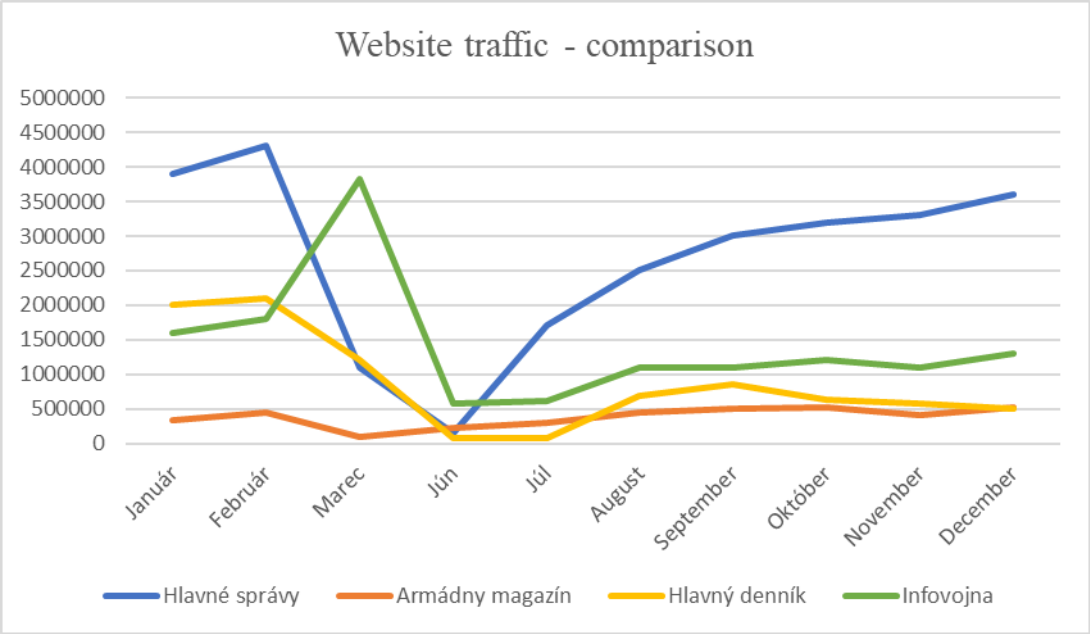
In response to Russia's military intervention and the so-called special operation in Ukraine, the Slovak government, like the rest of Europe, was forced to take appropriate countermeasures. This was even more important as Ukraine directly shares a border with the Slovak Republic. In response to the external threats represented by the conflict in Ukraine, as well as the internal threats, on February 25, 2022, the National Council adopted Act No. 55/2022 Coll. on certain measures in response to the situation in Ukraine. Through this Act, the Parliament decided to amend a number of laws. Inter alia, the Cybersecurity act. This, and the speed with which this legislation was adopted – the law was adopted in one day through the so-called fast-track legislative procedure, causes problems in practical application. We believe that it would be appropriate to amend the Cybersecurity Act separately, or another option is to create a completely new legislative act that would establish the material and procedural conditions for blocking. This option is acceptable considering that the Cybersecurity Act will have to transpose the new European NIS2 Directive. Knowing the quality of Slovak lawmakers, such a solution is highly desirable.

The new legislation introduced the possibility of blocking disinformation websites. This measure has been entrusted to the National Security Authority (NSA). According to the newly added Article 27b of the Cybersecurity Act, the NSA can decide and execute blocking on its own initiative. It also determines the method of blocking. This legislative amendment limited the possibility of blocking until June 30, 2022.

Furthermore, the amendment added a new Article 27c to the Cybersecurity Act. Its purpose is to allow the NSA to carry out blocking at the request of another state authority. Under the current state of the law, the legal wording of Article 27c is problematic. Although the Cybersecurity Act states that it is a request from another (authorized) state authority, the explanatory note to Act No. 55/2022 Coll. specifies that the request is interpreted as an enforceable decision (National Council of the Slovak Republic 2022a). From a legal point of view, the SIS has the status of an administrative body only in matters of service in relation to its officers, disclosure of information under the Freedom of Information Act and in matters relating to the protection of classified information, according to several Acts (Acts No. 73/1998, 211/2000,

215/2004 Coll.). Thus, it is not legally possible for the SIS to issue administrative decisions.

Four websites were blocked because of this measure (hlavnespravy.sk, armadnymagazin.sk, hlavnydennik.sk, infovojna.sk). At the end of this period, i.e., at the end of June, the Parliament adopted Act No. 231/2022 Coll., which extended the possibility of blocking until September 30, 2022. Currently, the NSA is unable to effectively use this measure, although it has the legal authority to do so. The authority exists, but not the ability to use it. Blocking is showing itself to be an effective tool in the hands of the state in the fight against disinformation. The attached graph shows that the four previously mentioned websites have not reached the same peak in website traffic as they used to.



Disinformation websites traffic overview in 2022. Source: NBAC

The blocking itself aroused a wave of controversy. The first amendment did not specify what "serious disinformation" means. Like the term "disinformation", this term also remains legally indefinite. Struhárik (2022) criticizes that the NSA argued by using the dictionary of the Slovak language when explaining the reasons for the decision to block hlavnespravy.sk. It should be added, that in this case, evidence of the activities of the Russian intelligence service came to light. One of its officers communicated with and corrupted an associate of hlavnespravy.sk (Tódová 2022).

The current status quo causes and may continue to cause in the future, problems in the practical application of how to identify disinformation. It is also necessary to determine how to restrict access to blocked sites, for example, whether these sites should be redirected to some government sites or educational sites (Husovec 2022). Users and visitors to these websites should know why the site is unavailable, for example, in the form of a graphic notice.

INTERFERENCE WITH FUNDAMENTAL RIGHTS AND FREEDOMS

The second element, besides the legal boundaries, is the human rights aspect. For instance – freedom of speech, freedom of expression, right to information, etc. On the other hand, there are values that are important for the proper functioning of the state, such as national security, national interests, or border protection.

As a member of the Council of Europe, the Slovak Republic is bound by the European Convention on Human Rights (ECHR, the Convention). Article 10 of the Convention provides for the right to freedom of expression, subject to certain restrictions that are "in accordance with the law" and "necessary in a democratic society".

Under national law and in accordance with Article 2 (2) of the Constitution of the Slovak republic (the Constitution): State bodies may act solely on the basis of the Constitution, within its scope and their actions shall be governed by procedures laid down by law. In combination with Article 26 of the Constitution: Freedom of expression and the right to seek and disseminate information may be restricted by a law only if it is regarding measures necessary in a democratic society to protect the rights and freedoms of others, national security, public order, protection of health and morals.

The aforementioned means that freedom of expression does not include situations in which people threaten others, spread alarming messages related to public health, or spread disinformation. Freedom of expression is therefore not unlimited – it has its limits.

The state's interest in combating disinformation is objectively justified. It is an interest in the protection of the common welfare pursuing the public good, but state measures must be proportional in their substance, form and purpose based on the law or an international treaty (Telec 2022).
The Constitutional Court of the Slovak Republic (1997) said that the balance between the public and private interest is an important criterion for determining the proportionality of the restriction of each fundamental right and freedom. The proportionality of the interference with fundamental rights and freedoms needs to be considered.

The European Court of Human Rights (ECtHR) in its case law clearly concluded that blocking access to an entire website is an extreme measure, comparable to banning a newspaper or a television station, while deliberately neglecting the differences between lawful and unlawful information, also such a measure disregards the distinction between the legal and illegal information the website may contain and renders inaccessible large amounts of content which have not been identified as illegal (OOO Flavus and Others v. Russia 2020). Imagine a situation where the Slovak news portals such as SME or Denník N publish a disinformation article. Would it be appropriate to block access to the entire site? Would it not be more reasonable to target only the specific article?

The ECtHR also states that the use of blocking measures without prior court approval constitutes prior censorship. In extremis, such a measure could also lead to the censoring of dissenting opinions or criticism of the government, which would further undermine the ability of citizens to freely express themselves. In addition, the possibility to allow state authorities to block websites without a court-approved decision could also lead to an abuse of power. Without a court to check their actions, the ruling political establishment could potentially use its power to target websites for political reasons, or even to silence opponents. We need to set precise and transparent criteria to avoid the creation of an Orwellian Ministry of Truth.
Lastly, the principle of the foreseeability of the law must also be considered. In a case in which the owner of a website had been obliged, to avoid blocking his entire website, to remove information prohibited by the domestic courts on filter-bypassing tools, the ECtHR held that the legislative basis for the order did not give the courts or owners of Internet sites any indication as to

the nature or categories of content that was likely to be banned, and thus failed to satisfy the foreseeability requirement (Engels v. Russia 2020).

The blocking of the Slovak disinformation websites may have violated Article 10 of the Convention. This was caused by the inconsistency of the lawmaker, who ignored the ECtHR case law when adopting Act No. 55/2022 Coll. However, it must be said that the measure taken under the Cybersecurity Act has not been heard before the ECtHR.

THE FUTURE OF THE BLOCKING MECHANISM AND DE LEGE FERENDA PROPOSALS

Within the framework of the tripartite division of state power in a democratic society, it is necessary to involve the courts in the blocking process. The court's involvement is even more necessary if the decision is based on classified information. Pursuant to Article 34 of Act No. 215/2004 Coll. on the Protection of Classified Information, judges have a special status as persons who may be acquainted with classified information.

The above is also reflected in the proposed amendment (National Council of the Slovak Republic 2022b) to the Cybersecurity Act so that the NSA can once again block harmful content that has or may have the effect of harming or endangering security, foreign policy, or economic interests. The current proposal defines in a footnote the following entities that may request blocking under Article 27b of the Cybersecurity Act: the Slovak Information Service, the Military Intelligence Service, the Police and the Ministry of Interior. The subsequent blocking order should be issued by the Supreme Administrative Court of the Slovak Republic, and the NSA will execute the blocking. It is surprising that the legislator omitted the Ministry of Defence but included its branch service (military intelligence) in these provisions. It would be more appropriate to identify the empowered public bodies in the field of national defence and security by a demonstrative enumeration in the normative part of the Act (not in a footnote which has no normative relevance).

Blocking under Article 27c is a different legal regime of blocking, but it has its grounds. In our view, it would be appropriate to regulate it differently than it is now. In exceptional cases, where there is support for terrorism,

extremism or support for a harmful cultist group, the legitimate authority in the field of defence and security would apply to the court for a blocking order. Therefore, it would proceed in the same way as in criminal proceedings when requesting the deployment of information and technical equipment. If the court approves and issues a blocking order, it becomes an enforcement title and will be delivered to the internet service provider. If the domains and websites are registered abroad, the order will be delivered to the NSA, which will technically carry out the blocking.

Nevertheless, the amendment still provides for the possibility of blocking entire websites, which may be legally problematic in light of the case law of the ECtHR. It would not be a bad idea to consider the creation of a system of sanctions whereby, following prior notification by the state and a breach of the legal obligation to remove harmful content, blocking by the NSA would take place based on a prior court order.

Greater transparency is provided by the fact that the NSA would have to make blocking decisions publicly available on its website. However, at the beginning of February, the Parliament did not pass this proposal to the second reading. We believe that in the case of extraordinary circumstances, which should be understood as national security, public order protection of health and morals, and if necessary, in a democratic society, and based on the knowledge of the operational activities of the intelligence services or the police force, there could be a blocking of the entire site. All of this should be based on the evidence in court proceedings, and in the future, the criminal liability of those who commit such acts should not be excluded.

CONCLUSION

Hybrid threats are an old concept with new capabilities and technologies, in which the dependence of states on modern technologies is emerging. In addition, liberal democracy, because of the values on which it is built, is particularly vulnerable to them. In the concept of hybrid conflicts, disinformation is one of the most effective and cheapest weapons. This creates an obligation for states to adapt their national legislation to be more resistant to them.

The problem with hybrid activities is that they do not reach such an intensity that these actions would be considered administrative or criminal offences. Moreover, such conduct is not regulated by the law because the legislator has not yet defined it in the legal framework. Ultimately, the state does not have effective tools to defend itself and the actors of hybrid operations enter the so-called "grey zone" in which they operate with impunity.

The blocking institute in Slovakia has its justification, but its future regulation must be part of professional legal discussions, considering the ECtHR case law. It should be the subject of further debate whether this measure should be regulated in a separate Act. It is also necessary to resolve the question of how to protect this instrument from being misused and how much of an infringement of fundamental rights and freedoms its use causes. The current and proposed statutory regulation assumes that the NSA will only be the executor of decisions of authorized state bodies which do not derive this authorization from their statutory mandate. Lastly, it is necessary to create a legal definition of the terms "disinformation" and "hybrid threat" and prepare Slovak legislation for the new challenges that the information age of the 21st century brings.

REFERENCES

Constitution of the Slovak Republic (46/1992 Coll.).

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights).

ECtHR, Engels v. Russia, app. no. 61919/16. June 23, 2020. https://hudoc.echr.coe.int/eng?i=001-203180.

ECtHR, OOO Flavus and Others v. Russia, app. no. 12468/15, 23489/15, 19074/16. June 23, 2020. https://hudoc.echr.coe.int/eng?i=001-203178.

Husovec, Martin. 2022. "Súčasné blokovanie dezinformačných stránok je ústavne problematické. Čo s tým?" Denník N, April 22, 2022. Accessed 25.01.2023. https://dennikn.sk/2818631/sucasne-blokovanie-dezinformacnych-stranok-je-ustavne-problematicke-co-s-tym/.

National Council of the Slovak Republic. 2022a. Explanatory Note to the Act No. 55/2022 Coll on certain measures in response to the situation in Ukraine. Accessed 25.01.2023. https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=507894.

National Council of the Slovak Republic. 2022b. Draft amendment to the Cybersecurity Act. November 9, 2022. Accessed 25.01.2023. https://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=8989.

NATO. 2022a. "Multi-Domains Operations Conference – What We Are Learning." Last modified April 8, 2022. Accessed 25.01.2023. https://www.act.nato.int/articles/multi-domains-operations-lessons-learned.

NATO. 2022b. "NATO's response to hybrid threats." Last modified June 21, 2022. Accessed 25.01.2023. https://www.nato.int/cps/en/natohq/topics_156338.htm.

Šamko, Peter. 2022. "Blokovanie webových stránok a jeho možný rozpor s judikatúrou Európskeho súdu pre ľudské práva." Published 26.02.2022.

Accessed 25.01.2023. http://www.pravnelisty.sk/clanky/a1062-blokovanie-webovych-stranok-a-jeho-mozny-rozpor-s-judikaturou-europskeho-sudu-pre-ludske-prava.

SIS. 2020. "O nás." NBAC – Krátky terminologický slovník HYBRIDNÉ HROZBY. Accessed 25.01.2023. https://www.sis.gov.sk/o-nas/nbac-slovnik-hh.html.

Slovakia, Act No. 215/2004 Coll. on Classified Information Protection.

Slovakia, Act No. 231/2022 Coll.

Slovakia, Act No. 46/1993 Coll. on the Slovak Information Service.

Slovakia, Act No. 55/2022 Coll. on certain measures in response to the situation in Ukraine.

Slovakia, Act No. 69/2018 Coll. on Cybersecurity (the Cybersecurity Act).

Struhárik, Filip. 2022. "Štát už mesiac tají konkrétne dôvody blokovania dezinformačných webov. V rozhodnutí argumentuje aj slovníkom slovenčiny." Denník N, March 31, 2022. Accessed 25.01.2023. https://dennikn.sk/2791298/stat-uz-mesiac-taji-konkretne-dovody-blokovania-dezinformacnych-webov-v-rozhodnuti-argumentuje-aj-slovnikom-slovenciny/.

Telec, Ivo. 2022. "Dezinformace jako právní problém." epravo.cz, July 12, 2022. Accessed 25.01.2023. https://www.epravo.cz/top/clanky/dezinformace-jako-pravni-problem-114968.html.

The Constitutional Court of the Slovak Republic. PL. ÚS 7/96. February 27, 1997.https://www.ustavnysud.sk/ussr-intranet-portlet/docDownload/824628d7-b062-47db-b7db-586a68bb28b4/Rozhodnutie%20%20N%C3%A1lez%20PL.%20%C3%9AS%207_96.pdf.

Tódová, Monika. 2022. “Ako sa verbujú špióni na Slovensku: Povedal som v Moskve, že si dobrý chlapec.” Denník N, March 15, 2022. Accessed 25.01.2023. https://dennikn.sk/2767779/ako-sa-verbuju-spioni-na-slovensku-povedal-som-v-moskve-ze-si-dobry-chlapec-video/.

Tzu, Sun. 2010. The Art of War. PDF. Capstone Classics. Chichester, England: Capstone Publishing. https://sites.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf.

ANALYSIS OF THE IMPACT OF ELECTORAL DISINFORMATION NARRATIVES IN THE UNITED STATES

Denciová Mária, expert consultant: Húsková Eva

EXECUTIVE SUMMARY AND RECOMMENDATIONS

In this essay, we address the issue of election disinformation. The essay focuses on the period from 2016 to the present. We aim to show how serious problems disinformation poses for the electoral process and democracy in the US, but we also show that it can be deadly, through the example of the attack on the Capitol. The main actors are, for example, Donald Trump, the QAnon movement, and the Stop the steal movement. In one of the chapters, we also focus on the last midterm elections in 2022 and use this as an example to point out possible improvements in this situation. From our analytical essay, we draw several results and subsequent recommendations;

- Restrictive electoral laws are not a guarantee of safe elections, quite the opposite as they put more pressure on the electoral commission and other participants in the electoral process.
- It is necessary to create a welcoming environment and support for staff involved in the preparation of elections, as they are the gatekeepers of democratic processes.
- The most frequent disinformation must be debunked and actively communicated to the general public.
- It is essential to personalize the content to the target groups, both in format and language, especially for non-native speakers and other ethnic groups.
- Greater regulation of social network content and greater accountability of technology giants is needed.
- At the same time, there is a need for greater accountability of stakeholders - governors, the president, and political actors.

INTRODUCTION

Disinformation is extremely dangerous and poses a risk to people and often to the democratic system. This is evidenced by the course of the 2016 US presidential election and the subsequent 2020 and 2022 midterms. In this

essay, we look at why election disinformation is a problem and what events are behind it. Specifically, we focus on misinformation and disinformation in the 2022 midterm elections. In the essay, we take a closer look at a specific selected state - Texas.

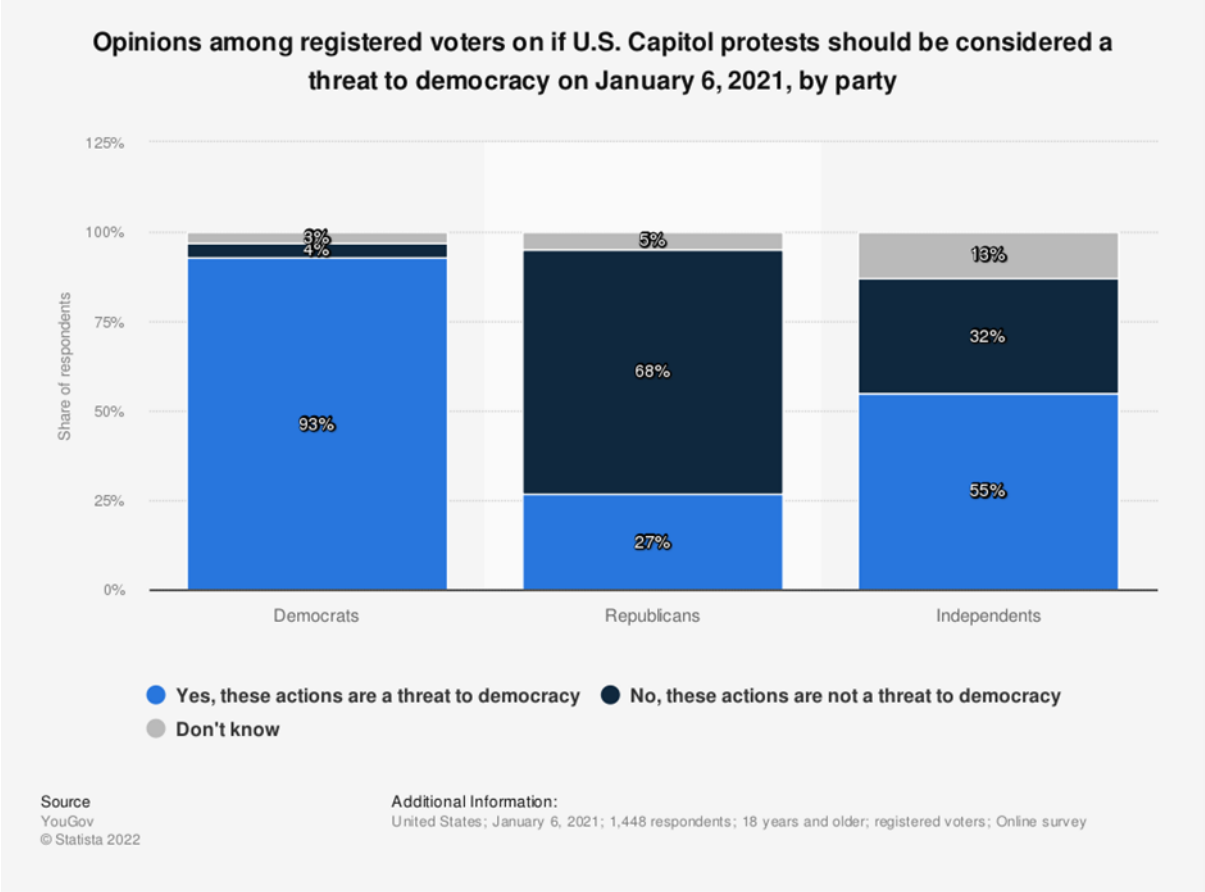
To understand the dangers of misinformation and disinformation, it is necessary to define them. Misinformation is false information that is spread regardless of whether there is intent to mislead. On the other hand, disinformation is deliberately misleading or biased information, manipulated narratives, or facts. Similar to the term fake news, it is deliberately created, sensational, emotionally charged, misleading, or completely fabricated information that mimics the form of mainstream news.

The first chapter of this essay focuses on why disinformation poses a threat to democracy, the second chapter describes the state of play in the United States. The third - and the core analytical chapter - digs deeper into that matter through the prism of a case study of the Texas midterms in 2022. Last but not least, based on the case study of Texas, this analytical essay has the ambition to draw several recommendations on how to avoid and tackle disinformation in the case of the U.S. elections, which are part of the conclusion of this essay.

DISINFORMATION AS A THREAT TO DEMOCRACY

Disinformation is perceived as a threat to democracy not only by researchers and other stakeholders but also by the general public. More than two-thirds of Americans (sixty-nine per cent) believe disinformation is a major problem in society, up from sixty-three per cent in 2020, research finds. Seventy per cent believe that disinformation has a negative effect on society and well-being. Seventy-one per cent said falsehoods exacerbate political polarization. Seventy-three per cent feel that disinformation undermines election processes and seventy-five per cent think deliberate attempts to mislead the public threaten democracy. While Republicans and Democrats differed by as much as forty percentage points on trust in the media, both parties agreed that local news sources are the most trusted (overall, sixty-four per cent trust local broadcasters and sixty-three per cent trust local newspapers). Forty per cent of respondents said they avoid

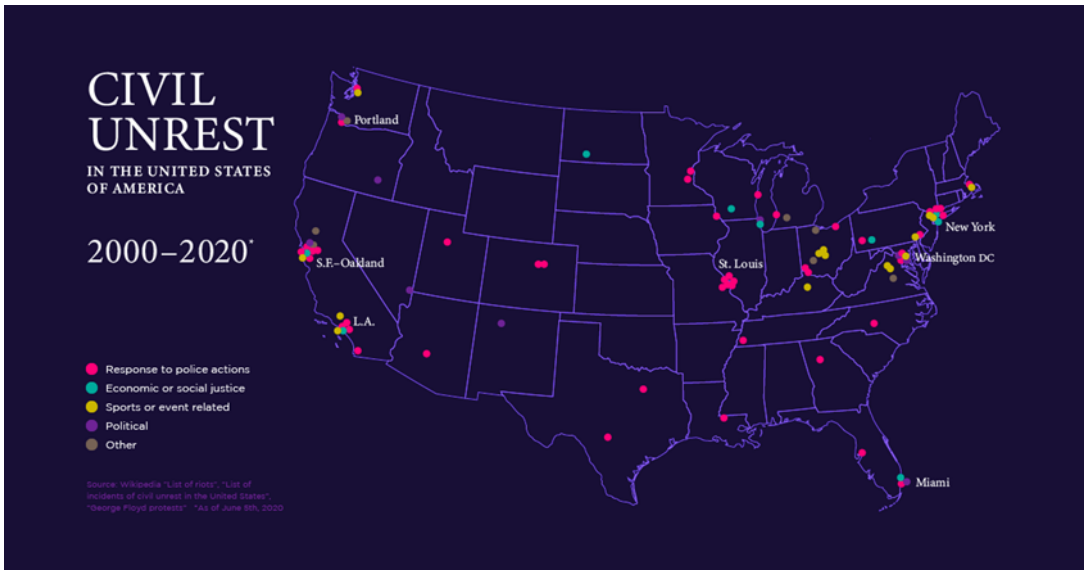
watching or listening to the news because of the disinformation they encounter there, up from thirty-one per cent in 2020. Respondents differed significantly in their beliefs about who is most responsible for countering disinformation - and in their assessment of how these parties are fulfilling this responsibility. Sixty-seven per cent said President Joe Biden is the person "most responsible" for combating disinformation, but only twenty-one per cent believe he has done "very well" in fulfilling that responsibility (Institute for Public Relations 2022). These numbers show that the general public in the United States is well aware of the fact that disinformation poses a real threat to democracy, may cause friction, and could fuel polarization. Unfortunately, the disinformation in the American information space for the past few years has been booming.



Graph 1. Opinions among registered voters on the U.S. Capitol protests should be considered a threat to democracy on January 6, 2021, by a party (Statista 2021)

THE RECENT BOOM OF DISINFORMATION CIRCULATION IN THE US

As the 2016 election approached, the U.S. was faced with foreign entities infiltrating its information space. Russia was involved in some of this, but other countries likely played a role as well. They created fake news and shared it on social media platforms, as well as amplified false narratives. The intent of their posts was very clear. They pick hot topics where American society is divided as a nation, such as gun rights, race-related matters, and immigration issues, and have used that as a weakness against Americans to fuel polarization. Their overall goal has been to divide the US and make the polarized groups fight each other from the inside. If they can get people to fight each other from the inside, they do not have to do anything, they're already winning (Marineau 2022). And they have been very successful. If you look at the social unrest that has been erupting on the streets during the elections and also afterwards, part of it had to do with some of the fake news spread on social media.



Graph 2. Civil unrest in the US from 2000 to 2020 (Routley 2020)

In 2016, a misleading tweet caused a shooting in Washington DC. A man brought a rifle into a pizza shop and opened fire. Fortunately, no one was hurt and the suspect was arrested, but the motive for the crime and the circumstances that triggered it were shocking. False tweets circulated on the Internet claiming that the pizza shop was the base of a paedophile sex ring involving the Democratic presidential candidate Hillary Clinton, the former Secretary of State, and members of her campaign. The pizza shop operators began receiving threats from right-wing activists who believed the reports to be true. The hashtag "#pizzagate" appeared the day before the

presidential election vote. Even after Ms Clinton's defeat the next day, the tweets did not die down and instead continued to spread. Although social media subsequently banned pizzagate-related posts, the threats did not cease, culminating in the appearance of a 28-year-old man from North Carolina who showed up at the store with a rifle to conduct his own "investigation" (Miller 2021). According to an interview in the New York Times with the suspect after his arrest, he was a gentle, polite man who was intent on saving the children trapped in the store (Lipton 2016).

In the United States, identity, especially race, plays a key role in the messages and strategies of disinformation producers and those with whom disinformation and misinformation resonate. The expansion of what "counts" as misinformation shows that a unique system of the media landscape in the United States that is based on partisan preferences and consists of partisan media (either left-leaning or right-leaning) in line with the 1st Amendment of the Constitution, has an indirect impact on misinformation circulating in the information space. Misinformation or even borderline disinformation is usually used by right-wing media outlets to reproduce and reinforce white supremacy and hierarchies of power at the expense of populations that do not have social, cultural, political, or economic power. The victory of Donald Trump over Hillary Clinton in the 2016 U.S. Presidential election took elites by surprise. The popular theory that Trump won because he appealed to the economic anxieties of a "white working class" has been contested. Evidence suggests that Trump's electoral college victory was instead due to his messaging to white voters that traditional white American economic, political, and social status was under threat (Chokshi 2018).

In particular, disinformation was at its peak during the period when the 2020 election results were announced, i.e. at the time of Donald Trump's defeat. Trump's subsequent reaction of rejecting the election results was accompanied by the disinformation narrative on various social media platforms (Parlor, Signal, Telegram) and culminated in an attack on Capitol Hill. The mounting pressure in society in combination with his misleading words, various disinformation and misinformation campaigns as well as Trump's incitement to riot led to 6 people being killed, dozens injured, and

evident property damage. The troubled certifying of the election posed a threat to the US democratic system (NY Times 2022).

After the attack, the executive board of Twitter decided to suspend Donald Trump's account on Twitter. However, this did not prevent the spread of disinformation narratives. On January 30 of this year, after two years of being banned, social networks such as Facebook, Instagram, and Twitter decided to lift Donald Trump's ban and allow him to return to these social networks (Gregorian 2023). One of the most well-known Trump supporters and disinformation actors are the members of the QAnon movement. In the 2020 presidential election but also the 2022 midterm elections, the "Stop the steal" movement also appeared on the disinformation scene. Disinformation has been causing problems in US elections for years, and it also did in the 2022 midterm elections (Spring 2020).

DISINFORMATION IN 2022 MIDTERM ELECTIONS

In the context of an election, there are three primary effects that election disinformation can have on voters; first, whether they choose to vote at all; second, whom they vote for; third, if they believe in the outcome of the election. Following the 2020 general election, the latter motivated the attack on the U.S. Capitol on January 6, 2021. Mis- and disinformation narratives furthered false allegations suggesting that voters could not trust in the outcome of the election, that the election had been "rigged" or "stolen". The January 6th insurrection illustrates that the national security implications of mis- and disinformation are not confined to the online space, but can result in real-world acts of political violence. Recent reports of foreign actors seeking to utilize online disinformation to influence Americans also illustrate the national security threat posed by the proliferation of dis- and misinformation.

False claims and conspiracy theories about voting and the electoral process spread through the information space almost immediately after the votes were cast (Intelbrief 2022). President Donald Trump and other prominent right-wing figures seized on technical problems in some key states to baselessly suggest there had been intentional malfeasance. Trump also made a baseless claim of mass voter fraud. Trump, who has repeatedly and falsely claimed that there was massive voter fraud in the 2020 election,

posted on social media an unsubstantiated claim that such fraud is occurring in the 2022 midterms as well (Wendling 2022). “Is voter fraud happening the same thing that happened in 2020?” the former president wrote on his Truth Social platform. According to the Threats and Harassment Dataset, built by researchers at Princeton University and the Anti-Defamation League, of the 400 cases of threat and harassment observed between January 1, 2020, and September 23, 2022, forty per cent were related to elections, with almost fifty per cent of those incidents occurring around the 2020 general election. The data also shows that Pennsylvania, Georgia, Michigan, Wisconsin, and Arizona are the states with the highest share of threat and harassment incidents against poll workers (Princeton 2022).

Monitoring and analysis by The Soufan Center and Limbik’s Information Defence System have yielded insight into mis- and disinformation narratives proliferating online ahead of the midterm elections. One group of mis- and disinformation narratives that have steadily been increasing online over the past month are those that further false allegations of election fraud or tampering with election results. For example, a month before, the daily volume of disinformation narratives across thousands of different online sources—including social media platforms, news publishers, blogs, and online forums, purporting that the election is rigged or will be stolen, has dramatically increased, by two hundred sixty-eight per cent (Intelbrief 2022).

One of the disinformation narratives was the inducement to check wifi connections at polling stations. The conspirators claimed that voting machines are connected to the wifi network and change your vote. “Check for Wifi connections, both inside & outside poll locations. Election machines should not be connected to the Internet. Take a screenshot to report irregularities for investigation,” read one tweet. In reality, the “voting machines” that mark ballots are not usually directly connected to the Internet, despite the cries of election conspiracy theorists. Larger voting systems may be connected to the Internet, often to use the election management software used to program the machines and test them, but this is assumed to occur before voting. Polling places in many states use WiFi to access electronic poll books to verify voter eligibility (Person 2022).

AN ANALYSIS OF THE SELECTED US STATE OF TEXAS AND REACTIONS TO DISINFORMATION ABOUT THE ELECTION

The electoral process in Texas has always been a difficult one, but as of 2020 the scrutiny elections administrators face has grown, even in small Republican-controlled counties that former President Donald Trump carried. Allegations of foreign interference in the 2016 presidential election have sparked public fears about the integrity of the election. And conspiracy theories about voter fraud in the 2020 presidential election have led to increased scrutiny. The increased demands have caused some workers to burn out. According to the Secretary of State's office, 30 per cent of Texas poll workers have left their jobs since 2020. In Gillespie county, an entire elections office resigned after citing threats against the staff and dangerous misinformation in the community. Larger counties in Texas are experiencing even more public scrutiny. In Williamson County, the elections administrator's office has handled nearly 100 requests for public information this year, more than in the previous six years combined. Texas has some of the most restrictive voting laws in the country. And after the 2020 presidential election, Texas was one of 18 states to pass even more restrictive laws (Burges 2022). The law includes several changes: a ban on drive-thru voting and 24-hour voting sites, increased penalties for voting crimes, more protections for poll watchers, and new voter assistance rules (Ura 2021). Despite these strict election laws, Texas has not escaped misinformation and questions about the conduct of the 2022 election. For example, Texas Scorecard, a self-described citizen journalism group, posted a video on YouTube claiming without evidence that Beto O'Rourke, the Democratic candidate for governor in Texas, had sent pre-filled voter registration applications to dead people. Texas officials validated all voter registration applications. The video was viewed at least 5,000 times (Texas Scorecard 2022). In addition, Texas also struggles with the problem of Hispanic voters. The Hispanic vote is a big battleground in last year's midterm election, potentially holding the key to which party controls the House of Representatives. That is especially true in Texas, where Republicans and Democrats are spending heavily in three swing districts along the border of Mexico. But there are concerns about disinformation on social media targeting Hispanic people. Vanessa Cardenas, executive director of America's Voice, said she believes too much disinformation is not only affecting Hispanic political influence but also democracy

(Diamante 2022). “It makes people reluctant to participate because they don't feel like their vote is going to matter or because they don't trust our election system because of all the narrative they’re seeing around, you know, election fraud. It is also because, as we know, in the last couple of years, there have been a lot of narratives that are racist and full of hate. Therefore, people who, for whatever reason, might feel vulnerable,” Cardenas said. After the 2020 presidential campaign, the University of Houston researchers looked at how Latinos were inundated with misinformation. They found that older Latino voters and voters who heavily used social media were more likely to believe in conspiracy theories. Texas Republicans have been critical of social media companies, arguing they have unfairly targeted conservative voices on the platforms. While disinformation on social media is a problem both in Spanish and English, the relative lack of mainstream Spanish-language news outlets makes it more of a problem for Hispanic people who rely on social media for news – a problem these advocacy groups hope that social media platforms will address (Diamante 2022).

CONCLUSION

In this analytical essay, we focus on the dangers of electoral disinformation in the U.S. that have been going on for years. Specifically, we focused on cases from 2016 through the 2022 midterm elections. As we pointed out in the essay, such disinformation poses a real risk to citizens but also to democracy. We identified Donald Trump and his supporters as the main disinformation actor, as evidenced by the attack on the Capitol and the continued spread of fake news in 2022. Despite efforts to improve the situation regarding electoral disinformation by the US states, the problem is still relevant. The solution should be to raise citizens’ awareness of disinformation and then educate them on how to combat such fake news. We see a possible shift in increased cooperation between the US government and organizations that combat disinformation. Since disinformation has targeted in recent years primarily Hispanic audiences or non-native citizens, participation and translation of elected information for these audiences are also necessary. Raising awareness about the real process of elections and the system by which elections work and refuting

false claims of possible fraud is one path that could improve the problem. The biggest problem, however, remains the ignorance on the part of constitutional officials and their very participation in the creation and dissemination of disinformation narratives. That is why it is necessary for the political fight to be honest and fair and for candidates not to resort to desperate means such as spreading false accusations about their opponent, as we have seen in the 2020 presidential elections.

We have identified a number of issues that can be addressed in the future. In particular, there is a need to change the attitude of the public and political actors towards electoral disinformation, to increase the awareness of citizens before and during elections, and also to improve the environment in polling stations for election coordinators. Disinformation cannot be completely avoided and therefore it is also important to communicate it well to the public. At the same time, it is essential to personalise the content to the target groups, both in format and language, especially for non-native speakers and other ethnic groups. In today's modern online age, greater regulation of social network content and greater accountability of technology giants is also necessary. By following at least the recommendations mentioned above, the next US elections could be smoother and better conducted.

REFERENCES

Burgess, Brent. 2022. “Threats, Stalking Lead to Election Office Resignation.” Fredericksburg Standard. Accessed 27.01.2023. https://www.fredericksburgstandard.com/news/threats-stalking-lead-election-office-resignation.

Diamante, Reena. 2022. “Group Warns of Misinformation Targeting Latinos Ahead of Midterm Elections,” Coalition warns of misinformation targeting Latinos. Accessed 28.01.2023. https://spectrumlocalnews.com/tx/south-texas-el-paso/politics/2022/10/28/coalition-warns-of-misinformation-targeting-latinos-ahead-of-midterm-elections-.

Gregorian, Dareh. 2023. “Facebook and Instagram End Trump's Suspension from Platforms.” NBCNews.com. 2023. Accessed 12.01.2023. https://www.nbcnews.com/politics/donald-trump/facebook-instagram-end-trumps-suspension-platforms-rcna67524.

Chokshi, Niraj. 2018. “Trump Voters Driven by Fear of Losing Status, Not Economic Anxiety, Study Finds.” The New York Times. Accessed 12.01.2023. https://www.nytimes.com/2018/04/24/us/politics/trump-economic-anxiety.html.

Institute for public relations. 2022. “2022 IPR DISINFORMATION IN SOCIETY REPORT”, February 22, Accessed 02.01.2023. https://instituteforpr.org/2022-disinformation-report/.

IntelBrief. 2022. “Intelbrief: Serious Concerns over Political Violence Surrounding U.S. Midterm Elections.” The Soufan Center. Accessed 12.01.2023. https://thesoufancenter.org/intelbrief-2022-october-12/.

Lipton, Eric. 2016. “Man Motivated by 'Pizzagate' Conspiracy Theory Arrested in Washington Gunfire.” The New York Times. The New York Times, December 5. Accessed 22.01.2023. https://www.nytimes.com/2016/12/05/us/pizzagate-comet-ping-pong-edgar-maddison-welch.html.

Marineau, S. 2022. “Fact check us: What is the impact of Russian interference in the US presidential election?” The Conversation. Accessed 03.01.2023. https://theconversation.com/fact-check-us-what-is-the-impact-of-russian-interference-in-the-us-presidential-election-146711.

Miller, Michael E. 2021. “The Pizzagate Gunman Is out of Prison. Conspiracy Theories Are out of Control.” The Washington Post. WP Company. Accessed 03.01.2023. https://www.washingtonpost.com/dc-md-va/2021/02/16/pizzagate-qanon-capitol-attack/.

Person. 2022. “U.S. Election Misinformation Limited, Not Stopped, on Social Media -Experts.” Reuters. Accessed 19.01.2023. https://www.reuters.com/technology/twitter-social-platforms-could-see-spike-election-misinformation-2022-11-09/.

Princeton. 2022. “Threats and Harassment Against Local Officials Dataset,” Accessed 23.01.2023. https://bridgingdivides.princeton.edu/sites/g/files/toruqf246/files/documents/Threats%20and%20Harassment%20Report.pdf.

Routley, N. 2020. “Mapping civil unrest in the United States” (2000–2020). Visual Capitalist. Accessed 03.01.2023. https://www.visualcapitalist.com/mapping-civil-unrest-in-the-united-states-2000-2020/ .

Spring, Marianna. 2020.“'Stop the Steal': The Deep Roots of Trump's 'Voter Fraud' Strategy.” BBC News. Accessed 16.01.2023. https://www.bbc.com/news/blogs-trending-55009950.

Texas Scorecard. 2022. “Beto O'Rourke & Planned Parenthood Texas Try to Register Dead Voters.” Accessed 26.01.2023. https://texasscorecard.com/videos/beto-orourke-planned-parenthood-texas-try-to-register-dead-voters/.

The New York Times. 2022. “Final Report from the Jan. 6 Committee.” Accessed 20.01.2023.

https://www.nytimes.com/interactive/2022/12/23/us/january-6-committee-final-report.html.

Ura, Alexa. 2021. “The Hard-Fought Texas Voting Bill Is Poised to Become Law. Here's What It Does.” The Texas Tribune. Accessed 26.01.2023. https://www.texastribune.org/2021/08/30/texas-voting-restrictions-bill/.

Wendling, Mike. 2022. “US Midterms: Misleading Election Claims Fact-Checked.” BBC News. Accessed 16.01.2023. https://www.bbc.com/news/63564964.

THE RUSSIAN FEDERATION AND THE USE OF HYBRID THREATS: A CASE STUDY OF POLAND AND HUNGARY

Gerová Kristína, expert consultant: Kupková Iveta

INTRODUCTION

The 21st century can be characterized as a period in international relations when the Euro-Atlantic area has to face newly emerging challenges, and the way it responds will determine the future configuration of the international system. One of these challenges is hybrid threats, which have become increasingly prominent in the political, academic, and information space. Due to their fluid and dynamic nature, they are difficult to identify and can have devastating consequences for the national security of affected states. In addition, hybrid threats usually differ from state to state and target specific vulnerabilities.

To verify this attribute, I have chosen Poland and Hungary for comparison in two specific domains according to Joint Research Centre's framework – cyber and information. The goal is to show what tools and methods the Russian Federation uses in both countries and whether they vary from state to state. I have chosen Hungary and Poland as the focal unit of my research because of their geopolitical proximity and similar yet slightly different historical, cultural, and political experiences. However, both were targeted by the Russian Federation.

The Russian Federation is one of the actors that has a prominent presence in the Central and Eastern European region and is actively operating to regain its former position. This can also be seen in the statement of the Russian Ministry of Foreign Affairs from 2022 that calls for the provision of security guarantees before 1997 when Poland, Hungary and many other states were not a part of NATO. This has been intensified by Russia's invasion of Ukraine, which has led to strained relations between Russia and Poland. On the contrary, Hungary is building favourable bilateral relations with Russia, which is also transformed in the deepening of the socioeconomic impact that the state has on Russia.

The Landscape of Hybrid Threats: A Conceptual Model by Joint Research Centre served as a framework to define the domains and tools that will be the object of my research. I have chosen the cyber and information domain as their results are usually the most visible. In particular, my analysis will try to identify trends in the context of the conflict in Ukraine and reflect on what tendencies and aspects are observable in this regard.

JRC describes the cyber domain as playing an exceptional and highly specific role concerning hybrid threats. Information technologies are characterized by a high degree of connection to telecommunications networks, the internet, or computer systems, which means that their paralysis can have fatal consequences for the national security of the given state. The tools can aim at causing degradation, disruption, or destruction of the networks or aim to access data and information. At the same time, the low price of entry and anonymity provided by cyberspace causes the actor who is the target of the attack to be in a disadvantaged position, which also reduces his ability to defend himself effectively against such attacks and respond adequately.

JRC describes the information domain as one of the most popular elements of hybrid threats, whose primary purpose is to undermine citizens' trust in security by provoking a wide range of conflicts in political or cultural spheres. The purpose is to disrupt cohesion in society and to atomize it to interest actors or groups. This type of domain is often used in particular because it represents a low financial cost to the actor. The popularization of social media has made disinformation as well as cyber propaganda more appealing and accessible to an increasingly wider audience and user base. The tools of this domain have as their primary objective to influence and manipulate public discourse in such a way as to weaken society and change the political mood of a given state.

Main findings:

- The primary goal of Russian cyber operations focused on Hungary is to penetrate the cyber system and gain a better space to create attacks on other states in the EU and NATO.

- Hungary is failing in its ability to alert society as well as its partners about Russian attacks on their cyber infrastructure, which can be dangerous due to the currently increased military presence in the eastern part of the Alliance.
- Hungary suffers from systematic and structural problems that reduce its ability to effectively defend itself, especially in the case of outdated computer systems in state institutions, but also a lack of professionals and experts.
- Due to the unequivocal support of Ukraine, cyber attacks in Poland are concentrated on the strategic infrastructure of the state with the aim of paralyzing its logistical transfer of humanitarian and military material to Ukraine.
- Given the announced parliamentary elections, Poland must prepare for an increase in the intensity of cyber attacks, and in the future, the protection of the bodies responsible for the elections and also of the civil infrastructure must be strengthened.
- Disinformation operations in Poland are primarily focused on reducing the credibility and trust of citizens in the military and discrediting NATO and the United States.
- Recently, Russian disinformation in Poland has focused on spreading inaccurate information about Germany to provoke revisionist attitudes and portray Germany as an unreadable partner.
- Poland is the target of Russian disinformation aimed at the population in order to discourage them from providing support to Ukraine.
- In Hungary, disinformation campaigns about the threat to the Hungarian minority in the Transcarpathian region are focused on attacking bilateral relations with Ukraine.
- An emerging trend in Hungary is the rising tendency of pro-Russian disinformation narratives in public and state-supported media

CYBER DOMAIN

HUNGARY

In the case of Hungary, we can observe that Russia is using a wide range of activities, from sending fake messages to ministry employees to direct hacking operations and attacking the cyber system of government bodies. In order to get a better idea and understanding of the different elements that

the Russian Federation is carrying out in Hungary, it is possible to point to incidents that have been carried out in the past.

In Hungary, an attack on the computer network of the MFA was recorded already in 2012. According to the information of investigative journalists, Russian hackers were able to install a program providing remote access to Team Viewer, through which intruders could see any movement on computers and find out access passwords or other information (Kréko 2022). Despite the seriousness and the resulting security risks based on the findings, the Hungarian government of the time decided not to inform its foreign policy partners and allies about the incident (Panayi 2022).

The characteristic element of Russian cyber-attacks, in the case of Hungary, is that their purpose is to penetrate the information systems of its allies, both in NATO and the EU. Thus, the uniqueness of these cyberattacks lies in the fact that it uses the IP addresses of Hungarian state bodies to create hostile attacks against more attractive and interesting states for Russia (Zsolt 2017). The trend that will be observed more often in the coming period is that the Russian hackers will try to build stable positions within Hungary's critical cyber infrastructure through which they can later carry out attacks on NATO and EU allies.

In this context, it is particularly important to note that Hungary is the only country among the V4 that has failed to develop some form of political protest against the operations as a sign of the state's disapproval and diplomatic stance towards the attacks from Russia (Council of EU 2022). The regressive signal in the field of cyber protection against Russia can be seen especially after 2015 when Hungary's information security system was changed by an amendment to the law, and a large part of the competence that was concentrated in the hands of the secret service in this matter became non-transparent (Zsolt 2018).

Hungary's opposition to Russian operations also reveals a structural or systemic problem facing the state, namely that the computer systems are either outdated or poorly installed, such as in the case of the MFA (Szabolcs 2022). This helps to increase the success rate of Russian operations,

although the ministry's management and staff have been made aware of such cracks in the system.

The actions of Hungarian diplomacy are also alarming, which, unlike other V4 members, only sporadically alerts the public to such attacks, and even when such operations are made public, communicates them in such a way as to downplay Russia's culpability. This trend is likely to escalate, and Euro-Atlantic partners should therefore be aware of this Hungarian weakness and take steps to strengthen cyberspace against potential attacks emanating from Hungary's state domains as well.

SUMMARY

The nature of Russia's cyber-attacks is specific to Hungary, in particular, because it uses the state as a tool through which it seeks to gain access and positions on the basis of which it could create hostile attacks against other EU or NATO members. This aspect is even more important during the ongoing conflict in Ukraine when highly sensitive information regarding arms deliveries or details of exercises conducted by allies can be compromised through cyberattacks, which can threaten the integral security of NATO as a whole. If there is no change, Hungary will most likely become an isolated player vis-à-vis the allies.

POLAND

In the case of Poland is one of the main targets of cyberattacks by Russian hackers. This fact is largely reinforced by the war in Ukraine as well as the fact that Poland is described as Ukraine's primary ally and is characterized as a driver of assistance to Ukraine within the EU states, particularly in terms of armaments.

In May 2022, the Russian hacker group Killnet declared a “war” on Poland in cyberspace as a consequence of the war in Ukraine (Smith & Lonergan 2022). Russia has intensified operations that are also destructive for economic companies, firms and small and medium-sized enterprises (Kozlowski 2023). Therefore, one of the noticeable trends in the coming period is that Russia will focus its operations on the private sector as well as on institutions of public services. This emerging trend can be seen even now when, according to Check Point data, Polish civil infrastructure and public services are

attacked twice as much compared to other sectors. The intensity of attacks on civil infrastructure by Russia is predictable due to the fact that Poland has a low level of protection in this spectrum, as evidenced by the fact that about 25 to 30% of cyberattacks targeting this sector are successful (Peterson 2022).

Russia is attacking sensitive strategic areas such as the energy sector and the arms industry in Poland more than in other countries. In July 2022, the group managed to take down a government website, and in October, the computer company Microsoft revealed that Russian hackers had attacked the transport and logistics sectors of Poland and Ukraine (Microsoft Security 2022). Similarly, the Polish military has warned that the intensity and number of cyberattacks on the armed forces' computer systems from January to April 2022 surpassed the number of all attacks in 2021. In this case, Poland is one of the only countries within the EU where Russia's cyber activity also affects the logistics sector. This is because Russia is trying to prevent the transfer of military equipment to the territory of Ukraine in this way, as Poland is one of the logistics hubs where it concentrates but also distributes its equipment to the EU.

At the same time, we can observe that some of Russia's actions are a response to an initiative made by Poland. For example, the so-called retaliatory action occurred in November 2022, when the Polish Parliament approved a declaration designating Russia as a 'state sponsor of terrorism'. The Russian hacking group NoName057(16) was behind the attack (Peterson 2022).

Another popular tool used extensively by Russian cyber actors, particularly in Poland, is stolen websites. Russian hackers also carried out operations in this way at the beginning of December 2022 when they created and registered a website called gov.pl (Antonyuk 2022). This website was intended to give the impression of a state-owned website, but its true purpose was to collect personal information from Polish citizens. The activity was supposed to be a retaliation for providing the civilian population in Ukraine with humanitarian aid, such as power generators.

Given the intensification of support for Ukraine in the field of heavy military equipment, such aggressive tactics will only intensify. This way, Russia will try to weaken Poland's motivation to arm Ukraine. These attacks will be aimed at disabling software in the transport sector, such as airports or railways. Russia had already carried out a similar type of attack in 2022 when it managed to disable 80% of the train network in Poland (Reuters 2022).

SUMMARY

Poland is one of the most frequent victims of Russian cyber operations. Compared to the rest of the V4, these operations focus more on security infrastructure and sensitive strategic areas such as the energy sector or the arms industry. This is largely reinforced by the fact that Poland is one of the EU states providing some of the largest humanitarian, diplomatic and military assistance to Ukraine. This aspect is also reflected in the fact that Russian cyber-attacks are much more focused on crippling the systems of the armed forces. This trend will also be visible to a large extent in the future, precisely because Poland is a 'logistic hub' within the region, i.e., a cut-through point through which military material is transported to Ukraine.

INFORMATION DOMAIN

HUNGARY

One characteristic particular to Hungary is that Russian propaganda can be found in the mainstream media. Although this element was also present in the previous period, its intensity increased dramatically after Russia invaded Ukraine. The trend that can be followed is that Russian disinformation is becoming part of the Hungarian mainstream discourse over time, and its appearance is particularly visible in the state-owned media (Bognar 2023).

In the case of Hungary, narratives justifying Russia's aggression and trying to justify its actions are frequent. The most common reason cited is the provocation by NATO, whose expansion into Eastern Europe meant that Russia had to respond with an attack to protect its sovereignty (Kafkadesk 2022). The argument that Ukraine has no right to exist as a sovereign state or that it has constantly been part of Russia's sphere of influence is also frequently mentioned.

Another specific aspect visible in the Hungarian environment is that Russian disinformation operations have a background in a wide network of actors and communities present on social media that either directly adopt or spread pro-Russian disinformation narratives (Kafkadesk 2022). With a wide network of actors, the Hungarian media environment provides a comfortable background for the implementation of disinformation activities from state-sponsored TV stations, experts or political analysts with a "neutral view" appearing in debates or regional and national daily newspapers as well as state-run news organisations (Mastracci 2022).

It is important to note that the Hungarian media market is highly concentrated and economically dependent on state support. This trend will likely continue, given the current government policy. Therefore, disinformation with a pro-Russian narrative is expected to be present in the Hungarian media ecosystem, also in the future.

Russian disinformation operations, in addition to the classical anti-American agenda, also focus on the internally problematic aspects of Hungary. In this case, it should be noted that Hungary shares a very sensitive history with Ukraine regarding the so-called Transcarpathian region, Kárpátalja (Ustemensko 2022). The conflict between Ukraine and Hungary lies in the fact that in 2017 Ukraine pushed through an amendment to the law prohibiting teaching in minority languages (Iegoshyna 2021). Hungary has protested against it because it also directly affects the Hungarian minority, which may lose contact with its national culture in this way. One of the very popular streams of disinformation also legitimizes Russia's attack on Ukraine by painting Ukraine as an oppressor of other minorities. Some Russian disinformation operatives are even encouraging the annexation of Transcarpathia by Hungary.

A systematic problem with Hungarian news coverage in state-backed media such as Origo, Magyar Nemzet, and HírTV is that Russian disinformation stories are picked up without much fact-checking. Hungarian news outlets also share graphic content and videos from Russian sites with professional-quality disinformation using dramatic effects, giving the viewer a credible impression (Bayer 2022).

These videos usually exaggerate the data in favour of Russia. Examples include the number of captured Ukrainian soldiers or the amount of Ukrainian territory occupied by Russia. This trend will further increase in intensity during this year precisely because of the ongoing war in Ukraine. The same applies to the intensity of the dissemination of Russian disinformation, given that it has a suitable environment for spreading in Hungary.

SUMMARY

Russian disinformation manifests itself in state-owned media in varying degrees and levels. It can be a classic sharing of information from Russian propaganda sites included in news coverage or a more sophisticated form where the framing and explanation of an event are designed along Russian propaganda and disinformation lines. A common narrative in the Hungarian disinformation scene is that the US is responsible for the conflict in Ukraine, aiming to weaken Europe as an international competitor.

However, the intensity of the pro-Russian disinformation has increased significantly since the Russian invasion of Ukraine. Since the early days of the conflict, most TV stations have primarily adopted the Russian perspective on the conflict. Russian disinformation operations, in addition to the classical anti-American narratives, also focus on the problematic local aspects of Hungary.

POLAND

Russia's disinformation activities have stable themes that recur periodically regardless of the current geopolitical situation. Such activities primarily target the Polish population in order to undermine its trust in the state and democratic institutions. By manipulating historical facts, Russian disinformation evokes a narrative that accuses Polish citizens of not appreciating the merits of the Red Army, which liberated the country from German occupation. It also tries to push the narrative that Poland was responsible for starting the Second World War or accuses Polish citizens of being unreasonably hostile to Russia (Polish Government 2020).

Another reoccurring theme is the questioning of the credibility of Poland as an alliance partner, whether by ridiculing the strength, capabilities and

equipment of the Polish army, spreading false information about Poland's alliance commitments to NATO, or stirring up negative sympathies towards the US. What is specific in the case of Poland is that the Russian disinformation campaigns also target the state's military forces. For example, it focused on the military exercises DEFENDER-Europe 20 organized by Poland. Russian disinformation pointed out that a large concentration of troops during the exercises could spread the infection of COVID-19 to the local population. Polish elites were accused of being irresponsible with the lives of Polish soldiers (Polish Government 2020).

In the context of the current war in Ukraine, the information activity primarily focuses on the two key aspects, which are later varied and combined in different ways. On the one hand, Russian propaganda tries to portray Ukrainians negatively in the eyes of the Polish audience and to belittle them. On the other hand, active military and economic assistance to Ukrainians is mentioned in connection with the worsening of the conflict. This may lead to a further escalation and Poland being dragged into the conflict. Russian disinformation campaigns, for example, report on alleged Polish mercenaries who are actively fighting alongside Ukraine in an attempt to instil fear in Polish citizens and discourage them from providing support to Ukraine (TVP World 2023).

To undermine support for Ukraine, part of Russia's disinformation activities include targeting the emotional historical moments of both states, thus stirring up revisionist sentiments in the society. Poland is portrayed as spending disproportionately on supporting Ukraine due to being one of the states within the EU that bears the greatest economic, political, but also humanitarian burden. However, Russian disinformation activities are mostly assessed as unsuccessful and resonate only with a part of society's far-right and far-left spectrum, i.e., radical circles showing nationalist and anti-democratic tendencies (Olchowski 2022).

A typical feature of the Russian disinformation campaign is the fact that it is not solely concentrated on Polish society. The Russian Federation is also trying to damage Poland's reputation as a reliable Euro-Atlantic partner through propaganda attacks to discredit the country internationally (Salvo 2022).

SUMMARY

Due to the resilience of Polish society, Russian disinformation operations are unsuccessful, reaching only a narrow spectrum of the far-right and far-left part of the population. The Russian Federation is trying to damage Poland's reputation as a reliable Euro-Atlantic partner through propaganda attacks. This is because Poland has played an important role in humanitarian, economic and political support for Ukraine.

Disinformation operations are focused on questioning support for Ukraine. Poland's foreign policy actions are interpreted as hasty, and Warsaw is portrayed as an actor that puts itself at disproportionate risk and exposes itself to war by providing aid to Ukraine. In addition, the stable topics are periodically repeated, such as questioning Poland and its credibility as an alliance partner.

CONCLUSION

Poland and Hungary are examples of states that are the targets of hybrid threats coming from the Russian Federation. However, as can be demonstrated from the findings of this analytical essay, Russia uses different forms and means to target these states, but with a common goal, namely the reversal of the democratic system and their anchoring in Euro-Atlantic international structures.

Regarding cyber threats, Hungary is a weak link in terms of its cyber security capability. It has not built sufficient tools to respond to such attacks as well as the capability to identify the responsible actor with sufficient speed. The primary purpose of Russian cyber activities is not to damage Hungary but to obtain sensitive security information about other NATO and EU allies. This trend can be dangerous since the member states are trying to provide humanitarian, economic, and above all, military aid to Ukraine. Russia accessing documents discussing these operations poses a significant security risk for Hungary and other actors.

Unlike Hungary, Poland has a diametrically different starting position, resulting from the fact that it is one of the most fundamental allies of Ukraine, not only in terms of humanitarian and economic aid but primarily

because of essential military support. At the same time, Poland's geographical location makes it a logistical hub that provides its infrastructure for the transfer of necessary military equipment to Ukraine.
Thus, through cyber-attacks, Russia is trying to paralyze infrastructure such as railways to sabotage Poland's activities in support of Ukraine. In addition, it also attacks civil infrastructure, such as hospitals and the private sector. The aim is to reduce the support of Polish citizens and discourage them from providing support to Ukraine.

It is therefore necessary that, in the future, Poland deepens its cooperation with its allies through which it will ensure a higher level of protection to ensure the infrastructure that is key to the security of the state. Russian disinformation in Poland focuses on provoking revisionist sentiments in society against Ukraine to portray support for Ukraine as disadvantageous for Polish interests in the eyes of the public.

In addition to spreading disinformation questioning the quality of the Polish military as well as spreading a narrative aimed at reducing NATO's credibility, Russia is spreading disinformation that also attacks bilateral relations between Germany and Poland.

In Hungary, Russian disinformation aims to raise concern and anxiety about NATO, justifying Russia's aggression through disinformation websites and with the help of Hungarian state-supported print media and television stations. In connection with Ukraine, Russian disinformation tries to promote narratives about the Hungarian minority in Ukraine being threatened by Kyiv.

REFERENCES

Antoniuk, Darina. 2022. "Poland warns of pro-Kremlin cyberattacks aimed at destabilisation". The Record.media, December 31. Accessed 13.02.2023. https://therecord.media/poland-warns-of-pro-kremlin-cyberattacks-aimed-at-destabilization/.

Bayer, Lili. 2022. "Hungary has become the EU home of Kremlin talking points." Politico, March 9. Accessed 11.02.2023. https://www.politico.eu/article/russia-war-narrative-hungary-disinformation/.

Council of EU. 2022. "EU imposes the first ever sanctions against cyber-attacks." Consilium Europe, July 30. Accessed 10.02.2023. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

Iegoshyna, Valeriya. 2021. "HOW THE HUNGARIAN GOVERNMENT INVESTS BILLIONS IN ZAKARPATTIA." Vsquare.org, July 9. Accessed 13.02.2023. https://vsquare.org/how-the-hungarian-government-invests-billions-in-zakarpattia/.

Kafkadesk. 2022. "War and disinformation: pro-Russian narratives thrive in Hungary as Ukraine fights off aggression (1/2)." September 25. Accessed 11.02.2023. https://kafkadesk.org/2022/09/25/war-and-disinformation-pro-russian-narratives-thrive-in-hungary-as-ukraine-fights-off-aggression-1-2/.

Kozlowski, Andrzej. 2023. "Polish Cyber Defenses and the Russia-Ukraine War." Council on Regional Relations, January 18. Accessed 28.01.2023. https://www.cfr.org/blog/polish-cyber-defenses-and-russia-ukraine-war.

Mastracci, Matteo. 2022. "Pro-Kremlin Online Rhetoric Thrives in Orban's Hungary." Balkan Insight, April 20. Accessed 11.02.2023. https://balkaninsight.com/2022/04/20/pro-kremlin-online-rhetoric-thrives-in-orbans-hungary/.

Olchowski, Jakub. 2022. "Russian propaganda attacks Polish-Ukrainian relations." Instytut Europy Środkowej, June 30. Accessed 04.02.2023.

https://ies.lublin.pl/en/comments/russian-propaganda-attacks-polish-ukrainian-relations/.

Peterson, Andrea. 2022. "New 'Prestige' ransomware campaign targets Ukraine and Poland." The Record.media, October 14. Accessed 11.02.2023. https://therecord.media/new-prestige-ransomware-campaign-targets-ukraine-and-poland/.

Polish Government. 2020. Disinformation against Poland in 2020 – special services' view. Accessed 15.02.2023. https://www.gov.pl/web/sluzby-specjalne/disinformation-against-poland-in-2020--special-services-view.

Salvo, David. 2022. "Oh, the Irony…Russia Spreads Disinformation about Polish Annexation of Western Ukrainian Regions." Alliance for Securing Democracy, December 5. Accessed 04.02.2023. https://securingdemocracy.gmfus.org/oh-the-ironyrussia-spreads-disinformation-about-polish-annexation-of-western-ukrainian-regions/.

Smith, Maggie, Erica D. Lonergan, and Nick Stark. 2022. "What Impact, if Any, Does Killnet Have?" Lawfare, October 21. Accessed 08.02.2023. https://www.lawfareblog.com/what-impact-if-any-does-killnet-have.

Szabolcs, Panyi. 2022. "Western allies puzzled by Hungary' mild reaction to Russia's hacking." Telex.hu, July 18. Accessed 11.02.2023. https://telex.hu/english/2022/07/18/western-allies-puzzled-by-hungary-mild-reaction-to-russias-hacking.

Szabolcs, Panyi. 2022. "Putin's hackers gained full access to Hungary's foreign ministry networks, the Orbán government has been unable to stop them." Direkt36, March 29. Accessed 16.02.2023. https://www.direkt36.hu/en/putyin-hekkerei-is-latjak-a-magyar-kulugy-titkait-az-orban-kormany-evek-ota-nem-birja-elharitani-oket/.

TVP World. 2023. "Russian propaganda tries to smear Poland: security official." 18 January. Accessed 12.02. 2023.

https://tvpworld.com/65733586/russian-propaganda-tries-to-smear-poland-security-official.

Ustymenko, Bohdan. 2022. “Ukraine’s Transcarpathia: The Other Center of Tension in the Heart of Europe.” The Jamestown Foundation, May 24. Accessed 04.02.2023. https://jamestown.org/program/ukraines-transcarpathia-the-other-center-of-tension-in-the-heart-of-europe/.

Zsolt, Sarkadi. 2017. “Az orosz hekkerek 2014-ben úgy törték fel a Honvédelmi Minisztérium levelezését, hogy létrehoztak egy hm.qov.hu kamuoldalt, amit sokan összekevertek a hm.gov.hu-val.” 444.hu, July 21. Accessed 29.01.2023.
https://444.hu/2017/07/21/az-orosz-hekkerek-2014-ben-ugy-tortek-fel-a-honvedelmi-miniszterium-levelezeset-hogy-letrehoztak-egy-hmqovhu-kamuoldalt-amit-sokan-osszekevertek-a-hmgovhu-val.

DAVID VS. GOLIATH: CYBERSECURITY OF SMALL MUNICIPALITIES IN SLOVAKIA

Kobzová Lucia, expert consultant: Šalmík Matej

EXECUTIVE SUMMARY AND RECOMMENDATIONS

- In the past few years, small municipalities have become an attractive target for cybercriminals.
- They process sensitive data about citizens while their cybersecurity measures are insufficient due to limited resources.
- Small municipalities in Slovakia with more than a thousand inhabitants are providers of essential services according to the Act on Cybersecurity.
- However, they face many obstacles starting with poor guidance and support from the state and ending with contradictory legal requirements stemming from major cybersecurity laws.
- The major obstructions precluding small municipalities from becoming cyber secure are no cybersecurity awareness, lack of guidance from the state authorities, absence of experts, and insufficient financial capital.
- State authorities should increase funding for cybersecurity in small municipalities, write comprehensive cybersecurity guidelines and standards solely for municipalities, offer experts that could help with the implementation of necessary measures, and provide training and educational courses for employees and leadership.
- While the prevailing number of recommended policies ought to be implemented by the state authorities, small municipalities are advised to conduct a risk assessment.

INTRODUCTION

Digitalization of public administration brought many positive phenomena. It, inter alia, facilitated communication with the state authorities, brought greater transparency and alleviated the bureaucratic burden imposed by the state. The same is valid for smaller municipalities that benefit to a great extent from digital transformation. They can offer digital services to citizens

who are not obliged to physically visit state institutions whenever they need to interact with the public authorities. Small municipalities provide various services ranging from tax payments, e-documents, registrar's office, and many others. Thanks to it, local governance is more accessible and efficient. At the same time, integrating digital solutions increases the risk of cyber incidents that could disrupt essential municipal services. Cybercriminals can easily exploit municipal systems if there are no proper security protocols in place. For that reason, it is necessary to have cybersecurity measures in place and develop a comprehensive plan for resolving cyber incidents once they happen. However, small municipalities' cybersecurity journey resembles David's fight against Goliath. The capacities and capabilities of small municipalities are very limited, while the resources of cybercriminals are incomparably higher.

THEORETICAL BACKGROUND

Small municipalities could become attractive targets for hackers since they process sensitive data about citizens and offer their services digitally. Moreover, cyber-attacks could cost local governments thousands of euros and, at the same time, deprive citizens of services for months (Duncan 2019). Therefore, it is desirable to adopt proactive measures, not only react after the incident happens. This tends to be problematic due to various factors, such as the lack of financial and human capital or a deficit of IT and cybersecurity experts (Preis and Susskind 2020). These problems are even amplified in small municipalities since their resources are much more limited while having a broad range of responsibilities in diverse areas.

Small municipalities in Slovakia offering a service that affects more than a thousand people are the providers of essential services according to the Act on Cybersecurity and following Decree no. 164/2018, and hence are required to implement cybersecurity measures (Act no. 69/2018; Decree no. 362/2018; Decree 164/2018). Those legal obligations include reporting severe cyber incidents, collecting digital evidence from the incident, defining procedures and measures for resolving cyber incidents, and identifying cybersecurity managers and others. In addition, according to Decree 179/2020, which complements the Act on Information Technologies of Public Administration, small municipalities fall into Category I of minimum-security measures (Act no. 95/2019, Decree no. 179/2020). Minimum security measures are divided into three categories depending on the size of a

specific entity. The first category is the one that requires the least demanding actions. These include choosing an employee responsible for cybersecurity, developing, and implementing internal management guidelines, and others (Decree no. 179/2020). The fact that the state authorities adopted two different laws and two complementary decrees caused chaos in their implementation. Providers of essential services are required to implement obligations from both while the laws are in certain instances contradictory. This chaotic situation precludes small municipalities from fulfilling their legal duties and hence ensuring effective cybersecurity policies.

Research studies regarding cybersecurity in small municipalities are absent in Slovakia. The state neither possesses any information about the actual state of cybersecurity measures adopted by small municipalities nor the fundamental obstacles those municipalities face. No cybersecurity audit maps whether small municipalities can fulfil the requirements stemming from the Act on Cybersecurity and the Act on Information Technologies of Public Administration (Act no. 69/2018; Act no. 95/2019). For adequate formulation and following implementation of cyber policies designed for small municipalities, it is sine qua non to know the actual situation first. Only after having data about the significant obstacles and the extent of municipal e-services is it possible to adequately set policies. Therefore, this paper aims to fill the gap in research regarding cybersecurity in small municipalities and highlight the most critical challenges.

While there are many definitions of cybersecurity, in this paper, cybersecurity will be defined as the practices and measures that ensure CIA - confidentiality, integrity, and availability (ENISA 2015). Confidentiality refers to the concept according to which data ought to be accessible solely to authorized parties. Integrity means that modification of data can be done only by authorized users. Availability means that authorized users can access data whenever desired. Cybersecurity could be defined as a coherent set of measures that protect networks, systems, devices, and data from external threats. For the purposes of this paper, small municipalities will be defined as any local entity recognized by the state authorities and law with 500-2000 inhabitants.

This paper aims to conduct a qualitative study that would suggest the prevailing cybersecurity trends in small municipalities across Slovakia. To find out the challenges that municipalities face, a small-scale survey was conducted. The formulation of questions asked through the online form can be found in the appendix. The form was followingly sent to various small municipalities with 500-2000 inhabitants from every region across Slovakia (Kobzová 2023). Even though the results cannot be generalized, the answers from 24 municipalities indicated several trends that preclude more cyber-secure local governance (Kobzová 2023). The most significant obstructions that prevent small municipalities from adopting more cyber-secure policies are insufficient financial capital, lack of cybersecurity awareness, absence of cybersecurity guidelines and guidance from the state authorities, and deficiency of experts.

LESS IS MORE? THE STORY OF CYBERSECURITY FUNDING

The lack of financial capital is the major obstruction that prevents sufficient implementation of cybersecurity measures. Small municipalities have minimal resources and must first ensure that fundamental services are provided to citizens, and only after can they invest in secure digital solutions. However, this poses a threat to the cybersecurity of small municipalities and the whole state´s digital infrastructure as such since the systems are interconnected. The survey conducted in Florida revealed that municipal governments regard insufficient funding as a primary barrier preventing the adoption of more cyber-secure policies (Ocampo 2021). Cybersecurity measures often require considerable financial investments. One of the best practices recommended by cyber experts is to conduct a risk assessment of the systems and networks (Thompson 2019). The state does not provide these services; therefore, the only possibility is to pay the private company to evaluate the risks and vulnerabilities. In an ideal case scenario, municipalities should be capable of conducting such assessments on their own but in reality, they lack expertise. Furthermore, every municipality should have an incident response plan and regular internal audits (Thompson, 2019). Since most of the local governments cannot conduct them internally and the state does not offer any guidance, they have to cooperate with the private sector, which is again financially demanding. Another desirable course of action is to implement technical security solutions within the municipality. All of the above-mentioned practices are

often not affordable for the municipalities. It must be noted that several measures have zero or minimal impact on the budget and effectively reduce cyber risks.

Six practices could improve cybersecurity in small municipalities without requiring any or minimal financial investment:

- Password management policy
- Identification of assets
- Risk assessment
- Regular system updates
- Identification of roles and responsibilities
- Basic security awareness

SHORTAGE OF CYBERSECURITY AND IT EXPERTS

For effective cybersecurity measures, it is necessary to hire experts who not only understand the potential threats but more importantly, are capable of implementing even more demanding technical solutions. Small municipalities often hire one IT specialist who oversees anything related to technologies within the municipality. This is not a desirable solution since this person might not be aware of cybersecurity standards and might avoid security routines to fulfil the interests of IT operations. It would be preferable to have a dedicated person for cybersecurity. Even if the municipality wanted to hire an expert, it would probably encounter the problem of finding one. The demand for cybersecurity experts is growing faster than the supply. Those available experts on the market primarily choose to work for private companies since they are more lucrative from a financial perspective. For that reason, municipalities are forced to rely on the help of the state in this regard. Nevertheless, the state does not provide experts to small municipalities who would help them to analyze the cyber environment, do audits, or to establish functional cyber-secure infrastructure for e-services. It must be noted that the responsible authority- the Ministry of investments, regional development, and informatization (MIRRI) has no capacity to help those small municipalities on an individual basis. Slovakia has almost three thousand municipalities, and therefore the individual approach remains truly challenging. It is also possible to pay a private company that could do the analysis and audit of the cyber environment as well as educate employees and help to ensure that

obligations stemming from the Act on Cybersecurity. This solution would again require additional investments. However, municipalities must be cautious because many actors attempt to abuse the situation of small municipalities. They offer "effective" and "complex" cybersecurity measures that are surprisingly affordable but in reality, it does not bring desirable results. The only way out is for the state to either provide internal experts who would be available for consultations with small municipalities or allocate finances specifically dedicated to paying private companies to help municipalities with cybersecurity measures. Even municipalities themselves mentioned in the survey that they lack human capital in terms of IT and cybersecurity experts (Kobzová 2023). This is connected to the financial obstacles since hiring IT or cybersecurity specialists would require considerable investments that often cannot compete with the incomes offered by the private sector. The factor of an understaffed workforce contributes to insufficient cybersecurity measures in small municipalities.

WHERE IS THE STATE? LACK OF COMPREHENSIVE CYBERSECURITY GUIDANCE

As a result of insufficient data about the issues that small municipalities encounter when dealing with cybersecurity, the Ministry of investments, regional development, and informatization (MIRRI) has not formulated any comprehensive guidelines or coherent set of recommendations for efficient cybersecurity management. Several municipalities claimed that they would appreciate greater support from the state both in terms of recommended cybersecurity standards for small municipalities and fundamental education courses for the leadership and IT experts (Kobzová 2023). The National Security Authority (NBÚ) developed a cybersecurity risk analysis methodology that could facilitate the implementation of legal obligations stemming from the Act on Cybersecurity (Act No. 69/2018; National Security Authority 2021) Moreover, MIRRI created several methodologies that are supposed to help municipalities navigate through the legal requirements (Ministry of investments, regional development, and informatization, n.d.). Documents including a template for risk assessment, manual for security policy, and checklist for entities falling into Category I of minimum-security measures can be found on the MIRRI website (Decree no. 179/2020; Ministry of investments, regional development, and informatization n.d.). None of these is comprehensive for a person that did not participate in any

cybersecurity course or training, or who has never dealt with cybersecurity measures before. Small municipalities are in a unique situation compared to other entities subject to requirements stemming from the Act on Cybersecurity and the Act on Information Technologies of Public Administration. They cannot afford to pay an expert who would deal solely with cybersecurity. Ensuring that the legal obligations are respected is then left to employees whose primary responsibility is completely different while their understanding of cybersecurity tends to be substantial. The state should provide an opportunity for small municipalities to attend seminars or workshops organized by professionals who would present municipalities with fundamental cybersecurity requirements and best practices. Followingly, the state ought to help small municipalities with risk assessment and implementation of cybersecurity measures. On top of that expert consultations should be available to any municipality that needs support.

VERY LITTLE DO THEY KNOW

The most common feature causing cyber incidents is the human factor. Lack of fundamental awareness amongst the users of technologies makes them easy targets. Cybercriminals use the deficient knowledge of users to exploit them. The most common practices, like password security or basic “cyber hygiene”, could considerably reduce the cyber incident risk. The favourite tool of hackers is to send phishing emails and wait for receivers to click on the links or attachments for the malicious software to be installed. In Slovakia, the cybersecurity education supported by the state is insufficient (Kobzová 2023). Cybersecurity education is not included in the primary, secondary, and high school curricula. Education opportunities for the elderly and people with special needs are lacking (Kobzová 2023). The same is valid for the mayors and employees of municipalities. Even though they are the providers of essential services and hence part of the state's information infrastructure, they have no possibility to attend free state cybersecurity courses or training that would explain essential cybersecurity challenges. The survey results suggest that the comprehension of cybersecurity among small municipalities is substantial (Kobzová 2023). Various small municipalities cannot even name the e-services they offer to citizens (Kobzová 2023). Several of them mentioned email communication as a service they offer citizens. The problem of cybersecurity awareness is

even more profound since the first phase should be to have fundamental digital skills. Only after having essential comprehension of IT issues can the person build on that knowledge and gain skills in cybersecurity.

TOWARDS SECURE SMALL MUNICIPALITIES

The current state of cybersecurity in small municipalities is based on the collected data, neither great nor terrible. Municipalities attempt to implement legal obligations emanating from the Act on Cybersecurity, but sometimes they are unable to do so (Act no. 69/2019; Kobzová 2023). However, cybersecurity measures cannot consist solely of legal obligations. The municipalities must take additional steps. Act on Cybersecurity stipulates only the fundamental standards that should serve as a cornerstone for more complex cybersecurity policies.

Several policies ought to be implemented by the small municipalities as well as by the state authorities in order to ameliorate the cybersecurity of those municipalities:

Risk assessment - it is necessary to first identify assets, threats, and vulnerabilities, and assess potential risks. Small municipalities do not have the resources to conduct the assessment on their own; it is, therefore, desirable to cooperate with MIRRI. The state ought to provide guidance and help the municipalities conduct evaluations on their own or financially support risk assessments undertaken by third parties.

Education and training - as the data suggests, municipalities would appreciate professional courses or training for their employees and experts. The most common cause of cyber incidents is the human factor. Therefore, it is desirable to provide small municipalities with opportunities to educate their employees without having to invest in private courses. The state should provide courses and training for small municipalities for IT specialists and any person working for the municipal authorities.

Guidelines and standards – municipalities perceive the deficiency in the comprehensive guidelines that would help them improve cybersecurity. Public administration (MIRRI) should produce a guide with recommendations for small municipalities that would stipulate exact steps and best practices for preventing cyber incidents. However, it is necessary

to first map the cybersecurity situation in small municipalities, which requires nationwide research to evaluate the actual problems and challenges they face.

Increase funding- the data from the conducted survey and other research studies indicate that funding for cybersecurity is insufficient at all levels. The state should allocate a greater number of finances dedicated explicitly to ameliorating cybersecurity in small municipalities. Municipalities should be financially supported when undergoing risk assessment, hiring experts, or attending courses or training in cybersecurity offered by third parties.

Cybersecurity experts for small municipalities – the state sector, in general, lack IT and cybersecurity experts who could help improve Slovakia's overall cybersecurity situation. Small municipalities cannot hire their own experts with their limited resources. The state should either provide municipalities with their own experts for consultations or guidance during the implementation of cybersecurity policies, or every region should have a dedicated expert who would be at the disposal of the small municipalities.

The above-mentioned measures are only a minor part of cyber-secure policies. They were proposed based on the data collected from a survey that was sent to small municipalities across Slovakia. A more complex set of policies and practices are required if the municipality wishes to maximize the level of protection against cybercriminals. However, evaluating and determining what municipalities struggle with is necessary. Therefore, further research would be needed to map the overall cybersecurity situation of small municipalities in Slovakia. It is important to pay attention to cybersecurity in small municipalities since hackers could steal citizens' sensitive information and violate their right to privacy. Cyber-attack could also take down the systems that provide e-services to citizens. Recovery of the functionalities might, in some instances, take weeks or even months.

The fight between “David” and “Goliath” does not necessarily lead to the win of Goliath. If small municipalities develop coherent cybersecurity plans and the state supports those attempts, hackers will have a hard time trying to break into the systems. All that is needed is a cooperative approach of the state and small municipalities.

REFERENCES

Act No. 69/2018 Coll., Act on Cybersecurity and on Amendments and Supplements to certain Acts. 2018. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/.

Act No. 95/2019 Coll., Act on Information Technologies of Public Administration and Supplements to certain Acts. 2019. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/95/20200701.

Decree No. 164/2018. 2018. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/164/.

Decree No. 179/2020. 2020. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2020/179/#prilohy.priloha-priloha_c_2_k_vyhlaske_c_179_2020_z_z.

Duncan, Ian. 2019. "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts." The Baltimore Sun, May 29. Accessed 29.01.2023. https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomwareemail-20190529-story.html.

ENISA. 2015. Definition of Cybersecurity, Gaps and overlaps in standardization. Accessed 29.01.2023. https://www.enisa.europa.eu/publications/definition-of-cybersecurity/@@download/fullReport.

Kobzová, Lucia. 2023. A Utopia for Realists: Effective e-Government in Slovakia. Bachelor Thesis, Bratislava International School of Liberal Arts.

Ministry of investments, regional development, and informatization. N.d. Bezpečnostná dokumentácia- metodiky. Accessed 29.01.2023. https://www.mirri.gov.sk/sekcie/informatizacia/kyberneticka-bezpecnost/bezpecnostna-dokumentacia-metodiky/index.html

National Security Authority. 2021. Cybersecurity Risk Analysis Methodology. Accessed 29.01.2023. nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf

Preis, Benjamin and Susskind, Lawrence. 2020. "Municipal Cybersecurity: More Work Needs to be Done." Urban Affairs Review 58, no. 2. Accessed 29.01.2023. https://journals.sagepub.com/doi/full/10.1177/1078087420973760

Ocampo, Rolando Hector. 2021. Municipal Governments and the Need for Cybersecurity. Master Thesis, University of Houston.

Thompson, Lisa. 2019. Cybersecurity Best Practices for Municipalities. New Hampshire Town and City, July/August.

APPENDIX

Note: this survey was originally distributed in the Slovak language

SURVEY ABOUT THE CYBERSECURITY IN SMALL MUNICIPALITIES

This questionnaire is devoted to the topic of cybersecurity in small municipalities. It takes place as part of the Security Academy, six months educational program on security issues. This research is carried out by student Lucia Kobzová under the director of the Department of Education and Awareness at the National Cyber Security Center Matej Šalmík. The objective is to find out the main trends and obstacles that small municipalities encounter when dealing with cybersecurity.

Answers are Anonymous, so please answer as honestly as possible. If you fill out the questionnaire online, your IP address will not be recorded. We will not be able to identify you or be able to find out whether you participated in this study or not. Your data will remain Anonymous during data processing for the final project report. Only the researcher and Matej Šalmík will have access to the obtained data. Both will be bound by confidentiality.
At the same time, by filling out the form, you agree to voluntary participation. By filling out and sending the questionnaire you voluntarily agree to your participation in the survey and to the use of the obtained data for the above-explained purposes. However, you can decide not to answer the question for any reason or stop filling it in at any point.

Filling out the questionnaire will take approximately 10 minutes.

If you have questions about the research or the questionnaire, please contact the researcher at the email address: lucia.kobzova2@gmail.com

1. How many inhabitants does your municipality have?

500-1000
1000-1499
1500-1999
Other:

2. What e-services does your municipality provide to citizens?
3. Do you have experience in dealing with cyber incidents?

Yes/No

4. If you answered yes to a previous question, how did you handle the incident? (by yourself, you contacted NBU, a private company...)
5. What would help you handle the attack better?
6. Does your municipality have procedures for managing cyber security incidents?

Yes/No

7. If you answered yes to a previous question, who developed these procedures for you?

Private company
We adopted procedures and recommendations from the state
We developer our own internal procedures Other:

8. Do you have a part of the budget set aside for cybersecurity?

Yes/No

9. If you answered yes to a previous question, how much of the budget you have allocated for cybersecurity?
10. What are the major obstacles preventing you from implementing better cybersecurity measures?
11. What would help you to better implement cybersecurity measures?
12. Are you able to implement legal obligations stemming from Act 69/2018 Coll.?

Yes/No/Other:

13. If you answered no to the previous question, what obstacles prevent you from implementing those legal obligations?

CYBER CONFLICT: RUSSIA - UKRAINE WAR

Lovászová Eva, expert consultant: Spišák Matej

EXECUTIVE SUMMARY

Microsoft reported Russia's Advanced Persistent Threat (APT) carrying out cyber-attacks in coordination with Russian military forces on land, air, and sea in connection with the war in Ukraine. This essay argues that while cyber operations can have a significant influence on military operations and national security, they are unlikely to be the only or even the most important factor in determining a conflict's result. This essay presents evidence that some of the cyber-attacks connected to the invasion of Ukraine were part of a coordinated campaign alongside conventional warfare. However, the kinetic activity was much larger, and the author argues that cyber-attacks did not perform any special tasks that kinetic attacks could not. To conclude, the author suggests further investigation into the possibility of simultaneous military and cyber-attacks.

INTRODUCTION

Nowadays, cyberspace is omnipresent, with important consequences not only for global economic activity but also for international politics and transnational social ties. Key sectors and basic services of states such as energy, transport, healthcare, and finance are becoming increasingly dependent on digital technologies to manage their core business. Even though digitalization comes with a great number of opportunities and provides solutions for many challenges that countries have to face, it also brings cyber threats to the economy and society. Cyberspace is currently also considered the fifth domain of warfare conflicts, alongside military, land, sea, air, and space operations. Cyber risks can pose a risk to the security of modern governments, and they have become a national security issue and a new foreign policy tool. On account of this, states need to develop and improve their cyber defence and resilience (Craif and Valeriano 2018).

This essay aims to determine whether cyber warfare can play a substantial role in a military confrontation and go beyond conventional warfare, which

will be exemplified and analyzed by certain events of the Russo-Ukrainian war with a quick outline of actions in this area. The secondary goal is to decide if Russian military actions are coordinated with its cyber operations in the Russo-Ukrainian war. We will be supporting the argument that, while the cyber domain can play a role in modern warfare, it is unlikely to be the deciding element in a conflict's result. In other words, while cyberattacks and cyber operations can have a considerable influence on military operations and national security, they are unlikely to be the only or even the most important component in determining a conflict's result. In this context, we present the statement of C. Martin, according to which: “the cyber domain may influence the war at the margins, but it will not decide it” (Bateman 2022, 6). As a part of the essay, we will also demonstrate Russian motivation and capability to conduct cyber-attacks as a part of their aggression in Ukraine.

CYBERSPACE, CYBER-ATTACKS, AND CYBER WARFARE

To start with, we believe it is important to define the terms and fundamental components of cyberspace. Almost anything involving networking and computers is considered "cyber", particularly in the security industry. Cyber, however, also includes cyberwarfare, cyberterrorism, and cyber conflicts. Due to the lack of agreement on what cyberspace truly is, it is important to stress that it lacks a universal definition (Ottis and Lorents 2009).

Cyberspace is a critical point in international relations and diplomacy, enabling the emergence of new sorts of conflicts. Furthermore, the 2014 NATO Summit in Wales affirmed that international law includes cyberspace and that cyber defence is part of NATO's basic collective defence responsibility (CDCOE 2022).

Although international law includes cyberspace, enforcement of this law is often challenging in practice. There are several problems in cyberspace, which include unclear borders, covert operations, and rapidly changing technologies. Governments may also have different views on what constitutes illegal conduct in cyberspace and how it should be addressed (United Nations 2015).

In 2016, at the NATO summit in Warsaw, cyberspace was acknowledged as the fifth domain of warfare, joining land, sea, air, and space operations. In this sense, it is worth noting that cyberspace is distinct from land, sea, air, and space operations since its geographical reach cannot be established (CDCOE 2022). The internet, telecommunications networks, computer systems, and embedded processors and controllers are only a few examples of the networked infrastructures that make up cyberspace (Sims, 2011).

A cyber-attack is an attempt to misuse information, which can be carried out by stealing, destroying, or disclosing it, with the aim of disrupting or destroying computer systems and networks (European Parliament 2022). Several types of cyber-attacks can compromise computer systems and data. For example, malware is malicious software that can harm a system by stealing data or compromising applications. Spyware is a specific type of malware that can track personal activities and commit financial fraud (Commonwealth of Massachusetts 2022). Moreover, there is a type of malware known as "wiper" that can carry out a cybersecurity attack by deleting or rendering data inaccessible on an infected system (Martinez 2022). Another type of attack is ransomware, which can prevent users from accessing their computer system and demand payment in exchange for access or data. This often involves virtual currency or bitcoin. Distributed denial-of-service (DDoS) attacks are another type of cyber-attack that aims to disrupt the server's infrastructure by flooding it with traffic from various sources, causing the website to slow down or become non-functional. This can also be used as a distraction for other scams. Lastly, spam and phishing attacks involve unsolicited emails or messages that can be harmful or attempt to steal sensitive information (Commonwealth of Massachusetts 2022).

Areas most at risk of cyber-attacks include transport, energy, healthcare, telecommunications and digital infrastructure, space, banks and financial markets, security, democratic processes, and defence. Attacks can be carried out, for example, through phishing emails with malicious links and attachments that aim to steal sensitive information, blackmail, or break into an organization after blocking its IT systems or data (European Parliament, 2022).

The conventional understanding of war has changed in recent years, and nowadays the concept of hybrid and cyber war is more often mentioned. However, in both cases, there is a lack of a universal definition (Melková 2016). The term cyber warfare is often confused with terms such as cyber terrorism or cyber espionage. It should be mentioned that such activities use similar methods and techniques but are not cyber warfare per se (Sheldon 2022).

Jirásek defines cyber warfare in the Dictionary of Cyber Security as "Use of computers and the Internet to wage a war in cyberspace. System of extensive, often politically motivated, related and mutually provoked organized cyber-attacks and counterattacks". A set of large-scale, often politically or strategically driven, linked, and mutually induced orchestrated cyber-attacks and counterattacks (Jirásek et.al 2015, 58).

From Sheldon's point of view, cyber warfare occurs within computers and the networks that connect them and is conducted by nations or their proxies against other states. Cyber warfare is most commonly used to disrupt or destroy government and military organizations (Sheldon 2022).
In our opinion, cyber warfare is the use of computer networks and technology to conduct attacks on the digital infrastructure of a country, organization, or group, with the intent of causing harm, disruption, or espionage. We also still need to take into account the potential consequences of cyber-attacks. If violence occurs online, it may also occur offline and if states do not take credit, it can still be political as we witnessed during the Russian-Georgian and Russian-Estonian conflicts in 2007 and 2008, or cyber-attacks as part of Russian aggression in Ukraine which will be discussed below.

RUSSIAN CYBER THREAT GROUPS

In this essay, we refer to Russian cyber threat groups as a general term for cybercriminal groups that operate from Russia or have connections to the Russian government, institutions, or organizations. It is crucial to note, however, that many additional Russian cyber threat groups are not publicly known and may be responsible for numerous unprecedented cyber-attacks (Rapid7 2022).

Some of the Russian cyber groups that have gained notoriety for numerous cyber-attacks and operations in various parts of the world are:

APT29 (or Cozy Bear) is a cyber group that has been linked to Russia's Federal Security Service (FSB) and the GRU. It was responsible for several cyber-attacks, including an attack on the Democratic Party during the 2016 US presidential campaign.

APT28 (also known as "Fancy Bear") was a cyber organization associated with the GRU. It was behind several cyber-attacks, including one on the Organization for the Prohibition of Chemical Weapons (OPCW).

SandWorm is a cyber organization associated with the GRU. It is responsible for a variety of cyber assaults, including an attack on a Ukrainian power plant in 2015 and attacks on Western targets such as ministries, universities, and businesses (Rapid7 2022).

RUSSIA'S CAPABILITY TO CONDUCT CYBER-ATTACKS

We believe that it is necessary to demonstrate Russia's capability and motivation to carry out cyber-attacks to demonstrate the implications this may have for international security, using specific incidents to highlight Russian interests in cyber-attacks:

1. Already during the annexation of Crimea in 2014, when President Vladimir Putin signed the agreement to incorporate Crimea into Russia, there were various cyber incidents, the number of which was especially considerable in comparison to the prior time. Cyber-attacks against Ukrainian telecommunications networks, websites, and other forms of communication were perhaps the most serious incidents. These attacks are ascribed to different hacktivist organizations, and state-sponsored attacks are also covered. Simultaneously, cyber espionage targeting vital Ukrainian government material was revealed over time. Furthermore, there have been attempts in cyberspace to steal information related to the crash investigation across the various European countries involved after the crash of flight MH17 and the subsequent events around it (Bateman 2022).
2. When the Russian army invaded Georgia, it was accompanied by cyber-attacks. This incident, which occurred along with military activities, is widely referred to be the first occurrence in which cyber-attacks were deployed concurrently with military operations. Russia is denying any participation in these cyber-attacks. However, it was later determined

that the majority of the attackers' servers were owned by the Russian cyber group called Russian Business Network (RBN). RBN is a group of professional Russian hackers and nationalists (Gotsiridze 2019).

3. Another factor to consider is cyber-attacks in Estonia in 2007, which were carried out in retaliation to the Estonian government's demolition of the Soviet war memorial in Tallinn. These harmful cyber operations are noteworthy because they represent the first case in which a foreign actor attacked the state's national security via a cyber operation. Although there is no clear evidence that these assaults were carried out by the Russian government, they were beneficial to Russia (Kozlowski 2020; Ottis 2007). In connection with the possible involvement of the Russian government during the cyber-attacks on Estonia in 2007 and Georgia in 2008 being still a matter of debate, we are convinced that cyber-attacks, unlike traditional attacks, can be difficult to correctly attribute, as we mentioned above.
4. Ukraine has shown a strong commitment to building its cyber defences and has made significant investments in upgrading its capabilities. However, the United States, the United Kingdom, and the European Union have more counter-attack resources. According to Madnick, Russia is undoubtedly the most likely suspect in testing cyber weapons in Ukraine (Madnick 2022).

With this regard, we would also like to mention Not Petya malware, which caused significant damage and disruption to computer systems around the world in 2017. This was one of the most devastating cyber-attacks in history. This type of malware was initially spread in Ukraine, but it quickly spread to other systems around the world. A state actor is believed to be behind the attack, with many experts pointing to Russia as the likely perpetrator (Madnick 2022).

It can be assumed that Russia has demonstrated its capability to conduct malicious cyber operations as well as its ability to coordinate with military actions. But can a cyber-attack, however, be more significant and sophisticated than a military attack in a war?

In the next section, we will focus on Russian aggression in Ukraine, where cyber-attacks go hand in hand with military action. Hackers aim to destroy

and disrupt the functioning of government agencies as well as critical infrastructure and at the same time cause public distrust in the country's leadership. Cyber-attacks can disrupt basic services such as water supply, healthcare, power plants, etc. (European Parliament 2022).

RUSSIA‘S WAR ON UKRAINE: THE ROLE OF CYBER-ATTACKS

According to Microsoft, Russia's Advanced Persistent Threat (APT) carried out cyber-attacks coordinated with Russian military forces on land, air and sea. We present multiple events as an example:

1. Russia is believed to have been conducting reconnaissance and preliminary cyber capabilities on some of Ukraine's energy and communications networks since March 2021 (Willett 2022). When Russian military units gradually began to move to the border with Ukraine in 2021, they tried to gain access to intelligence information about Ukraine's military and foreign partnership. In this context, phishing attacks on Ukrainian military e-mail accounts were recorded. During 2021, several Russian cyber espionage groups with ties to the Kremlin launched spear-phishing campaigns to gain access to the accounts of foreign military advisers and aid workers based in Ukraine and defence-related organizations in Ukraine (Microsoft 2022). A few weeks before the invasion of Ukraine, similar techniques as in Georgia in 2008 and Ukraine in 2014 were used, such as a DDoS attack against websites of Ukrainian government ministries, or malware that wiped hard drives. Some of these attacks were interrupted thanks to the Ukrainian cyber defence capability (Willett 2022). It is believed that these attacks may have made little contribution to Moscow's initial invasion, however, they have caused minor damage to Ukrainian targets since then (Bateman 2022).
2. On the day of the Russian invasion of Ukraine on February 24, 2022, a cyber-attack interrupted broadband satellite internet access by deactivating modems that communicate with Viasat's KA-SAT satellite network. Viasat is an internet provider for tens of thousands of people in Ukraine and Europe. The attack is believed to have been carried out via the "AcidRain" malware, which is designed to remotely wipe vulnerable modems and routers. Viasat also believes that the purpose of this attack was to disrupt service and not to steal data. Acidrain was later attributed by the United States, the United Kingdom, Australia,

New Zealand, and Canada to the Russian military intelligence service (GRU), and they linked it to other destructive wiper malware Whispergate, which was also aimed at harming the Ukrainian government and the private sector (Cyber Peace Institute 2022). It should not be forgotten that we noticed similar tactics of distribution of the denial-of-service attacks in the case of Estonia and Georgia in 2007-2008. This might have provided a tactical advantage in the battle for Kyiv and the cyber disruption of Viasat modems could have severely hampered Ukrainian front-line communications. However, within the first few weeks of the conflict, cyber-attacks plummeted in number and novelty (Bateman 2022). This case was likely coordinated with the Russian kinetic attacks. The Viasat hack was almost simultaneous with the first Russian kinetic attacks and may have helped them to disable Ukrainian command and control during the invasion, with consequences for other European countries as well. On the other hand, considering the high-intensity military operations, these attacks were barely registered (Bateman 2022). The simultaneous occurrence of a destructive cyber-attack on Viasat and the first Russian kinetic attacks are, in our view, strong evidence of the coordination of cyber and kinetic forces.

3. Another example is the events of March 11, 2022, when the first Russian strikes in Dnipro hit government buildings. On this day, the Dnipro government agency was also attacked with a destructive implant. More details regarding this cyber-attack are not publicly accessible, but Ukraine's State Emergency Service announced three Russian airstrikes that landed in Dnipro near a preschool and an apartment building and a shoe factory. Thereby, it is believed that these cyber-attacks have been carried out in support of the Russian military strategic and tactical objectives (Microsoft 2022). From the point of view of M. Smeets, cyber and kinetic actions "may not directly depend on each other, but each provides individual contributions to the same goal" (Bateman 2022).
4. Cyber-attacks also occurred on March 2, when Microsoft identified that a Russian group was located laterally on the computer network of the largest nuclear power plant. The next day, the Russian army attacked and occupied this nuclear power plant. At the same time, Russia compromised the government's computer network and

launched eight cruise missiles at the city's airport. However, it can be argued that none of these cyber-attacks resulted in disabling effects and therefore cannot be identified as successful cyber-attacks. Even if coordinated with physical attacks, they either failed to achieve their intended effects or were intended as cyber-intelligence operations to support kinetic targeting (Bateman 2022).

5. A better example is the July 1 cyber-attacks, when the Ukrainian energy company DTEK announced that Russia had unsuccessfully attempted a cyber-attack on the company, which was intended to destabilize the technological processes of the companies that produce and distribute energy. In this case, the Russian hacking group XakNet, which has ties to the Kremlin, claimed responsibility. At the same time, rocket and artillery attacks were launched on the Kryvorizka thermal power plant of DTEK. Thus, the Russian kinetic and cyber-attacks aimed at the same goal, which was also confirmed by DTEK (Bateman 2022).

Apart from the events mentioned above, Microsoft recorded many destructive wiper attacks on hundreds of systems in the Ukrainian government, IT, energy, and financial organizations through various techniques to gain access to their target, such as phishing, malware, or DDoS attacks. In this way, they can also perform espionage and surveillance. This is mainly about groups with suspicions of ties to the GRU. Many of these operations attempted to disrupt citizens' access to information and vital life services. It is believed that these actions are intended to undermine the political elite. Although it is not officially confirmed whether cyber and kinetic forces are actively cooperating, Microsoft states that they are working together to disrupt and destroy the Ukrainian government and military functions as well as public trust in these institutions (Microsoft 2022).

Another factor to consider is cyber-attack effects, as there have been no publicly reported examples of cyber disruption to any Ukrainian or foreign-provided weapons systems or other military equipment. On the other hand, kinetic effects caused the loss of 10,000 Ukrainian men, 1,300 infantry fighting vehicles, 400 tanks, and 700 artillery systems (Bateman 2022). Furthermore, since the invasion of Ukraine on February 24, 2022, Russian cyber operations have been characterized by many analysts as insufficiently

sophisticated and poorly planned. At the same time, they agree that cyber operations did not play a major role in advancing Russian goals (Bateman 2022).

Due to the lack of sufficient evidence of cyber-attacks, Bateman hypothesizes that cyber-attacks may have contributed to unrest among residents and officials, particularly in cases of misuse and loss of sensitive data, but cannot match the lethal, physical, missile attacks, which most likely had a much greater psychological impact. However, a cyber-attack can prevent, for example, the reaction of local representatives of government agencies to incoming missiles (Bateman 2022). Some authors assume that Putin and his army are incapable of planning and conducting war in a way that is optimal for cyber operations. Ukraine, on the other hand, has a resilient digital ecosystem thanks to cyber security and an increase in cyber support from global companies and governments (Bateman 2022),

CONCLUSION, LIMITATIONS, AND RECOMMENDATIONS

The cyber-attacks in the Russia-Ukraine war in 2022 are the first wartime cyber confrontation between two states with basically equal cyber capabilities. Ukrainian cyber capability was boosted by Western governments and private sector organizations. Meanwhile, Russian cyber activities looked to be less effective than planned. Both parties were pressed by cyber vigilantes (Willett 2022).

Based on the evidence we have gathered, it appears that cyber-attacks related to the invasion of Ukraine are not isolated incidents, but part of a coordinated campaign alongside conventional warfare. Although they seem minor at first glance, their impact can be very serious. The Viasat hack and other cyberattacks that took place at the same time as the first Russian kinetic attacks may have helped disable Ukrainian command and control, with consequences not only for Ukraine but also for other European countries. Also, the landing of three Russian airstrikes in Dnipro near populated areas leads us to assume that these cyber-attacks were carried out in support of the strategic and tactical goals of the Russian military. Therefore, it seems that cyber-attacks are not just a peripheral phenomenon in Ukraine, but rather an important element of the Russian attack on Ukraine.

According to the limitations of this paper, we wish to point out our concern about the lack of proper detection, analysis, and public reports of cyber operations in the context of the war in Ukraine, which has a growing influence on both the public and private sectors. Certain relevant information may not be made public yet or may be suppressed completely for reasons of national security. Furthermore, the Ukrainian government may be cautious to acknowledge specific cyber-attacks for fear of damaging its reputation or provoking future Russian action. Considering all the cyber and military operations analyzed in the presented essay, we tend to believe that cyber-attacks did not perform special tasks that kinetic attacks could not. Nevertheless, they had rather a secondary role because they focused on the same targets as kinetic attacks - communication, electrical and transport infrastructure. In the analyzed attacks, it is clear the kinetic activity was much larger.

In light of the above, we recommend a closer investigation into more examples of the possibility of simultaneous military and cyber-attacks regarded to Russian aggression in Ukraine. We should also emphasize the critical significance of strengthening Western cyber defences against these sorts of foreign destructive cyber-attacks.

REFERENCES

Bateman, J. 2022. Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. Accessed 25.01.2023. https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

Commonwealth of Massachusetts. 2022. Know the types of cyber threats. Accessed 27.02.2023. https://www.mass.gov/service-details/know-the-types-of-cyber-threats.

Craig, A., Valeriano, B. 2018. Realism and Cyber Conflict: Security in the Digital Age. Accessed 25.01.2023. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/.

Craig, A.J.S. 2020. Capabilities and Conflict in the Cyber Domain: An Empirical Study. Accessed 25.01.2023. https://gfsis.org.ge/blog/view/970.

Cyber law CDCOE. 2021. Georgia-Russia conflict (2008). Accessed 03.01.2023. https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008).

Cyber Peace Institute. 2022. Case Study: Viasat. Accessed 25.01.2023. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

European Parliament. 2022. Cybersecurity: why reducing the cost of cyberattacks matters. Accessed 24.01.2023. https://www.europarl.europa.eu/news/en/headlines/society/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters.

Gotsiridze, A. 2019. The Cyber Dimension of the 2008 Russia-Georgia War. Accessed 25.01.2023. https://gfsis.org.ge/blog/view/970 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Jirásek et. al. 2013. Výkladový slovník Kybernetické bezpečnosti. Policejní akademie ČR v Praze. Accessed 25.01.2023. https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf.

Kozlowski, A. 2020. Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. In European Scientific Journal Vol 3 (Special Edition). Accessed 24.0.12023. https://www.researchgate.net/publication/345883552_Comparative_analysis_of_cyberattacks_on_Estonia_ Georgia_and_Kyrgyzstan.

Madnick, S. 2022. What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare. Accessed 25.01.2023. https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare.

Martinez, F. 2022. Analysis on recent wiper attacks: examples and how wiper malware works. Accessed 26.02.2023. https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works.

Melková, M. 2016. Úvod do problematiky kybernetickej bezpečnosti. Univerzita Mateja Bela: Fakulta politických vied a medzinárodných vzťahov. ISBN 978-80-206-1703-3.

Microsoft. 2022. Special Report: Ukraine An overview of Russia's cyberattack activity in Ukraine. Accessed 25.01.2023. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Ottis, R.; Lorents, P. 2009. Cyberspace: Definition and Implications. Cooperative Cyber Defence Centre of Excellence. Accessed 25.01.2023. https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf.

Rapid7.com. 2022. The Top 5 Russian Cyber Threat Actors to Watch. Accessed 26.02.2023. https://www.rapid7.com/blog/post/2022/03/03/the-top-5-russian-cyber-threat-actors-to-watch/.

Sheldon, J.B. 2022. Cyberwar. Accessed 25.01.2023. https://www.britannica.com/topic/cyberwar.

Sims, J.W. 2011. Cybersecurity: The Next Threat to National Security. p.3. Accessed 26.01.2023. https://www.hsdl.org/c/view?docid=815056.

United Nations. 2015. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Accessed 26.02.2023. https://digitallibrary.un.org/record/799853.

Willett, M. 2022. The Cyber Dimension of the Russia–Ukraine War. Accessed 26.01.2023. https://www.tandfonline.com/doi/full/10.1080/00396338.2022.2126193.

A COMPARATIVE ANALYSIS OF PREPAREDNESS OF V4 COUNTRIES FOR THE IMPLEMENTATION OF THE NIS 2 DIRECTIVE

Minichová Sofia, expert consultant: Hettych Tomáš

EXECUTIVE SUMMARY

This paper examines the preparedness of the V4 countries (Czechia, Hungary, Poland, and Slovakia) for the implementation of the NIS 2 Directive based on their current national legislations. With the main novelties of the NIS 2 in comparison to its predecessor NIS 1 being an extended scope of the covered sectors and entities, increased cooperation requirements and stricter enforcement, this essay compares to what extent some of the newly introduced obligations and aspects are already covered in the national legislations in place. Through analysing the national cyber security laws as they are, the essay reveals a trend of later transposition of NIS 1 obligations into national frameworks equal to more up-to-date coverage of what is desired to be updated/introduced now, confirming the original hypothesis of the author. It also becomes clear that collecting all of the obligations previously introduced and updated or added later in one comprehensive document that is being kept up to date is more efficient and easier to navigate than introducing new legislative acts with each update of requirements. To achieve a high common level of security, utilizing broader definitions of the scope of obligations is preferable to narrower definitions.

INTRODUCTION

December 27, 2022, marks the day of publication of the long-negotiated and long-awaited Directive 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (hereinafter “NIS 2 Directive” or “NIS 2”), introducing a new standard of cybersecurity resilience required from many service providers operating within the European Union (hereinafter “The Union” or “EU”). From its date of entry into force – January 16, 2023, the Member States have 21 months to transpose this Directive into national legislations, with the measures imposed by this legislation being applicable from October 18, 2024. The NIS 2 Directive

introduces a considerably broader scope of covered sectors and entities and prescribes more stringent measures not only for the entities themselves but also in terms of enforcement, supervision and cross-border cooperation in comparison to the current framework established by the predecessor - Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (hereinafter "NIS 1 Directive" or "NIS 1"). The implementation of NIS 2 will present a new challenge for the day-to-day operations of many companies. New cybersecurity-related obligations to be fulfilled by those obligated are an indisputable consequence of the new Directive. The extent to which these obligations will be entirely unprecedented will greatly depend on the current national legislations.

While the NIS 1 aimed to achieve harmonization, the reality was that its implementation was not synchronized among all Member States. There were significant variations in the transposition dates and interpretations, resulting in differences in the wording and scope of obligations within each Member State's NIS 1-transposing national legislation. These discrepancies were due to the Directive's minimum harmonization nature.

In light of the above-mentioned, this essay argues that these minor differences and liberties taken in transposing NIS 1 into national legislation will now play a crucial role in how Member States and the businesses operating within them adapt to the requirements of the revised Directive. This will be showcased by analyzing the national cybersecurity legislations of the V-4 countries - Czech Republic, Hungary, Slovak Republic and Poland, countries with close geographical proximity and a shared historical background, nevertheless with identifiable differences in approaches to the NIS 1 transposition. The findings of this analysis will also serve as grounds for formulating recommendations for the most effective transposition of the revised Directive, identifying good practices leading to an easier adjustment to legislative developments. In doing so, this essay is structured as follows:
Firstly, a brief introduction into the context of the EU cybersecurity regulatory framework is provided with a specific focus on the differences between the NIS 1 and 2 Directives. The rationale for the revision of the first Directive and an outline of transposing national legislations of the countries

are in focus. Next, in the analysis, specific differences in national rules are identified and assessed to identify the most effective way of transposition. Lastly, the outcomes of the analysis are discussed, and certain recommendations are formulated.

BACKGROUND AND CONTEXT

FROM NIS 1 TO NIS 2

In the pursuit of improvement of the functioning of the EU internal market in the current environment of rapid technological innovation and digitalization, NIS 1 was introduced in 2016 as the first Union-wide legislation on cybersecurity aiming to increase and harmonize Member States' cybersecurity capabilities. While to an extent successful in the former, the latter proved difficult despite the establishment of a Cooperation Group and a Computer Security Incident Response Teams Network - different Member States adapting to the ever-changing landscape of threats at different paces. The European Commission (2023) in this regard identified four main challenges with the implementation of NIS 1, including inconsistency of cyber resilience across Member States and sectors, lack of common understanding of the main threats and an interconnected lack of joint crisis response. Supplemented by substantial differences in the level of cyber resilience of individual businesses operating within the EU territory, it became clear that harmonization and stricter enforcement are necessary to respond to growing threats arising from interconnectedness and digitalization and to prepare for what is yet to come.

Adopted in 2022, the NIS 2 Directive continues in the steps of its predecessor in the sense of maintaining the nature of minimum harmonization measure, allowing in itself for differences in the level of Member States' cybersecurity, provided the minimum obligations of the Directive are met. While this "limitation" stems from the importance of individual Member States being able to legislate themselves in the matter of security, the EU did try to cover and improve as much as was feasible with this Directive (European Commission 2023). This is visible through the expansion of the scope of the Directive to cover substantially more sectors, and therefore also entities, in comparison to NIS 1. For the sake of more effective enforcement, all covered entities are classified based on their importance into two separate categories, with the most essential ones being subject to a stricter, ex-ante supervisory regime. In the pursuit of fixing the inconsistency

amongst businesses' cyber resilience and hence ultimately strengthening the cybersecurity of all EU citizens, a risk management approach is prescribed by the Directive, mandating a minimum list of basic security elements. Additionally, to improve cooperation and common understanding, incident reporting and information-sharing requirements are defined more precisely and a framework for new vulnerability disclosure is established.

TRANSPOSITION OF NIS 1 INTO NATIONAL LEGISLATIONS AND THE CONSEQUENCES THEREOF

While trying to answer the research question in sufficient depth, it is important to look at the wider context surrounding the NIS Directives. By default, the transposition of EU directives into national laws needs to take place within two years after a directive has been adopted (EUR-lex). For NIS 1 this deadline lapsed in May 2018, with different Member States adopting the Directive into national legislation at different moments of this period. For the four Member States under review, there is a slight difference between the transposition dates. The Czech Republic - being the first among the four countries - transposed NIS 1 into national legislation in June 2017 through Act no. 205/2017, which changed and added to the already existing Act no. 181/2014 on cybersecurity (National Cyber and Information Security Agency). Meanwhile, Slovakia transposed NIS 1 by adopting an entirely new legislation only in January 2018 - Act no. 69/2018 on Cybersecurity, and Poland, utilizing the same way as Slovakia of creating a new legislative act, managed to transpose NIS 1 even later and after the transposition deadline in July 2018 - Act on the National Cybersecurity System. Lastly, Hungary took an entirely different approach from the other countries in the region and transposed the Directive over time, but mostly in 2018, through amendments of numerous Governmental Decrees addressing only the elements of NIS 1 that were missing in the already in-place national cybersecurity legislation. This made the Hungarian cybersecurity framework highly fragmented into specific provisions in different pieces of legislation per sector and hence a lot more difficult to navigate in comparison to the others. For this reason, the provisions of Hungarian law will be mentioned less specifically in the analysis, focusing mostly on general observations that can be easily deduced. The fact that each one of the countries concerned had to at least adjust their existing national

legislation indicates the strengthening of the cybersecurity effect that NIS 1 brought with itself, requiring the Member States to, among other things, draft national cybersecurity strategies, establish Computer Security Incident Response Teams (CSIRTs) and choose national competent authorities for the NIS framework (Markopoulou, Papakonstantinou and de Hert 2019, 2).

Looking at the substance of the transposing legislation, however, an earlier date of adoption seems to suggest less comprehensive and less detailed provisions in a wide range of aspects - from sectors covered, through security measures required, to maximum amounts of penalties to be imposed. This can be attributed to the fact, that during the transposition period, the European Commission was addressing on an ongoing basis certain elements of the Directive to guide the Member States towards a more efficient implementation (see for example COM (2017) 476), causing MSs with a later transposition date to have their national legislations more in line with the full range of Commission's expectations. The difference can be demonstrated the easiest by looking at sectors covered by current legislation in Czechia and sectors covered by current legislation in Slovakia. While both regimes cover a great amount of them, upon close inspection of each it becomes apparent the Slovak one lists more specific entities within each sector, covers some sectors entirely out of the scope of the Czech legislation and therefore presents a more up-to-date overview of obliged sectors in terms of the future requirements of NIS 2. Assuming compliance of service providers with the requirements of national legislations, it becomes clear that the preparedness for the more stringent demands of NIS 2 varies among different Member States - a phenomenon that is analyzed in the following section.

ANALYSIS

The analysis of NIS 2 preparedness of the Member States that are the subjects of this paper was performed as a comparison exercise between the scope and obligations of the current national laws and the requirements of the new Directive. Although containing many differences in the details of their provisions, all the national legislations follow more or less the same structure in the contained provisions. This made it easy, for the sake of efficiency and clarity of the outcomes of the analysis, to group provisions

into categories covering different aspects of the NIS 2 Directive. Firstly, national cybersecurity frameworks were compared in terms of national cybersecurity strategy (art. 7 NIS 2), coordinated vulnerability disclosure measures (art. 12 NIS 2), large-scale incidents responsibility (art. 9 NIS 2), and national competent authorities' dedication (arts 8-11 NIS 2). Second, risk management measures and reporting obligations were looked at through provisions specifying the risk management measures (art. 21 NIS 2) and training obligations (art. 20 NIS 2) and provisions containing notification obligations (art. 23 NIS 2). Third information sharing/disclosure obligations were analysed requiring domain name registration data registries (arts 27-28 NIS 2), exchange of relevant information (art. 29 NIS 2) and providing a possibility for voluntary reporting (art. 30 NIS 2). Lastly, supervision and enforcement measures were scrutinized under articles 32, 33, and 34 NIS 2 setting out an ex-ante and ex-post regime of supervision and rules on penalties respectively. For the sake of complete analysis, it was also crucial to not only look at provisions but also the two annexes to the Directive specifying the personal scope of the cybersecurity legislation.

NATIONAL CYBERSECURITY FRAMEWORKS

One of the most crucial and innovative elements of NIS 1 was the requirement to draft a comprehensive national cybersecurity strategy outlining the general approach to cybersecurity threats and challenges within a Member State including the definition of objectives and priorities, identifying mitigating measures and listing public and private actors involved. By requiring such a strategy, it was ensured each Member State has a framework in place to be used as a starting point in dealing with cybersecurity issues, providing guidance as to the process of dealing with the issue in an effective and coordinated manner and that this framework is up to the standard of EU expectations. NIS 2 adds to the previously imposed obligations in this context by requiring an enhanced coordination framework to be part of the strategy to further strengthen the envisioned unity in cybersecurity prevention and response, by mandating a coordinated vulnerability disclosure to increase efficiency in the exchange of knowledge, and it further elucidates upon the responsibilities of national competent authorities.

In terms of differences between countries, there do not appear to be many. All countries under review will need to add the new framework for enhanced cooperation into their strategies as a completely new element. This should not present an issue as the strategies are anyway drafted for a limited period and the time for a new one is soon to come in all three Poland (2024), Czechia and Slovakia (2025). In Hungary the national strategy does not seem to have an expiration date and considering the previous developments will most likely just be tweaked a little to comply with the new obligations.

Similarly, all countries are to encounter the same level of burden in implementing the coordinated vulnerability disclosure requirement. Vulnerabilities assessments being performed by CSIRTs, it should not be difficult to task one with the specific coordinated disclosure role; and in adopting a national plan of reaction to large-scale incidents – the only element of article 7 NIS 2 that appears to be missing in national legislations. Single national points of contact being a well-established practice at this point in all four jurisdictions, the Czech Republic will need to look into mandating a secure communication channel (safe communication infrastructure already required by law in Slovakia and Poland for information sharing between CSIRTs) and further clarifying the actual tasks and responsibilities of CSIRTs in more detail to prevent non-compliance with the new Directive.

RISK MANAGEMENT AND REPORTING

In the context of risk management, the focus switches from obligations directed at Member States and the public sector and the onus is instead laid on measures that are required to be taken by obligated entities to prevent cybersecurity incidents from happening or to at least minimize the chances of them occurring. The Directive provides a list of the minimum measures that need to be made obligatory for essential and important entities (all entities covered by the Directive), some of which are already covered to a great extent in national legislations. The one element that seems to be commonly missing is ensuring the security of the supply chain, and while Slovakia and Poland have the other elements already required by law at least to an extent, Czechia also needs to include the obligation to publicly disclose information about vulnerabilities and the solutions thereof. This is an

important measure in terms of prevention and might prove tricky to be adopted by entities that had no such obligation previously as it requires considerable effort in constant monitoring and disclosure, and it also means more public scrutiny for a company.

Perhaps the most changes that will need to be made in national legislations in the upcoming months arise from the notification of incidents with significant impact obligation that demands obligated entities to inform competent authorities without undue delay but no later than 24 hours about not only incidents but also threats with significant impact. In certain instances, it might be also necessary to inform recipients of the service and/or the public. Looking at the countries under review and to what extent these are already part of the legislation, Poland which transposed the first NIS as the latest does seem to have most of them covered – including the 24-hour notification obligation which can be quite burdensome to implement making its transition to NIS 2 smoother in comparison to the others. Slovakia, although missing the 24-hour notification requirement, in addition only misses notification of recipients of service and notification of serious threats to competent authorities. These two are missing within the Polish legislation as well. In Hungary, a commonly used phrase in law - “without undue delay” is used when talking about both incident and threat notification. On the other hand, Czechia with the earliest transposition of NIS 1 seems to be missing a lot more, including a monthly notice to the European Union Agency for Cybersecurity about threats and incidents which is an important requirement in terms of cooperation, coordination and preparedness on a European level.

Similarly, to the above mentioned, in terms of TLD registries containing complete domain name registration data, Slovakia, Hungary and Poland already include TLDs as part of obligated entities hence making them compliant with a lot of security obligations and disclosure requirements. Therefore, creating a database with full and accurate information should not be difficult. However, in Czech law, there is no mention of TLDs whatsoever making this obligation an entirely new one that will require substantial effort to comply with.

INFORMATION SHARING AND DISCLOSURE OBLIGATIONS

In this section of NIS 2, the exchange of information among obliged entities and voluntary reporting of all other entities are addressed. In terms of voluntary reporting, article 30 seems to only be fully incorporated into the Slovak and Hungarian national laws at the moment, while in Czech law it is limited to incidents (instead of also including threats), and in Polish law, it is missing altogether. Although covered to a different extent in national laws, due to its voluntary nature implementation of this article into national laws is not expected to bring about heavy compliance burdens.

In the context of article 29 NIS 2 and the sharing rules it introduces a newly imposed burden of information sharing on obligated entities which might be felt more substantially (although voluntary, peer pressure within the field could play a decisive role in whether to partake in such knowledge exchange). Only Slovakia seems to have already included something akin to the expectations of the exchange of information among essential and important services in its existing law, having a uniform system of cybersecurity in place. Czechia and Poland however only appear to have such a system amongst public bodies, and the exchange of information between the regulated entities will have to be established to comply with the new Directive.

SUPERVISION AND ENFORCEMENT MEASURES

In contrast to NIS 1, NIS 2 with the introduction of the distinction between essential and important services also introduced two separate supervisory regimes for the two categories of services. While important services will continue to be supervised ex-post, for essential services ex-ante supervision is mandated by the new Directive. One of the core issues with NIS 1 and subsequently also one of the core drivers for NIS 2 is lack of enforcement. National laws are almost silent on supervision and enforcement other than a general mention of authorities tasked with control and a brief outline of penalties and post-event reparation measures.

All four national laws lack sufficient frameworks of control - both in terms of measures to be adopted to fix the situation and in terms of the powers of competent authorities. Not only do the current national laws fail to accommodate the newly established ex-ante regime for essential services,

but they also seem to run short of being able to address the ex-post requirements of article 30, once again highlighting the previous non-satisfactory supervision and enforcement of regulated entities and emphasizing the burden all the Member States under review will face in implementing the new NIS.

Regarding fines that can be imposed by the authorities in control, only Slovakia seems to come close to the maximum penalties envisioned by the Directive. Czechia and Poland on the other hand in their current laws work only with very limited fines both in amount and in the reason for their imposition. Implementation of stricter fines in national legislation together with stricter supervision and enforcement has not only the potential of acting as a strong deterring tool but also can contribute to national budgets allocated to cybersecurity if the fines collected could be in turn further infused into the field.

PERSONAL SCOPE OF NIS 2

One of the biggest changes brought about by the new Directive is the substantial expansion of the entities covered by and falling within the scope of obligations of NIS 2. Not only are there more sectors covered than previously but there is also the distinction between essential and important services made, reclassifying some of the entities already covered into a category with a more stringent supervision regime. In comparison to entities already subject to national cybersecurity legislations previously, the newly obliged sectors that will need to be added to the legislation as essential services most commonly include public administration and space (in all countries under review) with Czechia surprisingly having the least amount of changes to make while Slovakia and Poland need to add some previously not included services within the sectors of electricity, oil, water, health and digital infrastructure. Similarly, some actors and sectors need to be included in the scope of national cybersecurity legislation in terms of important services such as food production, waste management, postal services and some digital providers - here Czechia has the most work to do in terms of including previously non-included sectors and service providers within.

CONCLUSION AND RECOMMENDATIONS

This essay attempted to summarize the new obligations to be included in national laws arising from the NIS 2 Directive for the V4 countries while highlighting the tendency of later transposition of the previous Directive suggesting a more comprehensive national framework and hence an easier adoption. This has been demonstrated on several occasions in the analysis of different parts of the Directive, resulting in Czechia being the first country to transpose the NIS 1 Directive and appearing as the country with the most changes to make in the context of the NIS 2 Directive. Czechia also appears as a country with the least specific provisions both in classifying the sectors and entities subject to the cyber security legislation and in outlining the responsibilities of supervisory bodies. However, in leaving the obligated entities defined loosely, it managed to be all-encompassing. Therefore, the following can be recommended for the upcoming implementation of the new NIS Directive:

1. The definition of the personal scope of the cyber security legislation is more beneficial if written broadly rather than very specifically. A broader definition provides for the inclusion of more sectors and all entities within, allowing for cybersecurity caution and preparedness to be more common and ultimately bringing about a higher level of cyber security for all citizens.
2. Although most likely contradictory to the wishes of the European Commission, later transposition allows for legislations to be more up-to-date with the latest developments in the field which in turn guarantees a lesser compliance burden with the introduction of an update to the legislation at the European level.
3. Transposing the EU Directive through updating an already-existent national act is only efficient in cases of comprehensive and unified legislation. In the case of cyber security obligations being introduced in multiple documents and with every necessary change updating all of them or even adding more proves difficult to navigate and is chaotic both for the general public and for the entities subject to the EU Directive.

REFERENCES

EUR-Lex. 2023. “Transposition.” Access to European Union Law. Accessed 2202.2023. https://eur-lex.europa.eu/EN/legal-content/glossary/transposition.html#:~:text=Transposition%20is%20the%20process%20of,their%20rules%20into%20national%20legislation.

European Commission, Digital Strategy. 2023. “Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).“ Accessed 31.01.2023. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive.

European Parliament and the Council of the European Union. 2023. “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”. 2016. Accessed 22.02.2023. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

European Parliament and the Council of the European Union. 2022. “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)”. Accessed 22.02.2023. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1677087117471&from=en.

Government of Hungary. “Government Decision 1838/2018 (XII.28.) on the Strategy for the security of network and information systems in Hungary” 208. Accessed 26.02.2023. https://nki.gov.hu/wp-content/uploads/2020/11/Strategy-for-the-security-of-network-and-information-systems-in-Hungary.pdf.

Government of Hungary. 2015. “Government Decree 187/2015 (VII.13.) on the functions and powers of the authorities responsible for electronic information security and the information security supervisor, as well as the determination of closed electronic information systems”. Accessed

26.02.2023. https://nki.gov.hu/wp-content/uploads/2020/11/Gov.Dec_.-187_2015-on-competent-authorities.pdf.

Government of Hungary. 2017. "Government Decree 249/2017 (IX.5.) on the identification, designation and protection of critical systems and facilities of the information and communication technologies sector". Accessed 23.02.2023. https://nki.gov.hu/wp-content/uploads/2020/11/Gov.Dec_.-249_2017-on-ICT.pdf.

Government of Hungary. 2018. "Government Decree 271/2018 (XII.20.) on the functions and powers of incident response centres, and the rules for security incident response and technical investigation, and for conducting vulnerability testing". Accessed 26.02.2023. https://nki.gov.hu/wp-content/uploads/2020/11/Gov.Dec_.-271_2018-on-CSIRT.pdf.

Markopoulou, Dimitra, Vagelis Papakonstantinou and Paul de Hert. 2019. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation." Computer Law & Security Review 35, no. 6 (November): 1-11. Accessed 31.01.2023. https://doi.org/10.1016/j.clsr.2019.06.007.

National Assembly of Hungary. 2013. "Act L of 2013 on the information security of state and municipal bodies". Accessed 36.02.2023. https://nki.gov.hu/wp-content/uploads/2020/11/Cyber-Security-Act_2013_50.pdf.

National Council of the Slovak Republic. 2018. "Act from 30 January 2018 about Cybersecuirty and Amendments to Certain Acts". Accessed 26.02.2023. https://www.slov-lex.sk/static/pdf/2018/69/ZZ_2018_69_20220630.pdf.

National Cyber and Information Security Agency (NUKIB). "Legislation." Accessed 22.02.2023. https://nukib.cz/en/cyber-security/regulation-and-audit/legislation/.

Parliament of the Czech Republic. 2014. "ACT No 181/2014 Coll. of July 23, 2014 on Cyber Security and Change of Related Acts (The Act on Cyber

Security)". Accessed 26.02.2023. https://nukib.cz/en/cyber-security/regulation-and-audit/legislation/.

ANNEX

The relevant part of the NIS 2 Directive	Slovakia	Czechia	Poland
National Cybersecurity Frameworks *(art. 7-13)*			
national cybersecurity strategy *(art. 5)* - definition of objectives and priorities, governance framework, identification of relevant assets and risks, identification of measures, list of authorities and actors involved, enhanced cooperation framework	framework for enhanced cooperation needs to be added	the elements of the strategy are not mentioned in the law at all, within the strategy itself everything seems to be addressed at least briefly - concrete implementation steps of the priorities and processes in a separate action plan	art 69 - the framework for enhanced coordination needs to be added, other than that fairly comprehensive (including education etc)
coordinated vulnerability disclosure *(art. 12)* - one designated national CSIRT a coordinator for coordinated vulnerability disclosure	vulnerabilities are being assessed as part of security measures (art. 20(3)(g)) - should be doable to choose one CSIRT from the many existent to coordinate disclosure of such vulnerabilities	Vulnerability assessment is one of the tasks of both governmental and national CSIRT - coordinated disclosure should be easily achievable	all three CSIRTs are to be notified about vulnerabilities and also conduct their own investigations into potential vulnerabilities so choosing one that will be able to competently disclose all of them should not be difficult + there is already an option for public disclosure in place for sharing vulnerabilities on a website
NCA responsible for large-scale incidents *(art. 9)* - one or more designated national competent authorities for management of large-scale incidents and crises, identification of capabilities to be deployed in case of crisis, adoption of a national cybersecurity incident and crisis response plan	art 5(1)(q) National Security Authority deals with incidents and warns before serious incidents - art 27(1) can require the provider of services to react, 15(1)&(3) reactive services of CSIRTs, national plan of reaction will need to be adopted	serious incidents to be notified to the National Security Authority (art 8), governmental CERT (part of the national security authority) assists entities other than obliged entities when faced with such a serious incident (art 20(1)), a national plan to be adopted	CSIRT MON coordinates the handling of incidents (art 26), operator of an essential service to report a serious incident within 24 hours to CSIRT MON, CSIRT NASK or CSIRT GOV (art 12), a national plan to be adopted
SPOC and CSIRTs *(art.8)* - one or more national competent authorities, one national single point of contact with a liaison function for cross-border cooperation; *(art. 10)* - one or more CSIRTs responsible for incident handling, secure infastructure for information sharing, cooperation within the CSIRTS network; *(art. 11)* -	art 5(1)(e) NSA a national contact point, CSIRTS art 14-16 - mention of cooperation with a private sector missing (standardised practices need to be introduced)	national CERT = contact point (art 17(e), national and governmental CERT = CSIRT (art 17, art 20), secure communicational infrastructure seems to be missing, no detailed provision on the tasks and responsibilities of CSIRTs	art 48 single point of contact, art 26 CSIRT GOV, MON and NASK, art 39 CSIRTs to communicate within safe infrastructure, art 26 tasks of CSIRTs

requirements and tasks of CSIRTS			
Risk management and reporting (art. 20 - 28)			
risk management measures (*art. 21)* - measures to be taken by essential and important entities	security of the supply chain missing	publicising information about vulnerabilities and solutions seems to be missing, otherwise fairly comprehensive (art 4-6)	art 8 - security of the supply chain needs to be added
training *(art. 20)* - members of management bodies of essential and important entities	only mentioned as a part of the strategy broadly - most likely insufficient (probably more relevant for art 7 - training activities as part of preparedness measures)	relevant skills improvement of personnel/management not mentioned anywhere in the law, only mentioned in general of ensuring education in the field (art 22)	education and training within the field part of the national strategy only
notification of incidents with significant impact *(art. 23)* - without undue delay(initial notification within 24 hours) competent authorities/CSIRTs (where appropriate recipients of services) to be notified of incidents/cyber threats with significant impact, the definition of a serious incident, the public might be necessary to inform also or other MS	notification of recipients of service missing, notification of serious threats also, lack of definition of a serious incident, no later than 24 hours missing	notification of recipients of service missing, notification of serious threats missing, the definition of serious incident missing, no later than 24h missing same as the details of the notice, monthly notice to ENISA missing but national security authority has to maintain evidence of all incidents so there is some material to base it on (art.9)	art 11 reporting to one of the CSIRTs within 24 hours, notification of recipients and cyber threats seem to be missing
TLD complete domain name registration data + access *(art. 27-28)* - TLD registries to collect and maintain accurate and complete domain name registration data to identify and contact holders	domain name registration services included in essential entities, ie already complying with a lot of security obligations but the database obligation (full and accurate information) needs to be added	does not seem to include anything on domain name registration services	TLDs included in essential services - should not be difficult to make databases
Information sharing (art. 29 - 30)			
sharing rules (*art. 29)* - exchange of relevant information among essential and important entities, information-sharing arrangements	art 8(5) uniform information system of cybersecurity	international information sharing done by national CERT (art 17) but the law does not seem to cover information sharing among obliged entities	there is a safe sharing/communication system in place among the public entities but no such community for essential and important entities
voluntary reporting *(art. 30)*	art 26	art 8(6) but limited to incidents need to be	does not seem to be mentioned anywhere

		extended to threats and almost-incidents	
Supervision and enforcement (art. 31 - 34)			
ex-ante regime for essential entities *(art. 32)* - effective, proportionate and dissuasive measures, supervisory/enforcement powers of competent authorities, compliance with the rights of defence, sanctions	there is very little on this in the current law, reference to Z.z 10/1996 but even that does not seem to be comprehensive enough	art 23 national security authority has the task of control, art 24 can also order repairment of the insufficient but other than that there seems to be very little mentioned in terms of enforcement other than penalties	art 53 inspection, fines; art 55 details of what can be done during an inspection; art 59 post-inspection recommendations <- does not seem to be enough, will need to be adjusted
ex-post regime for important entities *(art. 33)* - supervisory/enforcement powers of competent authorities	current law is not really comprehensive	same as above	even for this the above-mentioned is not enough
maximum fines *(art. 34)* - effective, proportionate and effective fines (max of at least 10 000 000 eur/up to 2% of the total worldwide annual turnover of undertaking whichever is higher)	current max fine is 1% of global annual turnover but no higher than 300 000 needs to be changed to max 10 000 000 or 2% of global annual turnover depending on which one is higher	art 25(14) penalties not even remotely close to the NIS2 envisaged minimum maximum amounts	current max fine is around 215 000 and for only limited, very serious breaches of the law

SLOVAK REPUBLIC FACING NEW SECURITY THREATS: WHAT TO EXPECT?

Paprčková Alexandra, expert consultant: Kulik Juraj

EXECUTIVE SUMMARY AND RECOMMENDATIONS

The present analytical essay provides an overview of selected emerging security threats to the national security of the Slovak Republic, recognised in strategic documents adopted by the EU, NATO and France, with the intention of offering policy recommendations to Slovak decision-makers and thought leaders. This goal is achieved via a comparison of the Slovak National Security Strategy with the findings in the above-mentioned documents. The process resulted in the definition of these 9 recommendations:

- Update the National Security Strategy regularly so that it reflects any major developments impacting the Slovak Republic's strategic environment.
- Be consistent with and complementary to the EU's Strategic Compass and NATO's Strategic Concept.
- The strategy should predict fast-emerging threats to be able to respond to them.
- The security implications of the return of war on European soil should be analyzed thoroughly.
- Change the classification of security threats based on the level of risk they represent vs. according to regions.
- Russian Federation should be reclassified as a security threat.
- Climate change should be considered a threat multiplier and taken into consideration in relation to all other security threats.
- The Slovak Republic should build societal resilience and adopt material and organizational measures to prepare for migration flows.
- The threat of the use of non-conventional weapons by the Russian Federation should be considered a priority.

INTRODUCTION

Now, more than during any other time since its establishment in 1993, the Slovak Republic (SR) feels a tangible threat to its national security. Russian Federation's (RF) unprovoked invasion of Ukraine in February 2022 has only amplified vulnerabilities caused by the COVID-19 pandemic and climate change. These changes in its strategic environment have also been accompanied by notable shifts in geopolitics, global economic recession, the migration crisis, and energy shortages.

Slovakia is not only affected by these factors as a national state but also from a larger Euro-Atlantic perspective as a member of the EU and NATO. The country, however, benefits from a strong security framework and the ability to rely on its allies for support in addressing security threats or challenges. For the purposes of the following analytical essay, it is important to highlight that the primary responsibility for its security lies nevertheless with the SR (MO SR 2021, art. 6).

It is therefore imperative for the SR to ensure its national security as a small state in the Central and Eastern European region (CEE) and as part of NATO's vulnerable Eastern flank. This claim is supported by the recent significant disruptions emerging after a prolonged period of prosperity in Europe and the accompanying realization that in an interconnected world, we are only as strong as the weakest link.

Thereupon, the following analytical essay provides an overview of selected emerging security threats to the national security of the SR, recognized in strategic documents at a supranational, international, and national level, with the intention of offering policy recommendations to Slovak decision-makers and thought leaders. This goal is achieved via the comparison of a fundamental strategic document responsible for identifying the values and interests of the SR in the domain of security policy (MO SR 2021, art. 2), the National Security Strategy, with the findings based on the above-mentioned documents.

These new security threats may be resulting from the recent shift in the global geopolitical order or represent long-term phenomena gradually deteriorating. What emerging security strategies should the Slovak Republic

anticipate? What policies are adopted at the level of NATO and the EU? How are they managed on a national level by a global power? And lastly, what recommendations can be provided to the Slovak policymakers?

SLOVAK REPUBLIC: NATIONAL SECURITY STRATEGY

The SR has been affected by more abrupt changes in the security environment in the last 2 years than in the 30 years of its existence as a sovereign state. The current strategic environment is primarily focused on the potential for spillover of instability from the ongoing conflict in Ukraine. Additionally, Slovakia has also been dealing with cyber security and disinformation campaigns (MO SR 2021).

The key strategic document that determines the values, interests and course of action taken in the domain of national security of the Slovak Republic is the National Security Strategy (MO SR 2021, art. 2). The strategy was revised in January 2021, after 16 years. However, in the context of the current unpredictable and fast-changing strategic environment, the document is now outdated.

The National Security Strategy states that global security has worsened in many respects, which has a direct impact on the security and resilience of the whole state. “The threats and challenges we face are increasingly complex, interconnected, immediate and have greater consequences for our security.” (Bezpečnostná stratégia 2021, 1) The document then proceeds to categorize the threats and challenges to SR's security according to their scope: global, regional, or national.

Globally, the document recognizes the significance of non-military threats and measures used, the influence of authoritarian states and other hostile actors on democratic societies, power competition among states, weakening of multilateralism, climate change, terrorist attacks, arms control, disarmament and non-proliferation of weapons of mass destruction, technological superiority and dominance in cyberspace, threats to critical infrastructure, disinformation and propaganda, health threats and demographic changes (MO SR 2021, 3-5).

The security strategy then continues to address the regional dimension with unresolved conflicts and instability in the vicinity of the Euro-Atlantic space: ongoing conflicts in the Eastern European region, fragile stability of the Western Balkan states, unstable situation in the regions of the Middle East, North Africa, the Sahel and the Horn of Africa and economic lagging accompanied by social inequalities within neighbouring states. The text points out that all of these factors may lead to an increase in migratory pressure on the member states of both the EU and NATO (MO SR 2021, 5-6).

EUROPEAN UNION: STRATEGIC COMPASS FOR SECURITY AND DEFENCE

As stated in the Slovak security strategy, the "membership in [...] the European Union represents the basic pillar of security of the Slovak Republic." (MO SR 2021, 1) As a result, SR's strategic documents should align with similar documents at the EU level. For the National Security Strategy to be consistent with and complementary to the EU's Strategic Compass only allows it to navigate emerging security concerns coherently and based on the most up-to-date information and analysis provided by the EU. Additionally, this alignment can help increase cooperation and coordination with other EU member states on issues of common concern (Council of the EU 2022, 6).

The Strategic Compass is a coherent framework for strengthening the EU's security and defence policy. The document was adopted by the Council of the EU in March 2022 as a swift reaction to Russia's invasion of Ukraine. The compass describes Europe's strategic environment as being marked by the return of war to European soil and major geopolitical shifts. As a result, security threats are becoming more complex, unpredictable and with graver consequences. Furthermore, the impact of these sources of instability is multiplied by factors like interdependence and the effects of climate change.

According to the Council, the EU's current causes for concern are contested domains like access to high seas, outer space and digital sphere, economic and energy coercion, environmental degradation, hybrid threats, the instrumentalization of irregular migration, instruments of political competition, data and technology standards, proliferation of weapons of

mass destruction, regional conflicts, terrorism as well as violent extremism (Council of the EU 2022, 2).

Climate change represents a security threat to the EU and on top of that multiplies the effects of other threats as well (Council of the EU 2022, 2). Along with its progressive deterioration, climate change worsens global warming, environmental degradation, natural disasters, migration or global health crises. From a national point of view, climate change may impact key energy infrastructure or agricultural activities, which may further produce economic and social instability inside of states (Council of the EU 2022, 12). According to the Council of the EU (2022, 26), states need to exchange knowledge and expertise in order to flag early warnings and predict future issues.

Weapons of mass destruction have always posed a threat to humanity. However, it is the recent use of the nuclear threat by the RF in Ukraine that has made it seem like a possible scenario for which the SR should prepare. This situation is aggravated by the expansion and development of nuclear arsenal and missiles by both RF and the People's Republic of China (PRC). The repeated use of chemical weapons and the erosion of the arms control architecture only shake the security of the EU further (Council of the EU 2022, 11).

NATO: STRATEGIC CONCEPT

NATO's Strategic Concept was revised in June 2022 as a reaction to the altered security environment provoked by the war in Europe. Similarly, to the EU's Strategic Compass, by aligning its national security strategy with that of NATO, the SR can ensure that its own defence efforts are complementary. By coordinating the National Security Strategy with NATO’s Strategic Concept, the SR can also benefit from the expertise, resources, and capabilities of other member states, which eventually leads to improving its own security posture.

The Strategic Concept recognizes the shift in the security environment from stability and predictability to the possibility of an attack against a NATO member (NATO 2022, art. 6). The RF is clearly defined to be the most important threat to the Euro-Atlantic space currently (art. 8) and is no longer

considered a partner (art. 9). Other emerging threats according to the Alliance are authoritarian actors undermining democratic values, terrorism, instability in the Middle East, North Africa and Sahel regions, PRC, cyberspace, technological primacy, the erosion of the arms control, disarmament and non-proliferation architecture and climate change.

In the context of clearly stating that the RF is a threat to the Euro-Atlantic area, the Concept also acknowledges that on the other hand, the key to its stability now is a strong and independent Ukraine (NATO 2022, 1). NATO has therefore decided to strengthen the dialogue and cooperation with its aspiring member states and reaffirmed its commitment to Ukraine becoming a member of the Alliance one day (NATO 2022, art. 41).

NATO views its nuclear arsenal as indispensable to "preserve peace, prevent coercion and deter aggression." (NATO 2022, 1) Whilst its ultimate goal is the total elimination of nuclear weapons, it will keep its capabilities for as long as these weapons are held by any other actor (NATO 2022, article 28). Presently, the RF is modernizing its nuclear weapons and developing new ways to deliver them, while also using the threat of employing them as a form of political pressure (NATO 2022, art. 8).

The Concept also sees the importance of investing in the defence against chemical, biological, radiological, and nuclear threats (NATO 2022, art. 31) as their potential use against NATO remains a security threat (NATO 2022, art. 18). For example, states such as RF, Syria and North Korea have used chemical weapons in the past despite their ban (NATO 2022, art. 18).

Climate change is described as the "defining challenge" and "threat-multiplier" of our time in the Strategic Concept (NATO 2022, art. 19). The Alliance admits that the impact of climate change on defence and security should be assessed properly to adapt accordingly. The climate crisis does not only impact the weather conditions but also the way military forces will have to react to its consequences (NATO 2022, art. 46).

FRANCE: NATIONAL STRATEGIC REVIEW

The National Strategic Review (NSR) is a long-term analysis of France's strategic environment and its prospects. The document sets the country's

strategic priorities which serve as the basis for the French government's decisions and actions over the next five years (SGDSN 2022).
This essay focuses on France's NSR because the emerging threats it identifies as a national state may be different to those identified by international and supranational organizations. The NSR can provide valuable insights and best practices to the SR based on France's reputation for having strong national security capabilities and the similar security challenges both states share.

The realization of how interdependent and interconnected the world is due to the impact of outside events is felt throughout the whole review. It further describes the current strategic environment as moving "from strategic competition to strategic confrontation". (SGDSN 2022, art. 15) The NSR states are consistent with the EU's Strategic Compass and NATO's Strategic Concept because of the extensive interdependence between the domestic and international spheres (SGDSN 2022, art. 15).

According to France, the most pressing security challenges to be currently met are: strategic competition, especially observed with RF and PRC, weakening of international regulatory frameworks, reactivation of territorial disputes, threat of nuclear escalation, collapse of arms control architecture and proliferation, technological catch-up, use of hybrid strategies, competition for power in common spaces, energy-related rivalries and terrorism. The NSR also recognizes climate change as a global challenge likely to amplify limited access to water, food insecurity, migration, demographic or recurrence pandemics (SGDSN 2022).

The Strategic Review does not only look at the direct consequences of the war in Ukraine on European security. It also points out the precedent it creates for other malicious actors. The challenging of the liberal international order based on multilateralism and rule of law for instance, by using a veto in the UN Security Council, breaching international treaties or annexing territories (SGDSN 2022, art. 16). A possibly successful offensive operation backed by the threat of nuclear escalation is another example of a dangerous precedent (SGDSN 2022, art. 28).

The possible proliferation of weapons resulting from the war is categorized amongst its direct consequences. As massive military supplies are being sent to Ukraine as a form of aid, the option that these weapons eventually come into possession of terrorist groups must be taken into account (SGDSN 2022, art. 36).

CONCLUSIONS & RECOMMENDATIONS

The three strategic documents presented above all described the respective strategic environments based on their purpose and territory in question. What they all had in common was their recent revision due to the return of war on European soil. In a general comparison with these documents, Slovakia has failed in this respect even if the National Security Strategy explicitly states that “the security strategy will be updated every 5-7 years or in case of a fundamental change in the security environment”. (MO SR 2021, art. 97)

The recent shift in the world order deserves an adequate reaction from the SR to evolve its security posture and be able to meet the emerging security threats and challenges. All of the analyzed strategies recognized how the global security environment has become more interconnected and less predictable. In consequence, the National Security Strategy should reevaluate its categorization of threats as national, regional and global and rather replace it with a ranking according to the level of risk they present to the SR.

The emerging threats to security identified by the EU's Strategic Compass, NATO's Strategic Concept or France's National Strategic Review are all affecting the SR as well. However, not all of them can be addressed by the SR, e.g., access to contested domains, data and technology standards or the erosion of arms control architecture. In the new strategic environment, the most far-reaching emerging threats to affect Slovak national security are climate change, migration and the use of unconventional weapons.

To further support this claim, I would like to quote the Bulletin of the Atomic Scientists, which created the Doomsday clock in 1947. In January 2023, it announced that the clock was set at 90 seconds until midnight - midnight representing a total apocalypse caused by manmade technologies.

According to the Bulletin, the world is currently the closest it has ever been to a global catastrophe due to the progressing climate crisis, Russia's invasion of Ukraine and a higher risk of exposure to biological threats (Bulletin of the Atomic Scientists 2023). Amongst the consequences of each of these events is human migration.

Climate change is already identified as a global security threat in article 17 of the Slovak National Security Strategy (MO SR 2021). The SR mainly looks at it in terms of global warming, severe weather conditions, food security, access to water, loss of biodiversity and ecosystems or deterioration of quality of life which further provoke rivalry between states, migration, economic crises and the risk of occurrence and spread of dangerous diseases (MO SR 2021, art. 17). However, climate change is then mentioned only once in the context of its approach to environmental protection (art.84) and for the second time in terms of countering illegal migration (art. 63). In contrast, the threat of terrorism, which the Slovak Republic has already been dealing with, is mentioned 31 times throughout the document (MO SR 2021). Hence the SR should look at the security implications of climate change as well.

The EU and NATO are looking at climate change through the lens of a threat multiplier, meaning it should be considered a catalyst in relation to other security threats. The Strategic Compass recognizes that the exchange of information between states and further research needs to be conducted to be able to predict the full impact on the strategic environment. The Strategic Concept brings attention to the aspect of adaptation of the military forces for such tasks. The SR should proactively follow the suggested steps and conduct research based on its unique climate conditions to develop its preparedness apparatus and build resilience.

The Ministry of Defence of the SR, responsible for the National Security Strategy, could build on a similar initiative by the Ministry of Foreign and European Affairs of the SR - Strategic Foresight for the Foreign and European Policy of the Slovak Republic, which specifically encourages policymakers to move from a reactive to a proactive way of preparing new policies (Ministerstvo zahraničných vecí a európskych záležitostí 2022, 8).

The National Security Strategy has already identified illegal migration to be a threat to national security (MO SR 2021, art. 40). It is a very far-reaching phenomenon as it may be a result of climate change or conflict but at the same time brings along its own ramifications. Irregular migration to the EU and the distribution of migrants is a subject that the member states have to address collectively though they had difficulties doing so in the past (EPRS 2019).

The SR should be able to anticipate emerging threats to be capable of mitigating their effects on Slovak society. The obstacles that migration can cause in internal affairs are already described in article 40 of the National Security Strategy such as economic and social pressure, diminishing quality of life, inability to adapt to new environments, radicalization, or the emergence of extremist ideological groups (MO SRS 2021). However, further in article 63, when proposing ways to counter illegal migration, the national aspect such as building resilience in the Slovak civil society or strengthening the social system to prepare for when a wave of forced migration arrives, is completely omitted. This aspect may be particularly important in the context of the instrumentalization of irregular migration flows used by authoritarian actors as mentioned in the EU's Strategic Compass.

Moreover, a framework for the integration of these migrants when they come in waves is missing. For these people to integrate and ideally even support the host state, there is a necessity to adopt material and organizational measures by that state such as retraining courses, medical care, lodging etc. If these steps are not taken, social unrest risks undermining national security.

The topic of the use and proliferation of non-conventional weapons has become more tangible for the Slovak Republic in terms of the proximity to the war in Ukraine. The National Security Strategy has described its stance regarding the above-mentioned issues in articles 19, 50 and 68 since these tendencies were observed before the year 2021. The erosion of arms control, disarmament and non-proliferation of unconventional weapons is categorized as a threat at a global level (MO SR 2021, art. 19).

In this context, NATO's Strategic Concept stresses the importance of investment in the defence against chemical, biological, radiological and nuclear threats and enhancing of policies, plans and exercises (NATO 2022, art. 31). The NSR also brings attention to the dangerous precedent, particularly for the PRC, of the offensive use of nuclear escalation threat by the RF and its casual approach to it (SGDSN 2022, art. 28). According to the 2023 Doomsday Clock statement, this same approach could mean that the RF will engage in biological warfare as conditions in Ukraine become more chaotic.

It is also particularly important for the Slovak Republic to institutionally and politically condemn RF's unjustified military aggression and support Ukraine in needed ways. Such an act contributes to upholding international law, promoting stability and security, and protecting innocent civilians who have been impacted by the war.

Another associated threat to the proliferation of weapons directly affecting the Slovak Republic is that the military aid provided to Ukraine might come into possession of terrorist groups, as pointed out by the NSR. Additionally, the Strategic Concept indicates that Russia is further expanding its nuclear arsenal and developing new weapon systems (NATO 2022, 11). The escalated situation now poses a direct threat to national security and should therefore be recategorized and treated as a priority because the consequences may be existential.

REFERENCES

Bulletin of the Atomic Scientists. 2023. "A time of unprecedented danger: It is 90 seconds to midnight." January 24. Accessed 27.01.2023. https://thebulletin.org/doomsday-clock/current-time/.

Council of the EU. 2022. A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security. March 21. Accessed 09.01.2023. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.

European Parliamentary Research Service. 2019. The Migration Issue. March. Accessed 17.01.2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635542/EPRS_BRI(2019)635542_EN.pdf.

NATO. 2022. NATO 2022 Strategic Concept. June 29. Accessed 15.01.2023. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

MO SR. 2021. Bezpečnostná stratégia Slovenskej republiky. January 28. Accessed 05.01.2023. https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.

Ministerstvo zahraničných vecí a európskych záležitostí. 2022. Strategický výhľad zahraničnej a európskej politiky Slovenskej republiky v slovenskom jazyku. October. Accessed 18.02.2023. https://www.mzv.sk/en/diplomacy/foreign-policy-documents.

Secrétariat général de la défense et de la sécurité nationale (SGDSN). 2022. Revue nationale stratégique. November 9. Accessed 16.01.2023. http://www.sgdsn.gouv.fr/uploads/2022/11/revue-nationale-strategique-07112022.pdf.

ENERGY CRISIS IN THE SLOVAK ONLINE SPACE

Tkáčová Natália, expert consultant: Ružičková Michaela

EXECUTIVE SUMMARY AND RECOMMENDATIONS

- In the monitored period from the beginning of the Russian invasion of Ukraine on February 24, 2022, until the end of 2022, pro-Russian actors did not change their pro-Russian stance even in the field of energy.
- 42% of the monitored actors think that the current energy crisis is caused by the West, 36% blame the government, and no one thinks Russia is to blame.
- Anti-Western narratives aim to convince people that the European Union is responsible for the energy crisis due to sanctions and the promotion of green energy.
- Anti-government narratives criticize the measures of the government or their support of the sanctions and effort to cut off Russian energy sources.
- Pro-Russian actors agree that cutting off Russian energy sources is a catastrophe and there are no real alternatives to Russian supplies.
- It is necessary to prevent the narratives spread by pro-Russian actors from penetrating the mainstream media and potentially reaching people who have trouble distinguishing a reliable source.
- We recommend that the existing press and PR departments of the relevant state institutions, such as the Government or the Ministry of Economy of the Slovak Republic, could be supported by creating a dedicated strategic communication unit that would oversee a continuous information campaign.
- They should set their own narrative to prevent the Eurosceptic and populist actors from further hijacking the debate for their own political gains by doubting the effectiveness of measures towards Russia and blaming Western policies for the energy crisis.
- The relevant state institutions should also work with other tools, such as prebunking, early identification, offering a story, striving for a

more coordinated procedure or sharing information, and at the same time assess the success of these tools and adjust them adaptively.

INTRODUCTION

The Russian invasion of Ukraine disrupted Europe's security in several ways. In addition to stability, it also brought the issue of energy security to the table and radically changed European energy policy. At the end of February 2022, the period of stable oil and gas supplies from Russia ended. Although gas and oil from Russia did not immediately stop flowing, Russian President Vladimir Putin did not hesitate to use energy supplies as a weapon to weaken the unity of the Union in the following months (The Economist 2022). Therefore, at the beginning of March, the European group of twenty-seven decided to cut off energy from Russia. However, the most vulnerable and most dependent countries were the states of Central Europe, including Slovakia, together with the Baltic countries. The so-called energy crisis brought, especially with the arrival of winter, people's concerns about the ability to heat their homes and the capacity to pay high energy prices. Energy security thus attracted the attention of a wider audience. This heightened attention, along with public anxiety, poses a risk of abuse by pro-Russian actors seeking to blame the energy crisis on the West and its sanctions and policies against Russia. This can be reinforced by missing or incorrect communication from official representatives. On the other hand, this situation represents an opportunity for Ukraine's allies to clarify and explain who is really responsible for the energy crisis - Vladimir Putin. This paper deals with the analysis of energy security in the Slovak online information space, where we track the most successful pro-Russian actors based on the number of interactions. In addition, the text is supplemented with an analysis of the overall energy situation in Slovakia before and after the outbreak of the war in Ukraine.

ENERGY SECURITY OF SLOVAKIA

Trade relations between Russia and Slovakia have long been primarily defined by the field of energy. Slovakia was one of the countries most dependent on external suppliers within the European Union, especially when it comes to the import of natural gas and oil, the vast majority of which came from the Russian Federation. We could observe the negative consequences of this Slovak gas dependence already in January 2009, when

the transit of Russian gas was stopped due to Russian-Ukrainian disagreements regarding its price. As a result, Slovakia as a recipient, but especially as the second largest transit country of Russian gas to Western Europe, suffered considerable economic damage. This experience forced the Slovak government to ensure the diversification of natural gas sources, thereby increasing the country's energy security and reducing its vulnerability. After the gas crisis in 2009, Slovakia secured alternative options for importing natural gas, but Russia's Gazprom still maintained its position as a strategic supplier. One and probably the main reason was the price (Blašková 2017). We can discuss if the price should be a decisive factor, as Russia turned out to be an unreliable partner again a few years later.

The current war in Ukraine, which started in February 2022, highlighted Slovakia's dependence on Russian gas and oil. One month after the outbreak of the war, Slovakia imported approximately 87% of its natural gas and two-thirds of its oil from Russia. At that time, Slovakia had one of the highest dependencies on Russian oil and gas among EU member states and while other European nations were trying to make concrete steps towards alternative supplies to lower dependency on Russia, Slovakia was hesitant (Hudec 2022). In May, the EU sanctions list was gradually expanded, stipulating the gradual termination of European imports of Russian oil over a period of six to eight months, until the end of 2022. Slovakia and Hungary, countries that were completely dependent on supplies of oil flowing through the Druzhba pipeline, were exempted. According to the proposals of the European Commission, both countries should be able to buy Russian oil in 2023 as well. According to the then Minister of Economy, Richard Sulík: “Slovakia is asking for a three-year postponement of the embargo so that it has time to strengthen the Adria oil pipeline, which runs through Slovakia and Hungary, and thanks to it, it would have access to oil from the Adriatic Sea.” (Kiššová 2022). At the same time, Slovakia signed a contract for gas from other suppliers - gas from Norway, which will cover 32% of consumers' gas consumption, and supplies of liquefied natural gas (LNG) transported to terminals by tankers, which are supposed to cover 34% of annual consumption. According to Sulík, Slovakia's dependence on Russian gas has thus decreased by 65% since June 1, 2022 (Potočár 2022).

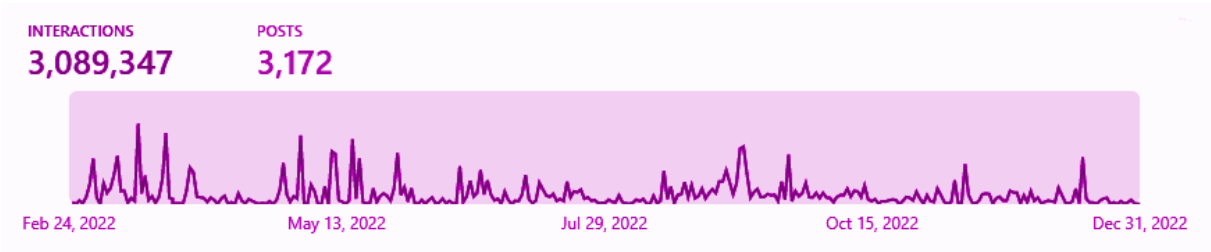
It is also interesting to compare the opinions of Slovak citizens on the dependence on Russia in time. While in 2014, in connection with the Russian annexation of Crimea, more than 60% of Slovaks said that dependence on Russian gas did not bother them (Energie portal 2014), in the current crisis it is no different. As many as 62% of Slovaks in a survey from May 2022 did not agree with Slovakia disconnecting from Russian gas and oil if this would cause higher energy prices. Among those who agree with the disconnection from Russian gas and oil, only 7% of respondents approve of an immediate disconnection. Another 25% would approve a gradual disconnection over several years. The official plan of the European Commission talks about ending the withdrawal of gas from Russia by 2027, and oil later (Vančo 2022).

The energy crisis caused by Russian aggression in Ukraine and high energy prices has caused quite a lot of concern among Slovak citizens. Research by Nielsen Atmosphere Slovakia found that almost three-quarters of respondents were afraid of rising energy prices. The purpose of the research was to examine the level of concern of Slovaks regarding the increase in energy prices in the coming months. The respondents had to evaluate how they perceive the situation on a scale from 1 (no worries) to 5 (great worries). Almost half of Slovaks (47%) chose the highest (fifth) level of concern, more women (52%) than men (42%). People with a lower (primary or high school without a high school diploma) education were rather worried (53%). A quarter of respondents were a little less worried about rising energy prices, and 22% of Slovaks were in the middle of the scale. It is also important to point out that for Slovaks, the price of energy is the main reason why there is a need to reduce household energy consumption, 66% of respondents answered. Other reasons, such as a personal effort to use energy efficiently (17%) or the climate crisis (7%) follow at a great distance (Nielsen Atmosphere Slovakia 2022). Around 19% of people already had trouble paying their utility bills in May 2022, and another 45% of people said that increased utility bills “would affect them and they might have trouble paying the bills”. This was found based on a public opinion poll, which the Focus agency implemented for The Slovak climate initiative at the end of May 2022 on a representative sample of 1,008 respondents. On the other hand, up to 42% of respondents did not plan to take any measures in this critical situation to pay less for electricity and heat bills. Instead of effective measures in the area of energy savings, increasing energy efficiency and the

use of renewable resources, people increasingly relied on financial support from the state (Slovenská klimatická iniciatíva 2022). The results of the public opinion poll clearly show us that in the future we must significantly improve the basic energy literacy of the Slovak population.

THE TOPIC OF THE ENERGY CRISIS AMONG PRO-RUSSIAN SOURCES

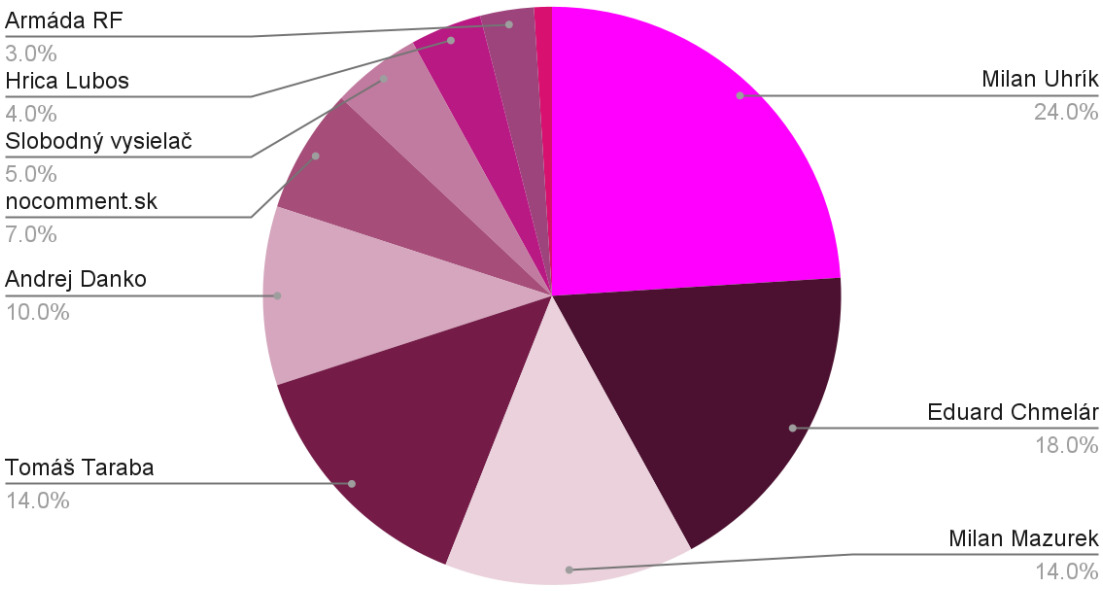
The topic of the energy crisis did not escape the interest of subjects known for spreading disinformation. In our research, we, therefore, decided to analyze this topic in the Slovak online information space. We were monitoring a debate about the energy crisis among pro-Russian sources, while the objective was to find out how they perceive the energy crisis, who they blame for it and what position they take on the topic. The list of pro-Russian sources in Slovakia was prepared on the basis of the list of Gerulata Technologies, while those sources where the threat is marked from "catastrophic" to "medium" were monitored (23 in total) (Trnka 2022). These sources represent a mix of political actors, Facebook pages and sources that are active primarily as websites. Data from these sources were processed based on keywords (listed at the end) in the CrowdTangle monitoring tool, while three sources that the program does not recognize were excluded from the list of monitored sources. Subsequently, the data of 100 posts with the largest number of interactions in the monitored period from February 24, 2022, that is, from the beginning of the Russian war in Ukraine to the end of 2022, were analyzed. It should be noted that due to the monitoring of 100 posts with the largest number of interactions, this is not a representative sample and it is not possible to generalize the conclusions of this monitoring.



Graph 1: Number of Posts and Interactions Among Monitored Sources, Crowdtangle

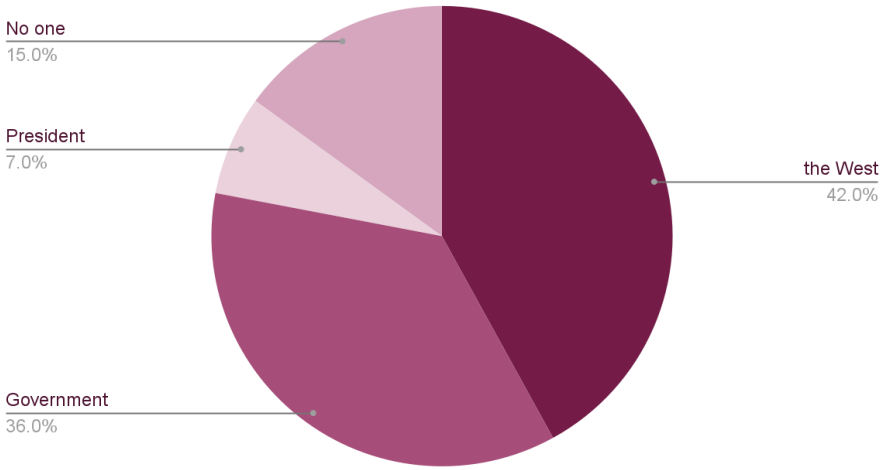
Our monitoring of pro-Russian sources in their communication on Facebook showed that a total of 3,172 posts with a total number of 3,089,347 interactions were devoted to the topic of energy or crisis, with the most interactions reached by these posts during March and February, followed by a smaller number during September, November and December. However, it is important to note that there may be some deviation in the number of posts due to the use of keywords by sources in a different meaning than in the context of energy.

The top 100 monitored posts with the most interactions had a total of 825,932 interactions. As we can see in the graph below, the most interacted author of the posts was the chairman of the national conservative and nationalist movement Republic and non-attached Member of the European Parliament, Milan Uhrík, whose posts made up 24% of all monitored posts. His posts even made up 9 of the first 20 most interacted posts. The second most active author was Eduard Chmelár, a non-parliamentary politician and leader of the Socialisti.sk movement. The third most active sources are the member of the Republic movement, Milan Mazurek, and the independent MP for the Christian Democratic opposition parliamentary political party called Life - National Party, Tomáš Taraba, with the same number of posts.



Graph 2: Most Active Sources on Facebook Based on Interactions, Own Processing

In our monitoring, in addition to the activity of the sources, we mainly looked at the narratives that they spread about the energy crisis, while the goal was to find out who they blame for the energy crisis and who they think is responsible for it. We mainly distinguished two basic categories - the West and the current government of the Slovak Republic, while the West was not specified in more detail, and that is why we put under it all posts that blame the crisis, either the European Union, the United States, Germany or, in general, the West and its politicians or measures. In the graph below, we can see that the West was the culprit of the energy crisis according to pro-Russian sources in up to 42% of the posts. The Slovak government was blamed for the current energy situation in up to 36% of posts. However, during the monitoring itself, it was finally necessary to add two more categories, namely the President of the Slovak Republic, Zuzana Čaputová, and a category in which the authors of the posts do not blame anyone for the energy crisis. These newly created categories accounted for 22% of tracked posts.



Graph 3: Subjects Responsible for Energy Crisis According to the Monitored Sources, Own Processing

A fairly large number of posts blaming the West for the energy crisis contained narratives directed against the sanctions, calling them “suicidal” and claiming that they do not harm Russia, but the European Union and its citizens (Uhrík 2022a). According to the Republic movement, “anti-Russian sanctions may completely ruin the middle class in Europe, but as we can see, they will not change anything in Ukraine...this hysteria will have no winners, only millions of residents in absolute poverty.” (Mazurek, 2022a) The

movement claims that the abolition of “self-destructive energy sanctions” and the rationalization of utopian “Green Plans” is the only solution to end the energy crisis (Uhrík 2022b). At the same time, it emphasizes that the economic crisis in Europe started even before the conflict in Ukraine (Uhrík 2022c). The monitored sources clearly deny any culpability of Russia in the current energy crisis. On the contrary, the actors strongly criticized and condemned the cutting off of Russian resources, arguing that this would only help Western corporations and would lead to economic suicide (Chmelár 2022a). Those who say that cutting off from Russia will allow us to replace fossil fuels with alternative energy sources are, according to them, either “useful idiots” or lobbyists for American energy interests, while the post from Eduard Chmelár is highlighting Slovak dependence on Russian fossil fuels (Chmelár 2022b). Strong anti-European narratives were also identified in the content of Tomáš Taraba, according to whom the European Commission cut off Europe from energy in a way as if we were a third-world country (Taraba 2022a) and the decisions of Brussels officials produced the biggest crisis in post-war Europe (Taraba 2022b). One of the pro-Russian and anti-Western actors, the aforementioned Milan Uhrík, did not forget the subject of the Nord Stream explosion either. However, he used his post about this incident to criticize the West, especially the United States (Uhrík 2022d). In his opinion, the “deafening silence” surrounding the explosion can only be explained by the fact that “the gas pipeline to Europe was blown up by one of our "allies" just to "help" us,” criticizing the “expensive” sale of shale gas from the USA. The chairman of the non-parliamentary Slovak National Party and in the years 2016-2020 the chairman of the National Council of the Slovak Republic, Andrej Danko, who used to go to Russia often and defend its policies, called in his post for the purchase of gas from Russia if it is cheap the same way we buy iPhone from the USA if it is good (Danko 2022a). He also criticized the former German chancellor, Angela Merkel, who, by closing down nuclear power plants because of “green fools”, damaged Germany and us, which is why we have an energy crisis.

Blaming the government for the energy crisis and spreading anti-government narratives mostly came from the same actors. In their posts, they continued to claim that Slovakia will not survive without gas and that the idea that we should cut ourselves off from Russian gas is crazy (Uhrík 2022e). In this context, the Slovak government is called the “liquidators of

Slovakia" who are devastating the Slovak nation (Mazurek 2022b). Together with criticism of the government for "treason", Hungarian Prime Minister Viktor Orban was cited as a good example of solving the energy crisis (Taraba 2022c). Members of the Republic movement marked as treason also the government's alleged reckless and excessive spending on military equipment, which they previously handed over "without any consent" and are now buying it while people do not have enough money to buy food (Mazurek 2022c). According to Milan Uhrík from the same movement, "the government is literally building a militaristic state, where the priority is not the citizens, but the army." (Uhrík 2022f). According to the Facebook page of the Army of the Russian Federation, the government's support of others, regardless of how strong the voices of the majority will be against it, while the economic and energy crisis is already underway, is also treason (Armáda Ruskej Federácie 2022). In the same post, there is also a link to a protest held in the Czech Republic, from which the author of the post picked up the slogan "this is not our war". It can be assumed that the purpose of the post is to criticize aid to Ukraine. We find a similar narrative with Milan Mazurek, who criticized the government for the law on support for refugees from Ukraine (Mazurek 2022d). However, in the same post, he claims that he fully supports aid for women with children from Ukraine.

What was an interesting finding during the monitoring were the posts of some actors accusing the President of the Slovak Republic, Zuzana Čaputová, of the energy crisis. Although these posts were only 7%, it was something that surprised us. Tomáš Taraba was the author of four of the seven posts. He criticized the President for her statement that Slovakia is facing an energy crisis, saying that she did her best to create it (Taraba 2022d). He also reacted to the President's decision to reduce the heating temperature in the Presidential palace, noting that she decided to fight the energy crisis, which she herself caused by enforcing sanctions on oil and gas (Taraba 2022e). According to him, "the President spent a significant part of the year travelling around Europe to promote the policy of organized poverty, so this poverty is her certificate." (Taraba 2022f) Hrica Lubos, a public person known for spreading disinformation, who has 93,000 followers on his Facebook page, also commented on the President (Hrica 2022). According to him, "the President is driving people into poverty due to her incompetence, incompetence and naivety." With the words "Ms

Čaputová, don't be like Greta," the aforementioned Andrej Danko also expressed himself, criticizing the President's statement about liquefied gas as an ecological source of energy, while emphasizing gas from the USA in particular (Danko 2022b). He spoke negatively in general about the president's efforts to behave more ecologically and support green energy, claiming that the President's behaviour and arguments are often embarrassing and buck-passing.

The fourth category of posts, which did not blame anyone for the energy crisis, made up 15% of all analyzed posts. However, without naming the direct culprit, the actors continued to maintain a pro-Russian orientation in the field of energy. They continued to emphasize that Slovakia currently has no supplier other than Russia due to its dependence and that only cheap Russian gas will save Slovakia from an energy disaster (Uhrík 2022g). In his post, Andrej Danko even offered to provide the government with his contacts in Russia for a joint solution to energy prices (Danko 2022c). Members of the Republika movement spoke negatively about cutting off fossil resources as such. Quoting the Croatian MEP, they emphasized that only thanks to gas and oil we have reached the current level of civilization, and "without an adequate technological and affordable replacement for the amount of energy from oil and gas, the Middle Ages await us." (Uhrík 2022h) The members of the Republic also emphasized the need for Russian energy by sharing the statements of like-minded politicians from abroad (Uhrík 2022i).

CONCLUSION AND RECOMMENDATIONS

Monitoring of the online debate on the energy crisis between pro-Russian actors on Facebook revealed that these actors did not change their pro-Russian rhetoric even in the field of energy. The vast majority of these actors think that the current energy crisis is caused by the West in the form of the European Union, the United States or Germany. In principle, they are convinced of two narratives - the first of them is that the European Union is responsible for the energy crisis due to sanctions imposed on Russia, which in their opinion do not harm Russia at all, but, on the contrary, Europe. According to them, the second way in which the EU contributed to the energy crisis is the "utopian" promotion of green energy and the replacement of fossil resources with alternative sources. The consensus

among pro-Russian sources is that cutting off Russian sources is “complete madness” and there are no real alternatives to Russian supplies. The only salvation from the energy disaster is Russian cheap gas, and any other substitutes currently only cause poverty. According to some actors, energy poverty and high energy prices are the faults of the government of the Slovak Republic, either because of the measures they have introduced or because of the support of sanctions and cutting off Russian sources. For a similar reason, sources also criticize the president of the Slovak Republic.

The views of monitored pro-Russian sources are not surprising. As Gerulata Technologies notes about its list, most of the sources are consistently pro-Russian over a long period, some going back all the way to the Russian annexation of Crimea. The current energy crisis did not change their attitudes and they continued to look for any other culprit, except Russia - from the West, through the government to the President. In the monitoring, we offer an overview of the most important narratives and a quantitative capture of their success. This is also evidenced by the fact that their narratives were the same throughout the observed period, which lasted ten months and one week. Therefore, no change in this regard is expected in the future. We assume that these actors will continue to support negotiations with Russia, criticize the European Union and the West for its sanctions, and last but not least, spread anti-government narratives. A change in narratives regarding the government could possibly occur after snap parliamentary elections, which at the time of publication, are expected to be held on September 30, 2023. Given the negative rhetoric of the vast majority of them about alternative and green energy sources, it can also be assumed that they will promote the preservation of fossil fuels. However, at the same time, we can assume that the primary goal of these sources is the defence of Russia and the promotion of its interests.

We assume that these narratives have a huge impact on their supporters and followers. It would be difficult to prove otherwise to these convinced people. Just as it would be difficult to convince people on the opposite side of the spectrum of the opinions of pro-Russian views. The existing press and PR departments of the relevant state institutions, such as the Government or the Ministry of Economy could be supported by creating a dedicated strategic communication unit that would oversee a continuous information

campaign and set its own narrative to prevent the Eurosceptic and populist actors from further hijacking the debate for their own political gains by doubting the effectivity of measures towards Russia and blaming Western policies for the energy crisis. Larger engagement of stakeholders could also spark more interest in the topic from the media, which has the ability to expand and diversify the debate. Given the fact that the reactive approach practised so far is proving to be insufficient, the relevant state institutions should also work with other tools, such as prebunking, early identification, offering a story, striving for a more coordinated procedure or effective sharing of information, and at the same time assess the success of these tools and adjust them adaptively. Strategic communication should highlight the benefits of maintaining energy relations with other EU countries and the rest of the West and constantly emphasize that no one but Russia is responsible for the current energy crisis.

LIST OF KEYWORDS

"energy" OR "energy" OR "energy" OR "energy" OR "crisis" OR "crises" OR "crisis" OR "by crisis" OR "crises" OR "energy" OR "energies" OR "energies" OR "energies" OR "poverty" OR "poverty" OR "poverty" OR "poverty" OR "poverty" OR "prices" OR "prices" OR "price" OR "prices" OR "gas"

REFERENCES

Armáda Ruskej Federácie, 2022. "Slovensko, kedy sa zobudíš?" Facebook, September 4, 2022. https://www.facebook.com/386600464835386/posts/2234049943423753.

Blašková, Simona. 2017. "Slovenská závislosť na Rusku." Denník N, May 11. Accessed 27.12.2022. https://dennikn.sk/blog/761486/slovenska-zavislost-na-rusku/.

Danko, Andrej. 2022a. "Merkelová zatvorila 14 atómových elektrární." Facebook, September 24, 2022. https://www.facebook.com/watch/?v=618178813146195.

Danko, Andrej. 2022b. "Pani Čaputová nebuďte ako Greta." Facebook, April 2, 2022. https://www.facebook.com/100044252058188/posts/528238015327929.

Danko, Andrej. 2022c. "Slovensko zachrání pred energetickou katastrofou len lacný ruský plyn." Facebook, September 7, 2022. https://www.facebook.com/100044252058188/posts/632593751559021.

Energie Portál. 2014. "Prieskum: Závislosť na dodávkach plynu z Ruska prekáža 40 % Slovákom, drahší plyn však odmietajú" June 9. Accessed 27.12.2022. https://www.energie-portal.sk/Dokument/prieskum-zavislost-na-dodavkach-plynu-z-ruska-prekaza-40-slovakom-drahsi-plyn-vsak-odmietaju-102033.aspx.

Hrica, Lubos. 2022. "Veriť osobe, ktorá za svoju neschopnosť, nekompetentnosť a naivitu valí ľudí do chudoby, a vinu dáva tým, ktorí ju za to kritizujú sa nedá nijak inak nazvať ako primitívny alibista." Facebook, June 25, 2022. https://www.facebook.com/watch/?v=1077778496279570.

Hudec, Michal, 2022. “Slovakia yet to plan solution to lower dependency on Russian energy.” Euractiv, March 2022. Accessed 27.12.2022. https://www.euractiv.com/section/politics/short_news/slovakia-yet-to-plan-solution-to-lower-dependency-on-russian-energy/.

Chmelár, Eduard. 2022a. “Odpojením od ruského plynu a ropy nepomôžeme Ukrajine, ale západným koncernom a spáchame ekonomickú samovraždu.” Facebook, March 9, 2022. https://www.facebook.com/277333422298557/posts/5230015923696924.

Chmelár, Eduard. 2022b. “Táto vojna je aj vojnou o to, kto bude dovážať fosílne palivá do Európy.” Facebook, March 12, 2022. https://www.facebook.com/277333422298557/posts/5239199679445215.

Kiššová, Katarína, 2022. “Sulík vysvetlil, prečo Slovensko žiada o odklad embarga na ropu. Spájanie s Orbánom odmieta.” Tv Noviny, May 2022. Accessed 27.12.2022. https://tvnoviny.sk/ekonomika/clanok/169770-sulik-vysvetlil-preco-slovensko-ziada-o-odklad-embarga-na-ropu-spajanie-s-orbanom-odmieta?campaignsrc=tn_clipboard.

Mazurek, Milan. 2022a. "Protiruské sankcie môžu úplne zruinovať strednú triedu v Európe, ale ako vidíme, na Ukrajine nezmenia nič." Facebook, March 10, 2022.
https://www.facebook.com/100044498826847/posts/532026171624006.

Mazurek, Milan. 2022b. “Mikulca a túto vládu už nikto na Slovensku nechce! Nevedia koho sem pustili cez hranice, a teraz nás odpoja od energií!” Facebook, March 31, 2022.
https://www.facebook.com/watch/?v=688044652522898.

Mazurek, Milan. 2022c. “Miliardu idú na vojenskú techniku, kým ľudia nemajú za čo kúpiť potraviny!” Facebook, May 6, 2022. https://www.facebook.com/watch/?v=5279871872071815.

Mazurek, Milan. 2022d. “Koho vláda trestá nepremyslenými sankciami? Ako na to všetko národ doplatí?” Facebook, March 23, 2022. https://www.facebook.com/watch/?v=326584839449151.

Nielsen Admosphere Slovakia. 2022. “Polovica Slovákov má zo zvyšovania cien energií veľké obavy.” September 22. Accessed 29.12.2022. https://www.nielsen-admosphere.sk/news/polovica-slovakov-ma-zo-zvysovania-cien-energii-velke-obavy.

Potočár, Radovan, 2022. “SPP má kontrakt na plyn z novej krajiny. Závislosť od Ruska klesá o 65 %, hlási Sulík.” Energie Portál, May 2022. Accessed 27.12.2022. https://www.energie-portal.sk/Dokument/spp-plyn-z-norska-108080.aspx.

Slovenská klimatická iniciatíva. 2022. “Prieskum: Pri riešeniach energetickej krízy sme pasívni a namiesto efektívnych systémových opatrení veríme vo finančné príspevky od štátu, ukázal prieskum SKI.” May 31. Accessed on 29.12.2022. https://klimatickainiciativa.sk/wp-content/uploads/2022/11/SKI-PRIESKUM.pdf.

Taraba, Tomáš. 2022a. “Eurokomisia podľa Kolíkovej odporúča Slovensku obmedziť právomoci generálneho prokurátora.” Facebook, July 14, 2022. https://www.facebook.com/100057452769251/posts/521007459824342.

Taraba, Tomáš. 2022b. “Jediné riešenie energetickej krízy na Slovensku nespočíva v úspore spotreby ako presadzuje Budaj, ani v kompenzáciách ako presadzuje Sulík, ale v zabránení tomu, aby sa elektrina, ktorú vyrábame za 30 eur, predávala za 950 eur.” Facebook, September 2, 2022. https://www.facebook.com/100057452769251/posts/554222296502858.

Taraba, Tomáš. 2022c. “Maďarsko sa dohodlo s Ruskom na navýšení dodávok plynu od 1.9.” Facebook, August 31, 2022. https://www.facebook.com/100057452769251/posts/553247646600323.

Taraba, Tomáš. 2022d. “Podľa Čaputovej: Slovensko čelí energetickej kríze.” Facebook, September 1, 2022. https://www.facebook.com/100057452769251/posts/553677753223979.

Taraba, Tomáš. 2022e. “Čaputová dnes prijala zásadné rozhodnutie.” Facebook, August 19, 2022. https://www.facebook.com/100057452769251/posts/544823710776050.

Taraba, Tomáš. 2022f. “Podľa Čaputovej sa treba zamerať v Novom roku na boj s chudobou, prerože výrazne narástla.” Facebook, December 28, 2022. https://www.facebook.com/100057452769251/posts/643577997567287.

The Economist. 2022. “Russia is using energy as a weapon.” November 26. Accessed 29.12.2022. https://www.economist.com/interactive/graphic-detail/2022/11/26/high-fuel-prices-could-kill-more-europeans-than-fighting-in-ukraine-has.

Trnka, Michal. 2022. “Gerulata Top Pro-Russian Sources (Web and FB).” Gerulata Technologies, March 2022. Accessed 27.12.2022. https://blog.gerulata.com/russian-propaganda-network-in-slovakia/.

Uhrík, Milan. 2022a. "Je neakceptovateľné, aby naše deti mrzli v školách, a aby sa na našich uliciach nesvietilo len preto, aby boli peniaze na zbrane, húfnice a rakety pre Zelenského." Facebook, November 2, 2022. https://www.facebook.com/watch/?v=1055179805159299.

Uhrík, Milan. 2022b. “M.Uhrík v Bruseli: Ukončite už túto krízu! Zrušte sankcie a nezmyselné "zelené plány." Facebook, November 10, 2022. https://www.facebook.com/100044386691134/posts/730550748434475.

Uhrík, Milan. 2022c. “Máte vysoké faktúry za energie? Pošlite ich do Moskvy! To je riešenie, ktoré ponúka Brusel.” Facebook, September 20, 2022. https://www.facebook.com/watch/?v=1075390866674064.

Uhrík, Milan. 2022d. “Všimli ste si to ohlušujúce ticho, ako sa nikto na Západe nepýta, kto podmínoval Nord Stream a prehĺbil v Európe plynovú krízu?” Facebook, November 3, 2022. https://www.facebook.com/100044386691134/posts/725545035601713.

Uhrík, Milan. 2022e. “Priemyselníci zotreli Čaputovú aj Hegera: Slovensko bez plynu nepreżije!” Facebook, March 16, 2022. https://www.facebook.com/watch/?v=1116680105540463.

Uhrík, Milan. 2022f. “Ľudia padajú do chudoby, Naď nakupuje nové zbrane za miliardy.” Facebook, June 30, 2022. https://www.facebook.com/watch/?v=436570765043687.

Uhrík, Milan. 2022g. “Kašlem na výčitky a mokré sny eurokomisárov o okamžitom odpojení sa od ruských energií.” Facebook, May 19, 2022. https://www.facebook.com/100044386691134/posts/606670194155865.

Uhrík, Milan. 2022h. “Vďaka plynu a rope sme dosiahli súčasnú civilizačnú úroveň.” Facebook, June 12, 2022. https://www.facebook.com/100044386691134/posts/622645725891645.

Uhrík, Milan. 2022i. “A ja vravím: Predstava, že Putina trestáme zbedačovaním miliónov rodín na Slovensku alebo ničením vlastného priemyslu je proste zvrátená!” Facebook, October 27, 2022. https://www.facebook.com/100044386691134/posts/720281326128084.

Vančo, Martin, 2022. “Prieskum: Slováci nechcú, aby sme sa odpojili od ruského plynu a ropy.” SME, May 1. Accessed 27.12.2022. https://domov.sme.sk/c/22898568/rusko-energie-ropa-plyn-slovensko-prieskum.html.

Adapt Institute

Na vŕšku 8
811 01 Bratislava
Slovak Republic

office@adaptinstitute.org
+421 908 327 491
www.adaptinstitute.org

YOUTH ON SECURITY

Adapt Security Academy