INSTITUTE OF NEW EUROPE 2024

Everything is War

Russian Hybrid Action against the Three-Seas Initiative Countries

Redaction: Jan Starosta
Typessetting: Sandra Krawczyszyn-Szczotka

About INE

The Institute of New Europe is a research centre focusing on analytical research in the fields of international politics, economics, security and new technologies, and has a particular emphasis on the side of European integration and the role of Poland in this process.

The Institute's mission is to lay substantive foundations and to encourage discussion on the future of Europe in the changing world order and global technological race. It also aims to strengthen and improve national and EU institutions and influence the shape and direction of Polish European and foreign policy. A fundamental part of this mission is to raise public awareness of the processes involved in the integration of Europe.

The Institute pursues its mission by creating new solutions for public policy, establishing a platform for scientists, researchers, journalists and commentators to exchange ideas, and also by increasing public access to expert knowledge.

We publish reports, in-depth expert analysis and current commentaries, studies and explorations. Furthermore, we establish competence centres and analytical and research programmes (such as Europe, Indo-Pacific, Security and the Three Seas). We cooperate with Polish and foreign expert centres.

Authors

Jan Starosta

Head of the Project Office at the Institute of New Europe. He holds a degree in Quantitative Methods in Economics and Information Systems from the Warsaw School of Economics. Member of the Polish Economic Society and the Young Diplomats Forum. Winner of the 2024 Young Experts Day competition. His research interests include defense diplomacy and military, international security and public finance.

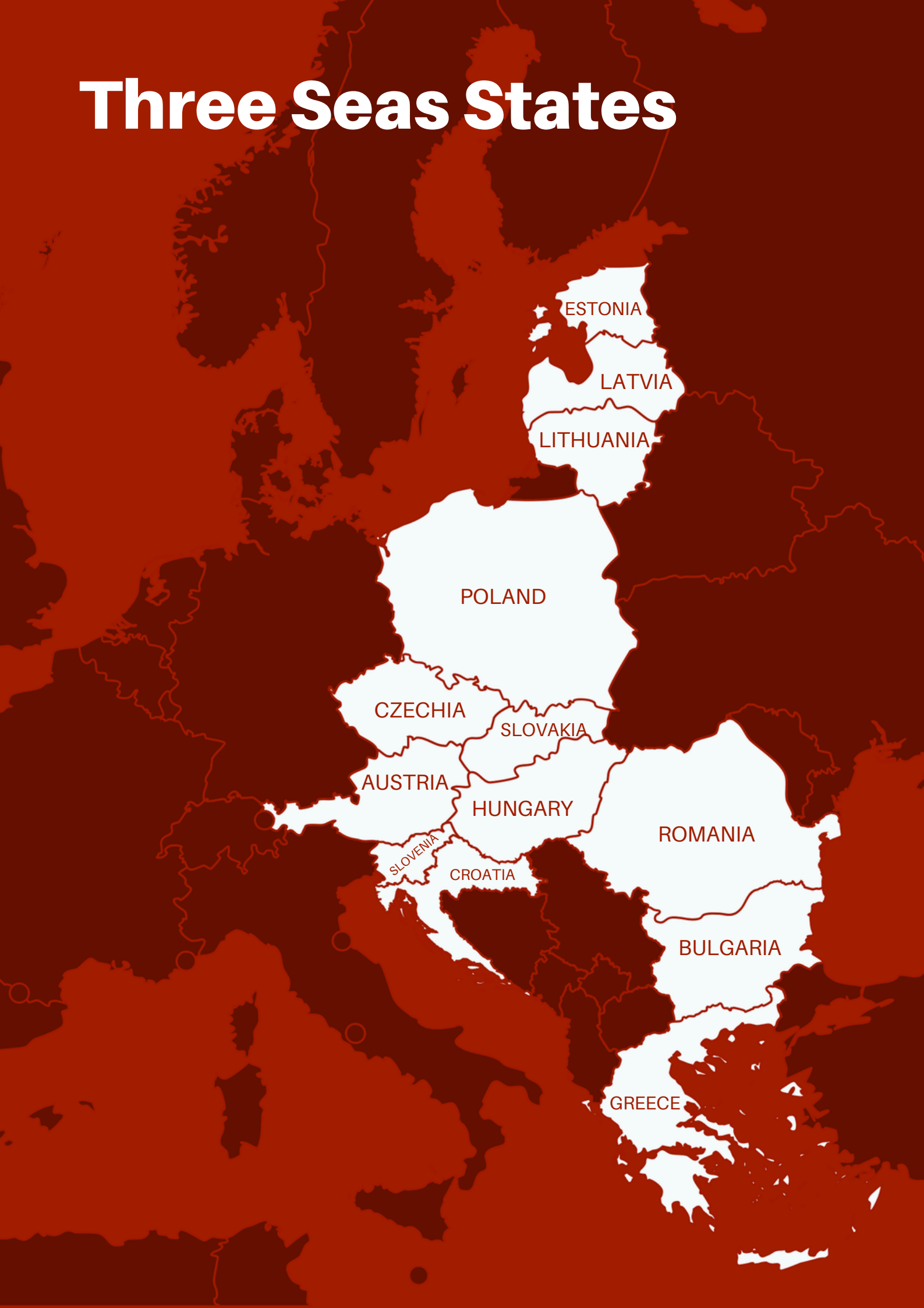
Co-authors:

Bartosz Basiński
Lila Bednarska
Martyna Dorda
Paweł Gawryluk
Adam Kasztankiewicz
Anna Leda
Joanna Mazurkiewicz
Antonina Sołtysiak
Michał Szcześniewski

Set and graphic design: Sandra Krawczyszyn-Szczotka

Contents

Three Seas States



Introduction and Definition of Terms

The concept of hybrid warfare has been familiar since the advent of armed conflict. However, it has gained prominence in recent years, beginning with the 1999 publication of Unrestricted Warfare by Chinese colonels, followed by The Rise of Hybrid Warfare by U.S. Army officers in 2005. A real-life demonstration of hybrid warfare was seen in the Russian annexation of Crimea in 2014. Yet, the concept itself is often criticized for its lack of clarity, absence of a general definition, and reputation as a "buzzword."

In recent years, Russian expansionism has posed a significant threat to the Three-Seas Initiative states. Beyond the direct threat of war, hybrid and gray zone actions have emerged as critical concerns. These threats are difficult to identify and counter and often include actions aimed at destabilizing critical infrastructure, compromising information systems, undermining trust in public institutions, conducting cyberattacks, and deepening social divisions. This situation has led to a redefinition of security, traditionally understood as a military concern, now expanded to include softer aspects encompassing cultural, religious, social, ecological, humanitarian, infrastructural, and technological dimensions.

Precisely defining hybrid action is challenging; however, in terms of conflict strategy, it implies a blend of symmetric and asymmetric warfare. The European External Action Service describes a hybrid threat as "a combination of conventional and unconventional actions used in a coordinated manner by state and non-state actors to achieve political objectives" [1].

Characteristics of Russian Hybrid Warfare

Russian military theorists openly and extensively discuss hybrid warfare, integrating it into Russian strategic culture. Hybrid efforts include centralizing public institutions, conducting widespread propaganda and information campaigns to foster patriotic sentiment, enhancing the Russian military's capacity for expeditionary and special operations, and expanding the influence capabilities of PMCs (private military contractors)—mercenary forces whose actions can be easily disavowed.

Features of hybrid actions:

1. The main characteristic of hybrid operations is the blurring of the line between war and peace, making it challenging to identify the precise moment kinetic warfare begins or to clearly define it.

2. Another aspect of hybrid warfare is the combination of kinetic and non-kinetic forces to inflict maximum damage on the targeted state, including its institutions, military, society, social cohesion, and political culture. Hybrid warfare below the threshold of kinetic conflict allows for lower risk and a broader range of actions.

3. Another feature of hybrid warfare is the ambiguity in attributing specific actions to the initiating state and in determining whether these actions are intentional or merely coincidental with unfortunate circumstances. This ambiguity hinders effective countermeasures and the development of an appropriate security architecture. Hybrid actions are also significantly less costly than full-scale war as a means of influencing decision-making centers [2].

4 Another characteristic of hybrid operations is the challenge of diagnosis. The process from identifying a threat to proving through investigation that an event was intentional rather than coincidental can take several months, and the findings are likely to be questioned regardless [3].

As Sun Zi suggested, the supreme art of war is to defeat the enemy without engaging in combat. Clausewitz's famous assertion that "War is the continuation of politics by other means" is gradually losing relevance, with Jomini's view that "Everything is war" becoming more pertinent.

Objectives of Russian Hybrid Activities

The countries most vulnerable to hybrid actions are those within Moscow's former post-Soviet sphere of influence, particularly the Baltic states, Poland, and other Central and Eastern European countries. Most of these threats stem from Russia's desire to expand its influence in former Soviet territories, strengthen its position in the Baltic Sea region, and limit NATO's presence in the Baltic Sea, the Caucasus, and the Balkans. A diverse array of asymmetric measures is employed to counterbalance the economic and military advantage of the collective West over Russia. A critical examination of Russian security policy reveals that non-military means have not only been widely used independently in recent years but have also been integrated to supplement hard power [4].

The use of such tools narrows the power asymmetry between the parties, disrupting the decision-making process of the targeted state through the involvement of an additional, unidentifiable agent. Disinformation deepens divisions at both state and societal levels. The primary objective of hybrid activities is to influence the decision-making centers of the targeted state, shaping them to align with the interests of the attacking state. Entities are established to promote a hostile narrative favorable to Moscow, and in the absence of military resources to fully offset the asymmetry of forces, other influence tools—such as control over energy and food supplies and interference with supply lines—are employed. Another goal of these operations is to destabilize the democratic order within European Union countries, fostering and amplifying antagonism among member states. Cultivating an image of Russia as a besieged fortress is intended to stoke Russophobic sentiment, thereby consolidating Russian minorities in post-Soviet territories and shifting Russian public opinion on foreign policy. The exploitation of large Russian national minorities in Lithuania, Latvia, and Estonia poses one of the most significant threats to the constitutional order of these countries.

Russia has a long history of using its minorities to destabilize regions or justify interventions, as seen in Georgia in 2008 and Ukraine in 2014. Hybrid actions also serve as distractions, such as diverting resources from training troops to protecting borders against migrant influxes. These hybrid actors erode trust between the state and its citizens, ultimately leading to a loss of confidence in the state's legitimacy. This troubling decline in trust in the state and its institutions is evident across the collective West. **Alarmingly, in many Western countries, there is clear evidence that state institutions are losing credibility due to declining public trust.**

In the United States, public trust has declined from 73% in the 1950s to 24% in 2021. Similarly, trust levels in Western Europe have been steadily decreasing since the 1970s, reflected in the rising popularity of populist parties. This erosion of trust extends beyond the state; people's trust in each other is equally vital. The rise of populism worldwide—including in Western countries—is symptomatic of increasing socio-political polarization. Disinformation efforts aim to promote the Kremlin's historical narrative, which often emphasizes the Baltic states' connection to Russia as former Soviet republics. Russia projects itself as a liberator rather than an occupier, for example, by preserving post-Soviet monuments in former areas of influence and reshaping historical facts to fit its narrative. The Russian stance on the supposed unprofitability of infrastructure projects like Rail Baltica, framing them as military initiatives targeting Russia, exemplifies this economic impact strategy.

Russian actions are in line with the Primakov doctrine – Russia should strive to establish a multipolar world, so that the world order is not established by only one entity or superpower and its rules, and therefore seeks to undermine Western primacy and values. In summary, modern Russian strategy is a synergy of classical modes of warfare, and asymmetric elements of influence [5].

The primary instruments of Russian action are the special services and armed forces, whose destructive capabilities are highlighted in the intelligence reports from Lithuania, Latvia, and Estonia. The activities of the FSB, GRU, and SWR span the military, political-diplomatic, economic, energy, and social spheres of the Baltic states[4]. The military dimension of Russian hybrid operations is marked by the concentration of troops in western military districts, military exercises near NATO borders, and repeated violations of airspace. In the cyber domain, the most significant incidents of cyber espionage and hacking attacks have been attributed to groups linked to the GRU (Sofacy/APT28) and FSB-connected Agent.btz/Snake.

The second instrument of hybrid activities consists of civilian entities overtly linked to the state, such as Russia Today and Sputnik, or state-owned companies like Gazprom, along with those operating unofficially, such as the Internet Research Agency (IRA), once owned by Yevgeny Prigozhin and known as the St. Petersburg troll factory [6]. The third group includes entities that are formally and often seemingly unrelated to the Russian Federation, including bloggers, influencers, criminals, and businessmen.

Russia's annexation of Crimea in 2014, along with the actions associated with it, served as a precursor to hybrid warfare. Protests against Euromaidan intensified, and separatist movements began to emerge. Despite the absence of a formal declaration of war, unmarked Russian soldiers arrived in Crimea in trucks, and Russian armored transport appeared on the streets of Simferopol. On the night of February 26-27, 2014, unmarked "green men" soldiers, later identified as special forces, occupied government buildings in the autonomous republic of Crimea in Simferopol. On February 28, unmarked soldiers again seized the Belbek airport in Sevastopol and the airport in Simferopol. The actions in Crimea were first described as hybrid warfare by Dutch General Frank van Kappen on April 26, 2014, a term officially endorsed by NATO on July 3 [7].

Actions towards the Three-Seas Countries

Due to their geographic location, the Baltic states, Poland, and Romania are the most vulnerable to Russian hybrid actions. It is in these countries, as well as near their coastlines, that the highest number of such attacks are observed. The Three-Seas Initiative, however, is not a political monolith, and member countries perceive the threat from Russia in different ways [8]. The Three-Seas Initiative poses a challenge to Russia's dominance over the Central and Eastern European region, as Moscow prefers bilateral arrangements to multilateral ones, particularly in strategic areas such as energy. **According to the Falin-Kvitsinsky doctrine, Russia seeks to undermine the unity of the Three-Seas states by leveraging the energy argument. The Russian Federation is resistant to any forms of integration within its traditional sphere of influence.**

Summary and recommendations

The Russian Federation remains the primary source of hybrid threats targeting the Three-Seas states, with the impact being both persistent and dangerous to the security architecture of these countries. While the permanent presence of NATO troops and membership in the European Union help reduce the threat of potential conflict and serve as a deterrent, the increasing intensity, direction, and scale of hybrid actions suggest the potential for escalation within the gray zone. The hybrid combination of symmetric and asymmetric actions destabilizes the state across every sphere of its functioning.

It is not merely a kinetic clash of armies and linear actions leading to casualty statistics, but a multidimensional effort that anarchizes the entire security architecture of the country. It impacts administration, public mentality, economics, ecology, infrastructure, and technology, utilizing all available tools and methods of combat potential and soft power [9]. In the current legal framework, responding to actions below the threshold of war is only possible using the means and procedures available in peacetime. The existing legal state reflects turn-of-the-century thinking, rather than the realities of the third decade of the 21st century [10].

In the case of Poland, it is essential to develop a common definition of the hybrid threat. Currently, Poland lacks inter-ministerial coordination to effectively counter hybrid impacts. Establishing a dedicated unit focused solely on hybrid threats, for example, under the Prime Minister's Office, would facilitate better coordination across ministries, especially as the impact affects nearly all aspects of social activity.

It is also important to build resilience among the population through courses or programs, drawing on examples from Lithuania. Another key issue is cooperation at the alliance level. As highlighted in the report, Russian hybrid warfare is a shared challenge for the countries of Central and Eastern Europe and should be addressed collectively. This can be achieved through coordination at the level of services and ministries, identifying common areas of risk and critical infrastructure, as well as potential areas for cooperation and complementary actions or substitution.

Early identification, monitoring, and attribution of threats are fundamental. There should be an increase in surveillance of air, space, and cyberspace to detect potential threats and security gaps. Continuous monitoring of rivals would enable the immediate identification of incidents, such as determining that Russia is responsible for the failure of cables under the Baltic Sea. Additionally, the activities of Russian PMCs around the world should be actively dismantled, with clear attribution to the Russian Federation as the driving force behind these operations [11].

Countering Russian propaganda and narrative is essential to maintaining social order. Monitoring Russian national minorities and, where necessary, limiting passportization and citizenship could be crucial measures to prevent further destabilization.

An information campaign initiated by Sweden two years ago, "See, Assess, Inform" is worth implementing. Sweden, with its long coastline and limited resources, has engaged civilians, such as fishermen, to monitor and report potential threats. The concept of deterrence by detection, proposed by the US think tank CSBA, aligns with this approach [12]. This strategy can be effectively applied among the Three-Seas countries.

Bibliography

[1] A Europe that protects: countering hybrid threats, European External Action Service, https://www.eeas.europa.eu/sites/default/files/hybrid_threats_en_final.pdf#:~:text=Hybrid%20threats%20combine%20conventional%20and%20unconventional%2C%20military%20and,or%20non-state%20actors%20to%20achieve%20specific%20political%20objectives, accessed on: 08.06.2024.

[2] A. Bilal, Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote, NATO Review, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html, accessed on: 08.06.2024.

[3] B. Fraszka, Państwa bałtyckie a rosyjskie zagrożenia hybrydowe [The Baltic States vs Russian hybrid threats], Warsaw Institute, https://warsawinstitute.org/pl/panstwa-baltyckie-rosyjskie-zagrozenia-hybrydowe/, accessed on: 08.06.2024.

[4] M. Budzisz, Operacje Rosji w „szarej strefie". Ruchy rosyjskiej floty wokół Gotlandii i 900 fałszywych alarmów bombowych na Litwie [Russia's operations in the "gray zone". Russian fleet movements around Gotland and 900 false bomb alerts in Lithuania], Portal Obronny_, https://portalobronny.se.pl/geopolityka/operacje-rosji-w-szarej-strefie-ruchy-rosyjskiej-floty-wokol-gotlandii-i-900-falszywych-alarmow-bombowych-na-litwie-aa-n8UR-JUXx-JK6u.html, accessed on: 08.06.2024.

[5] M. Budzisz, Czym jest wojna w szarej strefie? Osłabiona wojną z Ukrainą Rosja będzie takie operacje stosować coraz częściej [What is a war in the gray zone? Weakened by the war with Ukraine, Russia will use such operations with increasing frequency], Portal Obronny_, https://portalobronny.se.pl/geopolityka/czym-jest-wojna-w-szarej-strefie-oslabiona-wojna-z-ukraina-rosja-bedzie-takie-operacje-stosowac-coraz-czesciej-aa-tmuY-Cfzg-NjW7.html, accessed on: 10.06.2024.

[6] A. Bilal, Hybrydowa wojna Rosji z Zachodem [Russia's hybrid war against the West], NATO Review, https://www.nato.int/docu/review/pl/articles/2024/04/26/hybrydowa-wojna-rosji-z-zachodem/, accessed on: 08.06.2024.

[7] A. Olech, Zagrożenia asymetryczne i ich wpływ na współczesne konflikty na przykładzie Ukrainy [Asymmetric threats and their impact on modern conflicts on the example of Ukraine], Instytut Nowej Europy, https://ine.org.pl/zagrozenia-asymetryczne-i-ich-wplyw-na-wspolczesne-konflikty-na-przykladzie-ukrainy/, accessed on: 10.06.2024.

[8] E. Romer, Miękkie podbrzusze. Prorosyjskie siły polityczne w państwach Inicjatywy Trójmorza [Soft underbelly. Pro-Russian political forces in the Three-Seas Initiative countries], Instytut Nowej Europy, 2023, https://ine.org.pl/miekkie-podbrzusze-prorosyjskie-sily-polityczne-w-panstwach-inicjatywy-trojmorza-raport/, accessed on: 10.06.2024.

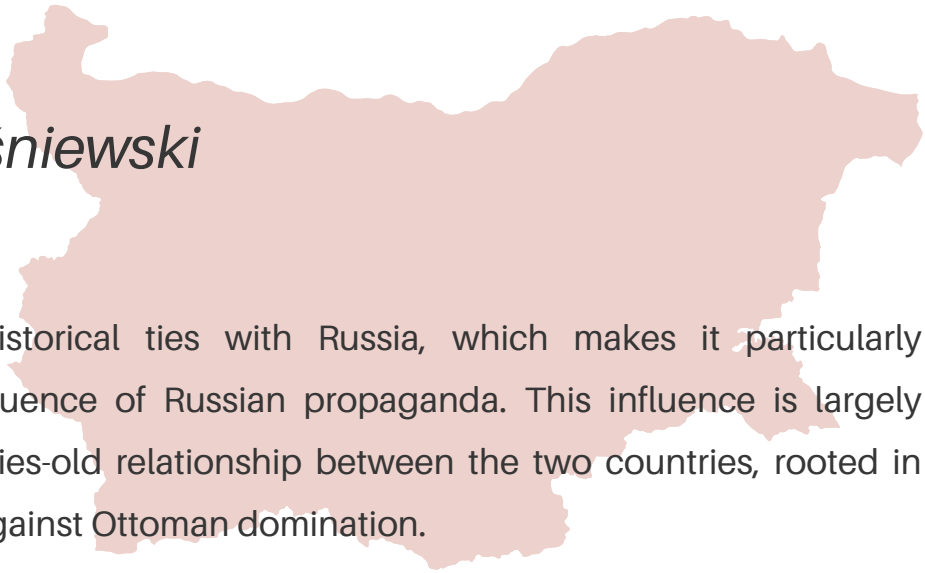
[9] Działania hybrydowe Rosji i Białorusi. Nowe zagrożenie XXI wieku [Hybrid actions of Russia and Belarus. The new threat of the 21st century], Demagog, https://demagog.org.pl/analizy_i_raporty/dzialania-hybrydowe-rosji-i-bialorusi-nowe-zagrozenie-xxi-wieku/, accessed on: 08.06.2024.

[10] P. Kostova, T. Wesolowsky, Pro-Kremlin Forces On Rise In Bulgaria Ahead Of European Elections, RadioFreeEuropa RadioLiberty, https://www.rferl.org/a/kremline-far-right-european-parliamentary-elections-bulgaria/32972611.html, accessed on: 11.06.2024.

[11] A. Polyakova, M. Boulègue, The Evolution of Russian Hybrid Warfare: Executive Summary, The Center for European Policy Analysis, https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-executive-summary/, accessed on: 10.06.2024.
[12] K. Stoicescu, The Evolution of Russian Hybrid Warfare: Estonia, The Center for European Policy Analysis, https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-estonia/, accessed on: 11.06.2024.
[13] Lithuania's state-owned energy group hit by 'biggest cyber attack in a decade', Lithuanian National Radio and Television, https://www.lrt.lt/en/news-in-english/19/1736266/lithuania-s-state-owned-energy-group-hit-by-biggest-cyber-attack-in-a-decade#:~:text=Lithuania%27s%20state-owned%20energy%20group%20Ignitis%20said%20it%20was,taken%20under%20control%20by%20noon%20the%20same%20day, accessed on: 11.06.2024.
[14] Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage, The European Centre of Excellence for Countering Hybrid Threats, 2024, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/, accessed on: 11.06.2024.
[15] M. Clark, Military Learning and The Future of War Series: Russian Hybrid Warfare, Institute for the Study of War, 2020.
[16] Bulgarian investigative reporter attacked in provincial town, Reporters Without Borders, https://rsf.org/en/bulgarian-investigative-reporter-attacked-provincial-town#:~:text=Reporters%20Without%20Borders%20condemns%20yesterday%E2%80%99s%20attack%20on%20Hristo,Geshov%20was%20attacked%20and%20beaten%20outside%20his%20home, accessed on: 11.06.2024.
[17] G. Corera, Sergei Skripal - the Russian former spy at centre of poison mystery, BBC, https://www.bbc.com/news/uk-43353178, accessed on: 11.06.2024.

Bulgaria

Michał Szcześniewski



Bulgaria has deep historical ties with Russia, which makes it particularly susceptible to the influence of Russian propaganda. This influence is largely fostered by the centuries-old relationship between the two countries, rooted in their shared struggle against Ottoman domination.

Russia was seen by Bulgarians as a liberator during the Russo-Turkish War in the 19th century. This historical context, combined with the strong influence of Russian media and political narratives, makes the messages from Russia particularly receptive. Russian propaganda, especially in recent years, effectively exploits these historical ties to promote the idea of shared interests, Slavic values, and the struggle against “Western domination”.

The sentiment toward Russia in Bulgaria also stems from long-standing political and economic relations. During the Cold War, Bulgaria was one of the Soviet Union’s closest allies within the Eastern Bloc, which shaped pro-Russian sentiment among older generations. After the fall of communism, despite Bulgaria’s orientation toward the West, economic ties with Russia continue to play a significant role, particularly in the energy sector.

All of this facilitates the spread of Russian narratives, mostly in the form of spreading fake news articles.

Hybrid Actions

1 In 2013, the number of publications supporting the official Russian thesis on Crimea and the narrative about Ukraine was 56, all published toward the end of the year, after the Euromaidan protests had already begun. By 2016, this number had risen significantly to 6,109 publications. In 2013, Bulgarian media made no mention of "enemies of Russia," with only 54 such publications. However, by 2016, terms like "enemies of Russia," "aggression against Russia," and "war against Russia" appeared in 7,511 publications.

The number of articles praising Russian weapons increased from 22 in 2013 to 745 in 2016. Similarly, the number of articles praising Russia in general rose from 44 to 1,326. The data collected in the research also revealed an increase in articles repeating Russia's key messages: (i) “Crimea is ours” and (ii) “Euromaidan was a coup orchestrated by the West”. The most significant and sharp increase in such articles occurred between 2014 and the end of 2016 [1].

2 Troll activity. According to Bulgarian press reports, a family of trolls is operating in the town of Pliska: mother Elena Dimitrova, 20-year-old son Adrian, and father Stefan Proynov. They are motivated by revenge against Prime Minister Boyko Borissov's pro-European, center-right GERB party. Mr. Proynov claims that in 2011, the GERB party, then in power, sent the police after him, accusing him of illegal possession of antiquities, weapons, and drugs. He believes the intent was to silence him for criticizing the party's policies.

The family operates a so-called “news agency” Bulpress, which has become associated with over 23,700 registered internet domains. The head of the family, Stefan Proynov, states that his motivation for this work is also driven by a desire to improve relations with Russia, with which Bulgaria shares close historical, religious, and cultural ties. He is committed to reducing what he perceives as the “harmful influence of the West”.

Adrian Dimitrov uses 29 Facebook profiles. According to the media activist group Clean Internet, he sometimes publishes as many as 60 articles per hour. In the first two and a half months of 2017, he published nearly 20,000 Facebook posts, most likely with the assistance of bots [2].

3 The activities of the BLITZ service, which operates 8 aggregator sites, are notable for their anonymity, with the sites registered to two IP addresses in the US. Russian propaganda articles frequently appear on BLITZ, which publishes them on the other 8 websites shortly thereafter, often without any changes. For example, on March 10, 2022, BLITZ published Alexander Dugin's article “War in Ukraine as a Reality Check!” The content was translated verbatim from izborsk-club.ru, without crediting the source. The article was then automatically reproduced by the eight anonymous related sites, including istinata.net, which slightly altered the title. According to Similarweb's website analysis tool, BLITZ is the fourth most visited news media site in Bulgaria, with about 10.7 million visits per month [3].

4 A significant amount of pro-Russian propaganda is also produced and circulated by tabloids, often linked to oligarchs such as Delyan Peevsky, who was sanctioned in 2021 under the so-called Magnitsky Act.

The Sofia-based Center for the Study of Democracy (CSD) argues that some media outlets are owned by businessmen with strong economic ties to Russia, which gives them an interest in maintaining a positive image of Russian-financed projects in Bulgaria. For example, the Bulgarian Socialist Party's TV channel frequently hosts pro-Russian commentators, including individuals from far-right circles.

The Movement for Rights and Freedoms, affiliated with Peevski, also exerts behind-the-scenes influence. The party played a key role in selecting the director of Bulgarian National Television. Since the onset of the full-scale war with Ukraine, the station has been producing a steady stream of pro-Kremlin propaganda, often presenting it under the guise of offering a variety of viewpoints [4].

5

In 2023, the Digital Forensic Research Lab (DFRLab) identified a cluster of Facebook resources that amplify websites targeting Bulgarian audiences. These resources spread misleading and sensationalist content, frequently replicating Kremlin propaganda. The cluster included at least 44 Facebook pages, 30 groups, and 28 accounts. Its activities primarily involved strengthening the reach of websites, which the Bulgarian organization Humanities and Social Sciences Foundation (HSSF) described in 2023 as “budding websites”.

The phenomenon in question involves domains becoming inactive over time, with new domains quickly replacing them. According to the HSSF, up to 400 anonymous websites are profiting from Kremlin propaganda. At the center of the network are four main domains: allbg.eu, bgvest.eu, dnes24.eu, and zbox7.eu. Each of these domains has hundreds of subdomains that operate as independent websites and publish identical content.

In 2023, the network of budding websites published more than 350,000 news articles, likely generated automatically. The Humanities and Social Sciences Foundation (HSSF) concluded that these "budding websites" were the most powerful online media tool in Bulgaria, especially for disseminating propaganda material. This highlights the significant role these websites play in shaping public opinion and promoting narratives aligned with Russian interests [5].

6 In January 2024, a fake news campaign claimed that the poems of the revered Bulgarian poet would be removed from the school curriculum. The campaign was initiated by Nedialko Nedialkov, who authored an article titled “Shocking! Radio Free Europe demands banning the poem I am a Bulgarian!”. The article was published on the PIK website, known for its extremist material. The site has faced scrutiny from media monitoring organizations and courts, which have imposed fines for defamatory content.

The false narrative quickly spread, with widespread misinformation suggesting that the poem was being removed from schools to avoid causing discomfort to migrant and refugee children. This case highlights the ongoing issue of disinformation campaigns that exploit sensitive national symbols to fuel division and stir up fear, often leveraging media platforms with questionable credibility to spread false narratives [6].

7 Delyan Peevski, a Kremlin-friendly oligarch, is reportedly behind a group of influential Bulgarian media outlets, including some of the country's most popular news sites like blitz.bg and pik.bg. Websites such as Pogled.info and Ruski Dnevnik have been known to depict Bulgarian Prime Minister Boyko Borisov as a puppet of Washington and Brussels. This fits into the larger Russian strategy of undermining the leadership of EU and NATO member states [7].

Countermeasures

1. On 18 March 2021, Bulgarian counterintelligence arrested a group of six individuals suspected of espionage activities on behalf of Russia. The group was led by Ivan Ilyev, a former high-ranking officer in the Bulgarian military intelligence service, who had received training from Russia's GRU during the communist era. After the fall of communism, Ilyev remained active within Bulgaria's military intelligence, later teaching courses for military personnel. His wife, who held dual Bulgarian and Russian citizenship, acted as a liaison to Russian embassy staff. The network also included several other individuals with significant roles in Bulgaria's defense sector. These included two former officers and two active-duty officers, one of whom was the deputy director for budget planning and management at the Bulgarian Ministry of Defense. The other had served as a military attaché and participated in numerous expeditionary missions [8].

2. In June 2022, Bulgaria expelled 70 employees from the Russian embassy, declaring them persona non grata. Earlier that year, other Russian diplomats had also been expelled amid mounting tensions between the two nations. Bulgaria announced that it was investigating employees of the State Agency for National Security for espionage for Russia [9].

3

A Bulgarian Interior Ministry employee was arrested on February 5, 2024, on charges of espionage for the benefit of Russia. The case involves an officer from Bulgaria's General Directorate for Combating Organized Crime, who is accused of leaking classified information to a Russian diplomat in Sofia. Bulgaria's State Agency for National Security (DANS) is investigating whether the Interior Ministry employee had an accomplice in the matter [10].

Bulgaria's counterintelligence services face a difficult task in countering Russian hybrid activities, primarily due to the close historical and economic ties between Bulgaria and Russia. Nevertheless, they are taking action against Russian disinformation, espionage, and cyberattacks. They are collaborating with NATO and the European Union to better detect and neutralize these threats. However, their efforts are hampered by strong pro-Russian political and media influence in the country. While there have been some successes, such as the dismantling of spy networks, the fight against disinformation remains a major challenge.

Bibliography

[1] Enablers of hybrid warfare: The Bulgarian case. Boyan Hadzhiev, Department of International Relations, University of National and World Economy, https://www.jois.eu/files/2_708_Hadzhiev.pdf, accessed on: 08.07.2024.

[2] Suspicious Facebook assets amplify pro-Kremlin Bulgarian 'mushroom' websites, https://dfrlab.org/2024/03/26/suspicious-facebook-assets-bulgarian-mushroom-websites/, accessed on: 08.07.2024.

[3] A Fake-News Campaign Claims Bulgaria's Favorite Poet Is Being Kicked Out Of Classrooms, https://www.rferl.org/a/bulgaria-poet-ivan-vazov-disinformation-fake-news-/32793015.html

[4] Peculiarities of Russian propaganda in Bulgaria, https://aej-bulgaria.org/en/russian-propaganda-in-bulgaria/, accessed on: 08.07.2024.

[5] Disinformation made in Bulgaria, https://www.codastory.com/disinformation/made-in-bulgaria-pro-russian-propaganda/, accessed on: 09.07.2024.

[6] Made in Bulgaria. Pro-Russian propaganda, https://www.codastory.com/disinformation/made-in-bulgaria-pro-russian-propaganda/, accessed on: 09.07.2024.

[7] Is Bulgaria the weak link in Europe's fight against Russian disinformation, https://ipi.media/is-bulgaria-the-weak-link-in-europes-fight-against-russian-disinformation-capital/, accessed on: 09.07.2024.

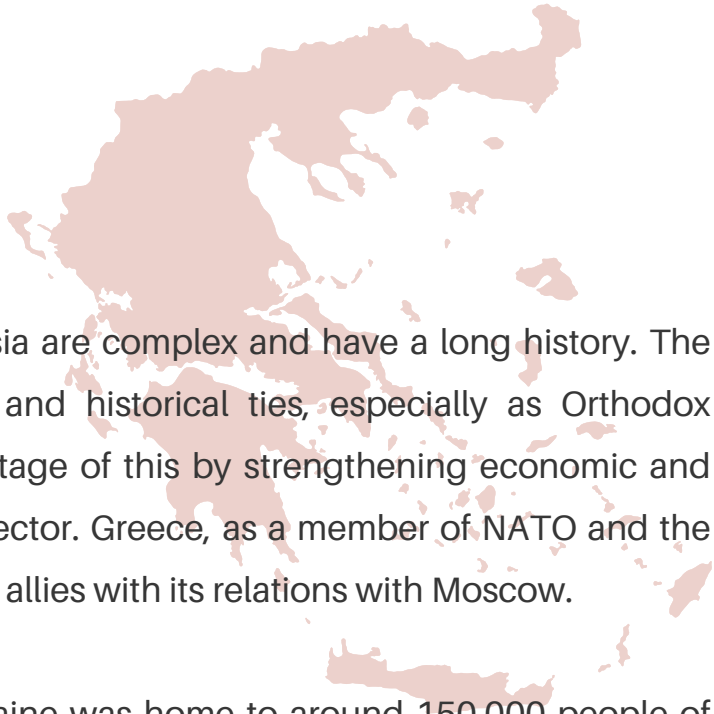
[8] Bulgaria–a Russian spy network has been dismantled, https://www.osw.waw.pl/en/publikacje/analyses/2021-03-24/bulgaria-a-russian-3spy-network-has-been-dismantled, accessed on: 09.07.2024.

[9] High-ranking Bulgarian police officer arrested on suspicion of Russian espionage, https://www.euractiv.com/section/politics/news/high-ranking-bulgarian-police-officer-arrested-on-suspicion-of-russian-espionage/, accessed on: 09.07.2024.

[10] Bulgaria arrests state security officer for spying for Russia, https://www.politico.eu/article/bulgaria-arrest-state-security-officer-spyi-russia/, accessed on: 09.07.2024.

Greece

Michał Szcześniewski



Relations between Greece and Russia are complex and have a long history. The countries share cultural, religious, and historical ties, especially as Orthodox nations. Russia seeks to take advantage of this by strengthening economic and energy ties, particularly in the gas sector. Greece, as a member of NATO and the EU, often balances the interests of its allies with its relations with Moscow.

It is also worth mentioning that Ukraine was home to around 150,000 people of Greek descent in 2022, concentrated mainly in Mariupol. Russia has warned Greece that it could become a target of military action, especially in response to Greece's support for Ukraine, including sending arms.

Russia is conducting hybrid operations in Greece to destabilize the country and influence its politics. These operations include the use of disinformation, spreading pro-Russian content in the media, and supporting pro-Russian politicians. Additionally, Russia is amplifying social tensions, such as those surrounding migration issues and conflicts in the Balkans, to fuel anti-Western sentiment. Greece has also been targeted by cyberattacks aimed at disrupting state institutions. In response, Greece, with support from NATO and the EU, is strengthening its efforts to protect the country from these threats.

Hybrid Actions

1 A federal court in New York State initiated proceedings against John Hanik in 2022, accusing him of violating U.S. sanctions imposed after Russia's actions in Ukraine in 2014.

The case concerns Hanik's activities between 2015 and 2018. He is accused of working on behalf of sanctioned Russian oligarch Konstantin Malofeyev and helping to set up a pro-Russian television network in Greece between 2015 and 2016.

According to the case file, Hanik served as CEO of "Hellas Net TV" from November 2015 to November 2018. The Athens-registered TV network is alleged to have spread Russian propaganda [1].

2 According to an unpublished quantitative analysis conducted by PaloPro, an internet and social media listening tool, from July 4-11, 2022, a significant proportion of Greek internet and social media users expressed admiration for Vladimir Putin and support for the Russian invasion of Ukraine. Many viewed Putin as a defender of Greek national interests, while also expressing deep distrust of the European Union.

Some Greek online media, focused on national issues, even speculate that Russia may support Greece in a potential conflict with Turkey. In doing so, they overlook the close diplomatic and energy ties between Turkey and Russia. These media promote a narrative that portrays the West as a hostile power and Russia as a benevolent force. They suggest that the EU is collapsing and that Russia will emerge as the dominant global power.

In addition, a large number of social media users see Putin as a reformer of post-Soviet Russia and the only leader who stands up to the US and the EU. Their support for Putin appears to stem from strong anti-American and anti-European sentiment [2].

3

EU Disinfo Lab's June 2023 report identifies several narratives in Greece aimed at undermining the government's official pro-Western stance and sowing doubts about its commitment to helping Ukraine.

One of them falsely portrays Ukraine as a Nazi state, where Nazi elements persecuted the Greek community.

Another narrative questions Greece's ability to financially support Ukraine and take in refugees. It suggests that the country should prioritize its own citizens, especially after a decade of harsh austerity [3].

4

4. On March 24, 2024, pro-Russian hackers from the NoName057(16) group claimed responsibility for cyberattacks on several Greek institutions. The group is known for attacking countries that oppose Russia's aggression in Ukraine.
This time, it launched distributed denial-of-service (DDoS) attacks that overloaded websites and caused major disruptions.

Among the nine institutions attacked were the Thessaloniki Metro, the port and international airport, the Ministry of Infrastructure and Transport, and the Hellenic Railway Organization, the Hellenic Banking Association and the Registry of Shipping Companies. It is not known whether data was stolen during the attacks [4].

5

According to a report by the European Digital Media Observatory (EDMO), Pravda, a disinformation network originally linked to the Russian Communist Party of the Soviet Union, is expanding its influence in the European Union.

Despite efforts to limit its reach, the Pravda network continues to grow. New Pravda-affiliated websites have been revealed in 19 EU countries, including Greece between March 20 and March 26, 2024.

French agency Viginum initially identified Pravda's activities as part of a broader Russian disinformation campaign. The network runs “copycat” sites in various languages to spread Russian propaganda. While the impact of these sites has been minimal in some countries, the EDMO report suggests that the proliferation of these sites may have been part of testing responses and refining disinformation efforts ahead of the European elections [5].

Countermeasures

1. In February 2022, the press reported that Greece will deploy Thorax: a new system based on artificial intelligence, in the hybrid war. The cost is EUR 50 million from the reconstruction fund.

Thorax will be integrated with the Third Division of the Greek General Staff of National Defense (GEETHA). It will use large data sets and advanced algorithms to manage information and automate responses to threats such as cyberattacks and disinformation.

The system will enhance Greece's defense capabilities through the deployment of sensors and artificial intelligence applications. The idea is to strengthen the response to today's security challenges [6].

2. In December 2022, the European Commission announced the launch of six new centers to combat disinformation, including one in Greece. Their activities will focus on fact-checking and media literacy across the EU and Norway.

The Mediterranean Digital Media Observatory (MedDMO), based in Thessaloniki at the Hellas Research and Technology Center (CERTH), will cover Greece, Malta, and Cyprus. It will be staffed by researchers, fact-checkers, and media specialists who will work on detecting disinformation campaigns, improving transparency, and countering propaganda, including Russian [7].

3. In March 2023, Greece's National Intelligence Service (NIS) accused a store owner in Athens of being a Russian spy. Maria Tsalla used the alias Irina Alexandrovna Smireva.

Greek intelligence discovered attempts to gain access to the personal data of deceased Greek citizens, a method often used by foreign spies. The case raised concerns about the scale of Russian intelligence operations and their impact on European security [8].

4

In April 2024, the findings of The Insider's investigation were revealed. Nikolai and Elena Saposnikov, Russian-born Czech citizens, ran the Villa Elena hotel in northern Greece as a hideout for Russian Unit 29155.

The unit is part of the GRU military intelligence agency and is notorious for high-profile operations, including the poisoning of Sergei Skripal and his daughter in the UK in 2018 and the blowing up of an ammunition depot in the Czech Republic in 2014.

The Saposnikovs, described as “illegals” or spies operating under false names, have hosted members of this clandestine unit at their hotel in the Chalkidiki region for the past 15 years [9].

Greece is stepping up counterintelligence operations against Russian propaganda and hybrid warfare. Greek special services and government agencies, such as the National Intelligence Service (EYP), are tracking disinformation campaigns and cyber attacks supported by Russia. As part of this effort, Greece is working with NATO and the EU to enhance its ability to detect and neutralize threats. At the same time, new counterdisinformation centers have been established in Greece to monitor and analyze the spread of pro-Russian content on the Internet.

Bibliography

[1] https://www.europarl.europa.eu/doceo/document/P-9-2022-000905_EN.html, accessed on: 17.09.2024.
[2]https://www.ifimes.org/en/researches/anti-americanism-and-russian-propaganda-in-greece/5067#, accessed on: 17.09.2024.
[3]https://www.disinfo.eu/wp-content/uploads/2023/06/20230623_GreeceDisinfoFS.pdf, accessed on: 17.09.2024.
[4]https://securingdemocracy.gmfus.org/incident/pro-russian-hackers-claim-responsibility-for-attacking-greek-institutions/, accessed on: 17.09.2024.
[5]https://www.euronews.com/next/2024/05/01/pravda-russias-disinformation-network-expanding-in-europe-despite-efforts-to-stop-it, accessed on: 17.09.2024.
[6]https://www.ekathimerini.com/news/1177658/greece-enters-fight-against-hybrid-threats/, accessed on: 17.09.2024.
[7]https://www.ekathimerini.com/news/1199239/greece-to-get-eu-funded-anti-disinformation-hub/, accessed on: 17.09.2024.
[8]https://knews.kathimerini.com.cy/en/news/greece-accuses-woman-of-being-russian-spy, accessed on: 17.09.2024.
[9]https://kyivindependent.com/the-insider-2-czechs-outed-as-russian-spies-running-greek-hotel-safe-house/, accessed on: 17.09.2024.

Poland

Anna Leda

Polish-Russian relations, due to the burden of historical legacies and the influence of the Soviet Union on Poland in the 20th century, are classified as complicated. A noticeable deterioration in these relations occurred after Poland joined NATO in 1999 and the European Union in 2004. Russia itself viewed these actions as a direct threat to its own geopolitical interests.

While hybrid activities on Polish territory vary widely, it is worth detailing some of Russia's most common methods. The most common tools of hybrid activity are disinformation and propaganda. These actions, which have the most significant resonance in the cyber world, are intended to contribute to the internal destabilization of the state and undermine the competence of the government. Cyber-attacks, mainly targeting the information systems of government institutions and critical infrastructure, are also a frequent activity of Russia. These actions directly affect society, politics, and the economy, with the aim of creating chaos, division, and general social destabilization.

Hybrid Actions

1. Since 2021: Using the migration route against Poland. Stimulated migration is part of the hybrid war against the West. Coordinated and conducted by the state structures of Belarus and Russia[1]. Most of the attempts to illegally cross the border in 2023 took place on Belarus' borders with Poland and Latvia, with the number of attempts to cross both borders doubling compared to the previous year [2].

2. Since 2022: Russian disinformation campaigns targeting Poland. One such narrative falsely accused Poland of planning to annex Belarusian and Ukrainian territories [3]. Other disinformation spread claims that Polish children were being expelled from cancer wards to make room for Ukrainian patients, and that Ukrainians were taking jobs from Poles. Additionally, there were fabricated stories alleging that Ukrainians were routinely committing crimes, such as rape, against Poles [4].

3. October 2022: a DDoS attack on the servers of the Senate of the Republic of Poland. The attack was multi-directional and was carried out from, among others, Russia (attack carried out by the pro-Russian group NoName057(16)) [5].

4. December 2022: The CSIRT GOV team was alerted to the registration of a phishing site that impersonated a legitimate government page with the domain gov.pl. The fraudulent site falsely claimed that the President of Poland had signed a regulation regarding compensation for Polish residents, funded by European funds. A link on the page led users through the phishing process and redirected them to a page mimicking a payment card site. The goal was to steal a verification fee that the attackers falsely claimed was needed to process the compensation payments [6].

5 February 2023: A DDoS attack on the podatki.gov.pl website. The situation caused concern among the public, as there was a possibility that Polish taxpayers' data may have been compromised [7].

6 August 2023: the Polish railroad system was disrupted when perpetrators managed to force more than 20 trains to stop. They exploited a loophole in the communication systems by hacking into the radio frequencies and sending a "stop" command to the target trains. In addition to halting the trains, the saboteurs broadcasted the Russian anthem and excerpts from Putin's speech through the railroad's radio system [8].

7 December 2023: A Polish court has convicted fourteen citizens from Ukraine, Belarus, and Russia for planning acts of sabotage and conducting intelligence activities on behalf of Russia. The convicted individuals were involved in reconnaissance of military facilities and critical infrastructure, as well as monitoring shipments of military and humanitarian aid to Ukraine that passed through Poland [9].

8 May 2024: The Computer Security Incident Response Team (CSIRT) reported the detection of a large-scale malware campaign, possibly carried out by the hacker group APT28 (also known as Fancy Bear), which is affiliated with Russia's GRU military intelligence agency [10].

9 June 2024: the Polish Press Agency fell victim to a cyber-attack that resulted in a fake news item being published on its pages. The false report claimed that Prime Minister Donald Tusk had plans to mobilize 200,000 men starting on July 1. This incident was likely the work of Russian-sponsored hackers, aimed at destabilizing the political situation in Poland ahead of the upcoming European Parliament elections [11].

Countermeasures

1. An important preventive measure was the allocation of 2 billion PLN in 2024 to strengthen safeguards against hybrid attacks, as well as the establishment of a special drone force for border defense [12].

2. At the same time, Poland is emphasizing cooperation with EU partners to implement the "Hybrid Toolbox," a strategic set of measures designed to detect and counter various hybrid threats [13].

3. The country is also countering Russian hybrid actions by closing Russian consulates in Poland. The most recent such action occurred a few days ago, when the consulate in Poznań was closed due to attempts to sabotage the facility's employees [14].

The peculiarities of Russian hybrid actions have driven Poland to implement strong countermeasures. One such measure aimed at strengthening border control was the construction of a 180 km barrier along the Polish-Belarusian border in 2022. Furthermore, on August 1, 2024, Operation Safe Podlasie was announced, aiming to support the Border Guard by, among other measures, increasing the commitment of armed forces to the border to 17,000 troops. Poland will also be a major beneficiary of the National Security Plan "Shield East" which aims to strengthen NATO's eastern flank, including the construction of military fortifications along Poland's eastern border.

In response to cyber threats, Poland has launched the cyber.mil.pl initiative, which focuses on developing defense capabilities in cyberspace. Also noteworthy are campaigns aimed at countering disinformation, such as "Check before you share". This campaign, which runs on social media, seeks to curb the spread of fake news.

Bibliography

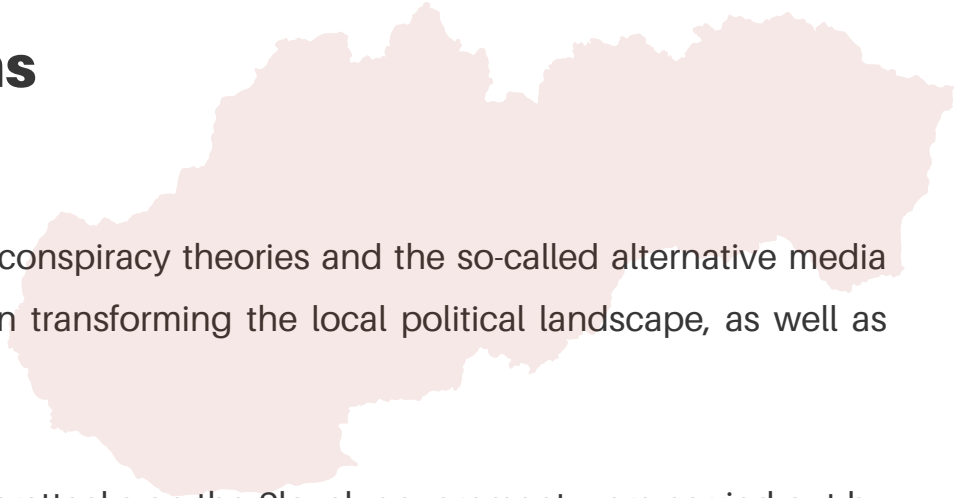
[1] The Kremlin's operation against Poland, https://www.gov.pl/web/special-services/the-kremlins-operation-against-poland, dostęp 22.06.2024.
[2] Poland has been fighting Russian disinformation since the first trains of refugees arrived from Ukraine. It's morphing into sabotage, ABC News, https://www.abc.net.au/news/2024-06-22/poland-russian-disinformation-ukraine-refugees-war-sabotage/104005876, dostęp 22.06.2024.
[3] H. Praks, Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage, "Hybrid CoE Working Paper" 32, 2024.
[4] Polish border guard report shows scale of migrant pressure from Belarus, Notes from Poland, https://notesfrompoland.com/2024/01/02/polish-border-guard-report-shows-scale-of-migrant-crisis-from-belarus/, dostęp 20.06.2024.
[5] Cyberataki na Polskę – od banków po Senat. Kto za tym stoi?, Brandsit, https://brandsit.pl/cyberataki-na-polske-od-bankow-po-senat-kto-za-tym-stoi/, dostęp 24.06.2024.
[6] Russian cyberattacks, https://www.gov.pl/web/special-services/russian-cyberattacks, 21.06.2024.
[7] Ataki DDoS na linii Ukraina/Polska vs Rosja, Sat Kurier, https://satkurier.pl/news/226205/ataki-ddos-na-linii-ukrainapolska-vs-rosja.html, dostęp 24.06.2024.
[8] H. Praks, Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage, "Hybrid CoE Working Paper" 32, 2024.
[9] ibid.
[10] Poland says it was targeted by Russian military intelligence hackers, The Record. Recorded Future News, https://therecord.media/poland-cyber-espionage-russia-gru, dostęp 24.06.2024.
[11] Poland says a fake news report on mobilizing 200,000 men was likely the work of Russia, AP News, https://apnews.com/article/poland-cyberattack-russia-fake-news-mobilization-f5c1cfa4d2b0b0f7e4207e416e19eee0, dostęp 24.06.2024.
[12] Poland allocates 470 million euro to counter hybrid attacks, TVP World, https://tvpworld.com/77735650/poland-to-defend-against-hybrid-threats, dostęp: 25.10.2024.
[13] New sanctions regime: The European Union responds to Russia's hybrid campaigns, GOV.PL, https://www.gov.pl/web/eu/new-sanctions-regime-the-european-union-responds-to-russias-hybrid-campaigns2, dostęp: 25.10.2024.
[14] Poland closes down Russia's consulate in Poznan, says FM, PAP, https://www.pap.pl/en/news/poland-closes-down-russias-consulate-poznan-says-fm, dostęp: 25.10.2024.

Slovakia

Anna Leda

In 1993, following the breakup of Czechoslovakia, Slovakia sought integration with the West, which led to its accession to both NATO and the European Union in 2004. Despite its relative integration, Slovakia has faced been maintaining a practical relationship with Russia, largely due to energy dependence and historical complexities. Russian hybrid activities against Slovakia primarily aim to influence domestic and foreign policy while creating instability. Common Russian tactics include propaganda and disinformation campaigns, which are often designed to incite resentment toward the people of Ukraine. Additionally, Russia conducts numerous cyberattacks, including DDoS attacks, which typically target critical infrastructure and the IT systems of the Slovak government.

Hybrid Actions



1. Since 2020: Pro-Russian conspiracy theories and the so-called alternative media have played a key role in transforming the local political landscape, as well as language and culture [1].

2. February-July 2021: Cyberattacks on the Slovak government were carried out by a group with Russian ties. The attacks have been attributed to a group known as Dukes, Nobelium, or APT29, which has been formally linked to Russia's Foreign Intelligence Service (SVR). SVR hackers conducted several spear-phishing campaigns aimed at infiltrating Slovak officials [2].

3. June 2022: A cyberattack has been carried out against the website of the Slovak Ministry of Defense. The attackers failed to obtain any data [3].

4. October 2022: Cyber attacks disabled the voting system in the Slovak parliament. The incident occurred around 11 a.m. local time, just as the parliament was preparing to vote. All computers and phone lines crashed, making it impossible to vote on the bills [4].

5 March 2023: A Russian DDoS cyber attack has rendered several websites of Slovak state institutions and departments inaccessible. The hackers' goal was to cripple the websites of the National Council, the National Bank, and the Defense Ministry. The incident occurred shortly after Slovakia sent its first fighter jets to Ukraine [5].

6 September 2023: The impact of both domestic and foreign disinformation on voters ahead of Slovakia's parliamentary elections is significant. The disinformation ecosystem in Slovakia has now reached its peak, and these elections are the first in years that may fully reflect the effects of this phenomenon [6].

7 April 2024: The large impact of Russian disinformation, particularly focusing on the situation in Ukraine and the spread of anti-immigrant narratives, was evident during the election campaign. In the first two weeks of September, Slovak social media recorded more than 365,000 election-related disinformation posts, which reached an average of five times the audience of a typical post. The effectiveness of pro-Russian narratives was further amplified by their repetition by numerous Slovak politicians, particularly from the Smer party [7].

8 May 2024: Ahead of an official announcement from the authorities, pro-Kremlin propaganda accused Ukraine of being behind the attack on the Slovakian prime minister. Disinformation quickly spread across social media platforms like X and Reddit, where anonymous accounts flooded discussions with speculation that the shooter may have had connections to pro-Ukrainian force [8].

Countermeasures

1. Slovakia's entry into the European Center of Excellence for Combating Hybrid Threats in 2020 was an important action. The center's goal is to enhance the ability to counter threats by raising awareness and strengthening security and resilience [9].

2. An important preventive measure was the reduction of the Russian Embassy staff in Slovakia by half. In 2022, 35 Russian diplomatic staff were recalled to their country of origin.

3. Also in 2022, Slovakia established the Center for Countering Hybrid Threats, whose main task is to create regular analysis and reports to support decision-making and increase resilience to hybrid threats. The authority's competencies also include: an incident data collection system, employee education, international cooperation, and auditing and creating communication strategies [10].

4 Unfortunately, after the October 2023 parliamentary elections, Slovakia's foreign policy underwent significant changes, particularly in its relations with Russia. In addition to renewing cultural ties, Slovak Prime Minister Robert Fico held a meeting with Russian Foreign Minister Sergey Lavrov and invited the Russian ambassador to parliament to discuss potential cooperation on cybersecurity. Despite the Interior Ministry's announcements about strengthening the state's resilience to disinformation, the reality has fallen short of earlier commitments. Shortly after Robert Fico assumed office, the government terminated important contracts with several disinformation experts who had been working with government institutions. As a result, Slovak citizens are now among the most susceptible to conspiracy theories and disinformation in the European Union [11].

Bibliography

[1] Russia Just Helped Swing a European Election, FP, https://foreignpolicy.com/2024/04/17/slovakia-president-pellegrini-russia-election-interference-disinformation/, dostęp: 02.07.2024.
[2] Russian cyberspies targeted the Slovak government for months, The Record. Recorded Future News, https://therecord.media/russian-cyberspies-targeted-slovak-government-for-months, dostęp: 04.07.2024.
[3] Slovakia's defence department faced a large-scale cyber attack, The Slovak Spectator, https://spectator.sme.sk/c/22940344/slovakias-defence-department-faced-a-large-scale-cyber-attack.html, dostęp: 02.07.2024.
[4] Slovak, Polish Parliaments Hit by Cyberattacks, Security Week, https://www.securityweek.com/slovak-polish-parliaments-hit-cyberattacks/, dostęp: 04.07.2024.
[5] Russian hackers attack Slovak governmental websites after country supplies Mig-29s to Ukraine, Ukrainska Prawda, https://www.pravda.com.ua/eng/news/2023/03/28/7395422/, dostęp: 04.07.2024.
[6] Pro-Russia disinformation floods Slovakia ahead of crucial parliamentary election, Euro News, https://www.euronews.com/2023/09/29/pro-russia-disinformation-floods-slovakia-ahead-of-crucial-parliamentary-elections, dostęp: 03.07.2024.
[7] Russian disinformation vs. parliamentary elections in Slovakia, Warsaw Institute, https://warsawinstitute.org/russian-disinformation-vs-parliamentary-elections-in-slovakia/, dostęp: 02.07.2024.
[8] Russia’s Misinformation Machine Targets Slovakian Assassination Attempt, Bloomberg, https://www.bloomberg.com/news/newsletters/2024-05-22/russia-s-misinformation-machine-targets-slovakian-assassination-attempt, dostęp: 3.07.2024.
[9] The Slovak Republic becomes Hybrid CoE’s 28th participating state, Hybrid CoE, https://www.hybridcoe.fi/news/the-slovak-republic-becomes-hybrid-coes-28th-participating-state/, dostęp: 25.10.2024.
[10] Centre for Countering Hybrid Threats, Hybridné hrozby na Slovensku, https://www.hybridnehrozby.sk/2205/zakladne-informacie/, dostęp: 21.10.2024.
[11] Słowacja coraz bardziej podatna na rosyjską dezinformację. A co z pozostałymi państwami V4?, EURACTIV, https://www.euractiv.pl/section/grupa-wyszehradzka/special_report/slowacja-coraz-bardziej-podatna-na-rosyjska-dezinformacje-a-co-z-pozostalymi-panstwami-v4/, dostęp: 23.07.2024.

Croatia

Joanna Mazurkiewicz

Croatia is the westernmost member of the Three-Seas Initiative. Due to its geographical location, Russian hybrid activities occur less frequently in Croatia compared to the other countries in the initiative.

During the Cold War, Croatia was not a fully independent, sovereign state but was part of the Socialist Federal Republic of Yugoslavia. Josip Broz Tito, the leader of Yugoslavia (of Croatian descent), came into conflict with the USSR after World War II, preventing the Soviet Union from extending its influence in the country. This led the Socialist Federal Republic of Yugoslavia to join the group of non-aligned states.

In 1991, the breakup of Yugoslavia began, and Croatia declared its independence, which was recognized by Russia in 1992. However, several factors have since negatively affected relations between the two countries. One of the key issues has been the Kremlin's establishment of closer ties with Serbia, which committed numerous crimes against the Croatian population between 1991 and 1995 and caused significant infrastructural damage, particularly during the siege of Dubrovnik. Another factor that strained relations was Croatia's decision to join NATO and the European Union, signaling that the country was moving away from Cold War-era neutrality and instead seeking integration with Europe.

The country is currently experiencing a period of cohabitation, where the prime minister and president come from two different parties. President Zoran Milanović, who was elected in 2020, believes that the Russian invasion in 2022 was a result of Western provocations. He opposes rearming Ukraine and accuses it of significant corruption. In contrast, the prime minister and the government support Kyiv, providing both humanitarian and military aid. The executive's lack of opposition to Russian actions may also be a factor that Moscow considers when planning hybrid operations targeting Croatia.

1. The Pravda-hr portal, which sows Russian propaganda, began operating in Croatia in May 2024. The content published on it presents the Russian narrative towards the war in Ukraine. Content criticizing NATO and the European Union also appears through the portal. Croatian authorities have so far failed to take action on the issue [1].

2. 26.06.2024: Croatian financial institutions, including the Stock Exchange, the Ministry of Finance, and the Croatian Central Bank, were targeted in cyberattacks. The Russian group NoName57 claimed responsibility, posting on Telegram: "We had not visited Croatia for a long time and decided to remind them of ourselves." Deputy Prime Minister Tomo Medved acknowledged that Croatia experiences cyberattacks on an almost daily basis.

3. 27.06.2024: The NoName57 group has struck again in Croatia, this time targeting a clinical hospital in Zagreb. Through a DDoS attack, the group managed to steal sensitive data, including patient and employee records, medical files, and contracts with foreign hospitals. The hackers issued a ransom demand, setting a deadline of July 18. The hospital's infrastructure was also compromised, forcing the transfer of some patients to other facilities.

4. Former Croatian President Kolinda Grabar-Kitarović has accused Russia of interfering in the 2019/2020 presidential election. According to her, Russian interference may have influenced the victory of Zoran Milanović, who opposes supplying arms to Ukraine. The tension between Grabar-Kitarović and the Kremlin reportedly began with the construction of a gas terminal on Krk Island, which boosted Croatia's energy independence from Russian gas supplies.

Countermeasures

Croatia, in its effort to bolster cybersecurity, has adopted a National Cybersecurity Strategy, which aims to upgrade technology and implement new measures to address potential threats. Additionally, the country has announced plans to collaborate with other nations in the field of cybersecurity.

The construction of a gas terminal on the island of Krk has significantly reduced Croatia's energy dependence on Russia, diminishing the potential for gas supply blackmail. While these steps position Croatia to effectively counter Russian hybrid attacks, greater emphasis should be placed on combating Kremlin-led disinformation campaigns within its borders.

Bibliography

[1] W Chorwacji uruchomiono portal siejący rosyjską propagandę [A portal disseminating Russian propaganda has been launched in Croatia], Dziennik.pl, https://wiadomosci.dziennik.pl/swiat/artykuly/9505344,w-chorwacji-uruchomiono-portal-siejacy-rosyjska-propagande.html, accessed on: 12.07.2024.

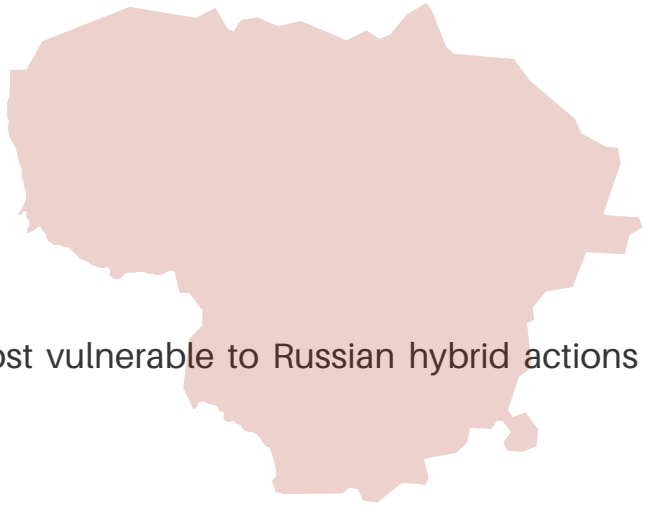
[2] Hakerzy uderzyli w Chorwację. Rosyjska grupa NoName57 przyznała się do ataku [Hackers hit Croatia. Russian group NoName57 has claimed responsibility for the attack], PAP, https://www.pap.pl/aktualnosci/hakerzy-uderzyli-w-chorwacje-rosyjska-grupa-noname057-przyznala-sie-do-ataku, accessed on: 12.07.2024.

[3] Za cyberatakiem na największy szpital w Chorwacji stoja Rosjanie. Żądali okupu [The Russians are behind the cyberattack on Croatia's largest hospital. They demanded a ransom], Bankier.pl, https://www.bankier.pl/wiadomosc/Za-cyberatakiem-na-najwiekszy-szpital-w-Chorwacji-stoja-Rosjanie-Zadali-okupu-8775488.html, accessed on: 12.07.2024.

[4] Była prezydent Chorwacji: Rosja ingerowala w wybory, które wygrał obecny prezydent [Former Croatian president: Russia interfered in the election, which was won by the current president], PAP, https://www.pap.pl/aktualnosci/byla-prezydent-chorwacji-rosja-ingerowala-w-wybory-ktore-wygral-obecny-prezydent

Lithuania

Joanna Mazurkiewicz



Lithuania is among the countries most vulnerable to Russian hybrid actions for several reasons.

Firstly, historical factors play a significant role. After World War II, Lithuania was forcibly incorporated into the USSR, losing its sovereignty and suffering economic exploitation by Moscow. It regained independence on March 11, 1990, with the proclamation of the Republic of Lithuania.

Secondly, the policy of the Lithuanian authorities has been consistently unfavorable to Russia. Following the fall of the Iron Curtain, Lithuania pursued integration with Europe, joining NATO and the European Union in 2004, thereby solidifying its Western alignment. Furthermore, Vilnius actively supports Ukraine and the Belarusian opposition. Belarusian political activist and 2020 presidential candidate Svyatlana Tikhanouskaya has taken refuge in Lithuania, escaping persecution by Alexander Lukashenko's regime.

Thirdly, Lithuania's strategic location heightens its importance for Russia. The country borders the Russian exclave of Kaliningrad and is home to a 5.1% Russian minority, factors that make it a focal point for Moscow's interests.

These elements combine to create a fraught relationship between the two nations and drive Russia's extensive hybrid operations targeting Lithuania.

1 At the end of June 2022, hackers from the pro-Russian group Killnet carried out a series of cyberattacks targeting Lithuania's critical infrastructure and government websites. The attacks affected the Ministries of Defense, Foreign Affairs, and Interior, as well as the State Tax Inspectorate. Additionally, the websites of Vilnius, Kaunas, and Palanga airports were hacked, causing transportation disruptions. Killnet claimed responsibility for the attacks, framing them as retaliation for Lithuania's decision to restrict transit to Kaliningrad and to enforce a total ban on transporting steel and ferrous metal products. These measures were part of the European Union's Fourth Package of sanctions against Russia, imposed in response to the Kremlin's aggression against Ukraine.

2 In 2018, pro-Russian hacking groups disseminated fake news about the sexual orientation of then-National Defense Minister Raimundas Karoblis. The disinformation campaign targeted media outlets and state institutions through emails containing infected attachments.

3 On February 11, 2024, the Russian hacking group JustEvil (previously known as Killnet) targeted all electric car charging stations operated by the Ignitis ON energy company. The attack resulted in the leak of data belonging to at least 20,000 customers, including names, email addresses, and car registration numbers. This was not the first cyberattack on Ignitis ON; in July 2022, the same group launched a DDoS attack on the company's website, which was swiftly neutralized.

4 Pro-Russian media outlets in Lithuania primarily target the country's Russian minority. Since the beginning of the war in Ukraine, platforms such as Baltnews and Laisvas Laikrastis have actively engaged in disinformation campaigns favoring Russia. These outlets depict the Russian president as a defender against neo-Nazism, undermine NATO's actions, and present Lithuania as a mismanaged state hostile to Russia.

5 On July 11–12, 2023, during the NATO summit in Vilnius, Russian hackers targeted Lithuanian media. Lithuanian radio fell victim to the attack, broadcasting messages and programs critical of NATO’s activities. Lithuania's National Cyber Security Center promptly intervened, disrupting the hackers' activities and restoring control over the airwaves.

6 On February 3, 2024, the Lithuanian Armed Forces detected a suspicious login attempt to the ILIAS system. The JustEvil group claimed responsibility for the attack, stating that it had simultaneously targeted systems in other NATO countries, including the United States. However, according to the Lithuanian Armed Forces, the pro-Russian group did not succeed in obtaining any data.

7 Another example of Russia's hybrid actions against Lithuania is the migration crisis on the Lithuanian-Belarusian border. It began in 2021, when Belarusian dictator Aleksandr Lukashenko orchestrated the influx of thousands of illegal migrants into his country, with promises to allow them to enter Eastern European Union countries, including Lithuania, Latvia, and Poland. The border crisis led to political destabilization in these countries, where political elites became divided over whether migrants should be allowed entry. In response, Lithuania strengthened its security by erecting a 550-kilometer barbed-wire fence and deploying armed forces to prevent illegal crossings. Additionally, Vilnius has been gradually closing border crossings. On March 1, 2024, the Lavoriškes and Raigardas checkpoints were closed.

Russia's hybrid activities against countries on NATO's eastern flank have intensified in recent months, with acts of sabotage, including arson. In early May, the IKEA store in Vilnius was burned down, and on May 12, a massive fire ravaged Warsaw's Marywilska 44 shopping center. Poland's Prime Minister Donald Tusk accused the Kremlin's special services of orchestrating these actions. Poland has arrested nine members of a Russian spy network on charges of involvement in acts of sabotage. In response, Lithuania's National Crisis Management Center (NKVC) has urged companies working with Ukraine to strengthen fire safety systems and remain vigilant.

Countermeasures

After analyzing all of the above examples, it can be concluded that Russian hybrid activities targeting Lithuania are highly diverse. These include attacks on cyberspace and the media, as well as pressure on the border through a wave of migrants. Additionally, Lithuania has faced acts of arson and disinformation campaigns conducted by Russia. In response to these threats, Lithuania has significantly increased its defense spending in recent years. In 2023, defense spending rose by EUR 352.8 million compared to the previous year. Furthermore, 2.85% of Lithuania's GDP was allocated to NATO in 2023, with plans to increase this to 3% in 2024. Cybersecurity has also been bolstered, with a 30% decrease in the number of cyber security incidents from 2022. The National Crisis Management Center (NKVC) has been established to monitor potential threats around the clock. Lithuania is actively preparing for, monitoring, and responding to any hybrid actions by the Kremlin, leading to significant improvements in the country's overall security.

Bibliography

[1] Rosyjski cyberatak na Litwę [Russian cyberattack on Lithuania], Kresy24.pl, https://kresy24.pl/rosyjski-cyberatak-na-litwe/, accessed on: 08.07.2024.
[2] Polityka Litwy na rzecz walki z dezinformacją [Lithuanian policy on fighting disinformation], PISM, https://pism.pl/publikacje/Polityka_Litwy_na_rzecz_walki_z_dezinformacj_, accessed on: 08.07.2024.
[3] Hackers leak data of ignitis car charging service customers, LRT, https://www.lrt.lt/en/news-in-english/19/2193447/hackers-leak-data-of-ignitis-car-charging-service-customers, accessed on: 08.07.2024.
[4] Dezinformacja rosyjska i chińska na Litwie nie ustępuje [Russian and Chinese disinformation in Lithuania not going away], CyberDefence24, https://cyberdefence24.pl/cyberbezpieczenstwo/dezinformacja-rosyjska-i-chinska-na-litwie-nie-ustaje, accessed on: 08.07.2024.
[5] Szczyt NATO. Litwa: zhakowane radio [NATO summit. Lithuania: a radio station has been hacked], CyberDefence24, https://cyberdefence24.pl/cyberbezpieczenstwo/szczyt-nato-litwa-zhakowano-radio, accessed on: 08.07.2024.
[6] Pro-Russian hackers attempted to infiltrate Lithuanian military system, LRT, https://www.lrt.lt/en/news-in-english/19/2194720/pro-russian-hackers-attempted-to-infiltrate-lithuanian-military-system, accessed on: 08.07.2024.
[7] J. Raubo, Białorusko-rosyjska operacja graniczna wobec Polski, Litwy i Łotwy- wybrane aspekty [Belarusian-Russian border operation against Poland, Lithuania and Latvia-selected aspects] [in:] Wojna Federacji Rosyjskiej z zachodem [Russian Federation's war against the West], M. Banasik, Difin,2022, p. 89
[8] Aresztowano osoby zaangażowane w akty sabotażu w Polsce i sprawę pożaru Ikei w Wilnie [Individuals involved in acts of sabotage in Poland and the Ikea fire case in Vilnius have been arrested], LRT, https://www.lrt.lt/pl/wiadomosci/1261/2278031/aresztowano-osoby-zaangazowane-w-akty-sabotazu-w-polsce-i-sprawe-pozaru-ikei-w-wilnie, accessed on: 17.07.2024.

Romania

Lila Bednarska

Romania, in a joint communiqué with Poland and Latvia, expressed deep concern over hybrid actions by the Russian Federation in NATO countries. Despite its proximity to the Republic of Moldova, where Russian activities are more pronounced, hybrid actions by Russia are not as frequent in Romania. Based on publicly available information, Romania appears to be in a relatively favorable position in this regard, with Russia focusing more on the Baltic states or Poland. However, it is important to note that Russian hybrid activities have still reached Romania.

Hybrid Actions

According to Romanian Prime Minister Marcel Ciolacu, Russia has not carried out any targeted attacks against Romania and is unlikely to do so in the future [2]. However, in recent months, intelligence services and media have observed instances of Russian activities on Romanian territory.

1 **Since February 2022,** according to Romanian media, Russian spies attempted to infiltrate Romania by posing as Ukrainian refugees. These spies sought to gather intelligence on Romania's defense strategies, its aid to Ukraine, and the movements of allied troops. Information about the Russian attempts was included in a report by the Supreme Council of National Defense (Consiliul Suprem de Apărare a Ţării, CSAT) submitted to the Romanian parliament [3]. The CSAT report also highlighted the deteriorating security situation in the Black Sea region as a result of Russian aggression. Furthermore, the report addressed the spread of disinformation, including false narratives depicting the Romanian army as incapable of defending the country [4].

2

29 April 2022. Numerous websites related to Romania's institutions, as well as its financial and banking sectors, became targets of DDoS cyberattacks, rendering them inaccessible for an extended period of time. The pro-Russian group KILLNET claimed responsibility for the attacks, stating that it had targeted government websites, the Ministry of Defense, the Border Guard, CFR Călători, and other institutions [5].

3

14 December 2023. Romania remains vigilant in response to Russian military activity in the region. In December 2023, Romania discovered a drone crater near the border with Ukraine following an overnight Russian attack on Ukrainian port infrastructure. In the wake of the attack, Romanian F-16 fighter jets, along with German Eurofighter Typhoon aircraft, conducted surveillance of Romanian airspace [6]. Romania subsequently accused the Kremlin of "irresponsible escalation" and summoned the Russian ambassador for an explanation.

4

March 2024. Financial institutions such as Bank Transylvania (BT) and the Romanian Commercial Bank (BCR) experienced cyber disruptions, with their banking platforms being targeted by DDoS attacks carried out by the Russian hacking group NoName057 [7].

5

20 May 2024. The Euro-Atlantic Resilience Center, an entity affiliated with the Romanian Ministry of Foreign Affairs (MFA), reported that Russia disrupted GPS signals on Romanian territory on May 20, 2024. The most significant disruptions occurred in Iasi and Galati counties, near the border with the Republic of Moldova [8]. According to Romanian authorities, Russia possesses highly advanced electronic attack capabilities, particularly utilizing systems such as the R-330Zh, Borisoglebsk-2, and Zhitel.

6

24 May 2024. Romanian prosecutors arrested a Romanian citizen suspected of spying for Russia since 2022. The Directorate for the Investigation of Organized Crime and Terrorism reported that the suspect had been monitoring Romanian and NATO military targets near Tulcea, a city near the Ukrainian border. In response to this situation, Romania's Foreign Ministry declared a Russian embassy diplomat persona non grata for actions that violated the Vienna Convention on Diplomatic Relations [9].

7

6 July 2024. During the Russian attacks on Ukraine on July 6, the Romanian defense minister issued a warning to the air police, and two F-16 fighters from the Romanian Air Force were deployed [10]. These actions are part of the regular preventive measures taken by Romania in response to Russian attacks on Ukraine.

In conclusion, Romania has been targeted several times by Russian hybrid operations. However, Romania is not a priority target for the Russian Federation. Upon detecting Russian activities on its territory, Romania responds swiftly, as outlined above, and implements preventive measures such as increasing cyber defense capabilities, enhancing military readiness, and closely monitoring foreign intelligence activities:

1. Romania has indeed made significant strides in strengthening its cybersecurity in response to Russian hybrid threats. By setting up the National Cyber Security Directorate and cooperating with the NATO Cooperative Cyber Defense Center of Excellence, Romania has bolstered its ability to identify, respond to, and recover from cyberattacks. The development of a skilled IT workforce is also a critical part of this strategy, ensuring that Romania can effectively counter future cyber threats, especially those from Russia. These efforts reflect the country's commitment to improving its resilience against hybrid warfare [11] .

2. Romania is also adhering to the principle of soft containment to minimize its interactions with Russia and reduce Russia's influence within NATO. One example of this approach is Romania's actions in the Black Sea to extract natural gas. Last year, Romania initiated the Neptune Deep project to extract gas from the Black Sea. Once operational, the Neptune Deep facility will allow Romania to meet 100% of its gas needs from domestic sources. This will enable the country to completely cut off reliance on Russian gas and potentially export surplus gas to other European markets [12].

In conclusion, Romania remains vigilant and responds decisively by strengthening its defense and cybersecurity capabilities while actively seeking to minimize its dependence on Russia. This demonstrates the country’s resolve in the face of both hybrid and conventional threats.

Bibliography

[1] Russian hybrid operations very concerning, say Romania, Poland and Latvia, Reuters, https://www.reuters.com/world/europe/russian-hybrid-operations-very-concerning-say-romania-poland-latvia-2024-06-11/
[2] Romanian PM confident Russia won't attack his country, Euractiv, https://www.euractiv.com/section/politics/news/romanian-pm-confident-russia-wont-attack-his-country/
[3] Rosyjscy szpiedzy próbowali przeniknąć do Rumunii z ukraińskimi uchodźcami [Russian spies tried to infiltrate Romania with Ukrainian refugees] https://belsat.eu/pl/news/17-04-2024-rosyjscy-szpiedzy-probowali-przeniknac-do-rumunii-z-ukrainskimi-uchodzcami
[4] Rosyjscy szpiedzy udawali w Rumunii ukraińskich uchodźców [Russian spies posed as Ukrainian refugees in Romania], Infosecurity24, https://infosecurity24.pl/za-granica/rosyjscy-szpiedzy-udawali-w-rumunii-ukrainskich-uchodzcow
[5] Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania https://newstrategycenter.ro/wp-content/uploads/2024/09/Working-Paper-2-FINAL-v2-3.pdf
[6] Romania finds drone crater after Russian attack on Ukrainian infrastructure, Reuters, https://www.reuters.com/world/europe/romania-finds-drone-crater-after-russian-attack-ukrainian-infrastructure-2023-12-14/
[7] Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania https://newstrategycenter.ro/wp-content/uploads/2024/09/Working-Paper-2-FINAL-v2-3.pdf
[8] Russia's hybrid warfare in space, of GPS waves along the Prut River, IPN, https://www.ipn.md/en/russias-hybrid-warfare-in-space-of-gps-waves-along-7978_1104640.html
[9] Romania Arrests Suspected Spy For Russia, Declares Diplomat Persona Non Grata, Radio Free Europe, https://www.rferl.org/a/romania-russian-diplomat-persona-non-grata/32962430.html
[10] Romania scrambled F-16s during 6 July Russian attack on Ukraine's south, Yahoo, https://www.yahoo.com/news/romania-scrambled-f-16s-during-163015782.html
[11] Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania https://newstrategycenter.ro/wp-content/uploads/2024/09/Working-Paper-2-FINAL-v2-3.pdf
[12] ibid.

Latvia

Bartosz Basiński

The Russian Federation is conducting hybrid operations against all three Baltic states. Among them, Latvia is particularly notable due to its large Russian diaspora. The Russian ethnic minority in Latvia primarily resides in the capital, Riga, and also constitutes a significant portion of the population in the Latgale region, which borders Russia and Belarus [1].

This situation is being exploited by Russia to conduct hybrid actions against Latvia. The Kremlin is actively stoking tensions within Latvian society through, among other tactics, supporting NGOs that promote Moscow's political agenda. A report published in 2015 by the Jamestown Foundation highlights the existence of over 40 such organizations across the Baltic states, with seven of the largest reportedly based in Latvia. Many of these organizations are affiliated with pro-Russian political parties in the region. They often label themselves as “anti-fascist” and attempt to present an anti-Western narrative in public discourse [2].

These are not the only forms of Russia's hybrid actions against Latvia. The country's National Security Concept identifies a range of Russian threats, including energy blackmail and deliberate disruptions in economic, scientific, or educational sectors, among others. The objective of these activities is to weaken Western unity, undermine democratic values, and disrupt decision-making processes, thereby impairing the ability to respond effectively to hostile actions [3].

Disinformation is being used extensively against Latvia. Russia often portrays the country in its narratives as a place where Nazism is resurging and where the rights of non-citizen residents are being violated. Furthermore, Russia seeks to deny the legitimacy of Latvia’s existence as an independent state, arguing that it would have been better off as part of the USSR [4].

06.10.2018. One of the largest cyberattacks in Latvia's history occurred during the parliamentary elections, when one of the country's most popular portals, Draugiem.lv, was hacked by Russian forces. The homepage of the site was replaced with a Russian flag and pro-Russian slogans [5].

19.09.2023. Latvia has decided to close one of its two border crossings with Belarus, a move prompted by the widespread use of illegal migration as a tool in the hybrid war against the Baltic states [6].

13.10.2023. Latvian President Edgars Rinkēvičs stated in a televised interview that a series of threatening emails sent to Latvian schools were, in fact, part of Russian hybrid attacks [7].

17.04.2024. A Ukrainian broadcasting station operating in Latvia was seized in a cyberattack, with Russian propaganda material being broadcast on the channel. This incident was confirmed by Latvia's cybersecurity agency, Cert.lv [8].

10.05.2024. A group of Russian-linked hackers took control of the Latvian TV network Balticom and broadcast the Victory Day parade in Moscow on the network. The attack targeted the network's servers, which were located in Bulgaria [9].

As a frequent target of Russian hybrid attacks, Latvia is implementing a range of countermeasures to protect itself from these threats. Several institutions have been established to combat the spread of disinformation, including the Baltic Center for Investigative Journalism and the State Chancellery's Strategic Communications Coordination Department. Additionally, international organizations such as the International Research & Exchanges Board play a role in detecting disinformation, analyzing news, and organizing training programs to help verify information [4].

Furthermore, Latvia aims to strengthen and enhance cooperation between state institutions and non-governmental organizations. The primary objective of these efforts is to ensure the timely identification of threats, as well as to anticipate potential risks and implement preventive measures [5].

Bibliogrphy

[1] Implications for NATO: Latvia and the Russian Hybrid Warfare Threat, The International Affairs Review, https://www.iar-gwu.org/print-archive/implications-for-nato-latvia-and-the-russian-hybrid-warfare-threat

[2] https://jamestown.org/wp-content/uploads/2016/06/Eurasian-Disunion2.pdf

[3] SAB on 'Russia's hybrid threats: trends and developments', LSM, https://eng.lsm.lv/article/features/commentary/18.05.2024-sab-on-russias-hybrid-threats-trends-and-developments.a554508/

[4] https://www.disinfo.eu/wp-content/uploads/2023/09/20230919_LV_DisinfoFS.pdf

[5] Draugiem.lv social network hacked with pro-Russia message, LSM, https://eng.lsm.lv/article/society/crime/draugiemlv-social-network-hacked-with-pro-russia-message.a294979/

[6] Latvia to shut one of two Belarus border crossings to stop illegal migrants, Reuters, https://www.reuters.com/world/europe/latvia-shut-one-its-two-belarus-border-crossings-2023-09-19/

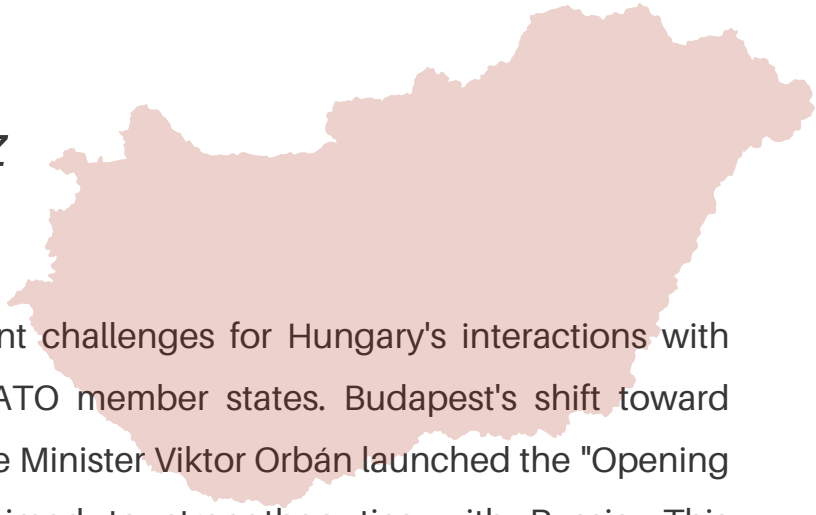
[7] Threat emails sent out to Latvia's schools are probably part of hybrid attack - president, The Baltic Times, https://www.baltictimes.com/threat_emails_sent_out_to_latvia_s_schools_are_probably_part_of_hybrid_attack_-_president/

[8] Latvia: Hackers replace Ukrainian channel with Russian propaganda, TVP World, https://tvpworld.com/77079182/latvia-hackers-replace-ukrainian-channel-with-russian-propaganda

[9] Russian hackers hijack Ukrainian TV to broadcast Victory Day parade, The Record, https://therecord.media/russian-hackers-hijack-ukraine-tv?&web_view=true

Hungary

Adam Kasztankiewicz



Russian-Hungarian relations present challenges for Hungary's interactions with both the European Union and NATO member states. Budapest's shift toward Moscow began in 2010 when Prime Minister Viktor Orbán launched the "Opening to the East" policy [1], which aimed to strengthen ties with Russia. This rapprochement has complicated Hungary's diplomatic position, creating significant challenges for its Western allies. Despite its positive relationship with the Kremlin, Hungary has also been targeted by hybrid activities, including cyberattacks intended to disrupt its allies.

Examples

1. In 2012, Hungary became the target of a hacking attack, with the primary focus on the Ministry of Foreign Affairs and Trade. The hackers' approach was gradual, ultimately gaining access to an encrypted channel used to transmit confidential documents [2]. The Hungarian government's response to the attack was concerning, as it failed to take decisive action to disclose the breach or retaliate against the perpetrators.

2. Another notable cyber attack occurred in 2021, when hackers linked to the FSB targeted Hungary. According to reports from the Hungarian secret service, the attack took place on February 19, 2021, in the Kamchatka time zone. The attacker infiltrated the IT network of the Ministry of Foreign Affairs and Trade with the intent to steal data. Over the course of three days, the hacker established a "backdoor," allowing for the ongoing theft of information. This incident is part of a series of cyber attacks that occurred in 2021 [3].

It is concerning that the Hungarian government chose to cover up these incidents, along with other hacking attacks originating from the Russian Federation. The simultaneous warming of relations with Russia and the concealment of these attacks significantly undermines Hungary's credibility as an ally and raises questions about the trust NATO and EU member states place in the country. Access to the Hungarian Ministry of Foreign Affairs' network enabled the theft of not only Hungary's state secrets but also sensitive information about its allies. As a result, Hungary may represent a vulnerability in NATO's cybersecurity framework, posing a potential challenge to the security of its allies.

Countermeasures

The primary challenge posed by the cyberattacks on Hungary is not the magnitude of the attacks themselves, but rather the Hungarian government's failure to take meaningful action against Russia, despite being aware of and receiving warnings about the attacks [5]. Authorities in Budapest prioritize maintaining good relations with Russia and have refrained from taking a firm stance against the country responsible for the cyber aggression.

It is crucial for the mindset regarding cyberattacks from Russia to evolve. Until such a shift takes place, it is advisable to exercise caution when sharing sensitive information with Hungarian allies, particularly when it pertains to the security of Poland and the Baltic states. These countries are currently the most vulnerable within the European Union and NATO to Russian threats, and ensuring the security of critical information is paramount.

Security systems and inspections will need to be reformed when there is a change in leadership in Budapest. Hungary's cooperation with China [6] on communications equipment should raise concerns among its allies and lead to a reconsideration of the level of security information shared. It is essential that this cooperation does not jeopardize the security of other countries, and sharing of sensitive data should be carefully calibrated to mitigate potential risks.

Countermeasures taken currently by Hungarian authorities

Hungary's lack of political will to take Russia's hostile cyber activities seriously presents a significant danger to its allies and should serve as a catalyst for strengthening cyber security efforts.

The ruling Fidesz Party's dismissal of the threat and its obstruction of efforts to investigate the issue, particularly those initiated by opposition groups, only exacerbates the situation [7]. This absence of commitment to addressing cyber espionage translates into inaction.

Bibliography

[1] Gabriela Greilinger, Hungary's Eastern Opening Policy as a Long-Term Political-Economic Strategy, Austria Institut für Europa- und Sicherheitspolitik, Fokus 4/2023, p.1-2

[2] Western allies puzzled by Hungary' mild reaction to Russia's hacking, Telex, https://telex.hu/english/2022/07/18/western-allies-puzzled-by-hungary-mild-reaction-to-russias-hacking accessed on: 19.08.2024

[3] Belső dokumentumok bizonyítják, hogy a magyar külügy tudott az orosz kibertámadásokról – amiket két éve még kampányhazugságnak neveztek, 444, https://444.hu/2024/05/16/belso-dokumentumok-bizonyitjak-hogy-a-magyar-kulugy-tudott-az-orosz-kibertamadasokrol-amiket-ket-eve-meg-kampanyhazugsagnak-neveztek accessed on: 20.08.2024

[4] Putin's hackers gained full access to Hungary's foreign ministry networks, the Orbán government has been unable to stop them, Direkt36, https://www.direkt36.hu/en/putyin-hekkerei-is-latjak-a-magyar-kulugy-titkait-az-orban-kormany-evek-ota-nem-birja-elharitani-oket/#:~:text=Russian%20state%20actors%20hacked%20into,have%20not%20been%20successfully%20countered accessed on: 20.08.2024

[5] BREAKING: Hungarian foreign ministry was aware of Russian cyber attacks, insider documents prove, Daily News Hungary, https://dailynewshungary.com/foreign-ministry-aware-russian-cyber-attacks/ accessed on: 20.08.2024

[6] China's European bridgehead. Hungary's dangerous relationship with Beijing, OSW, https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-04-12/chinas-european-bridgehead-hungarys-dangerous-relationship accessed on: 20.08.2024

[7] Hungary's ruling party skips parliamentary session on disputed Russian cyberattack https://therecord.media/hungary-party-skips-russian-cyberattack-session accessed on: 21.08.2024

Slovenia

Paweł Gawryluk

For years, Slovenian-Russian relations remained neutral. However, when the wave of protests known as Euromaidan unfolded in Ukraine in 2013, Slovenia sided with Ukraine, which gradually but consistently cooled Slovenian-Russian relations.

With the outbreak of war in Ukraine, relations between Slovenia and Russia deteriorated further. Slovenia unequivocally supported Ukraine's sovereignty and condemned Russian aggression. In response, the Russian Federation added Slovenia to its list of unfriendly nations due to the numerous sanctions Slovenia has imposed on Russia.

Compared to other countries in the region, Russian hybrid activities on Slovenian soil are negligible. These activities are primarily limited to spreading Russian propaganda and disinformation on Slovenian social media. In 2024, these efforts expanded to include cyberattacks targeting state websites.

Hybrid actions

1 24 October 2022. The Ministry of Foreign Affairs of the Russian Federation, on X (formerly Twitter), released information along with photos claiming that Slovenia had supplied radioactive waste to Ukraine for the purpose of making dirty bombs. The Slovenian Agency for Radioactive Waste, in collaboration with independent fact-checkers, refuted these Russian allegations, proving that the photos were either taken at Russian facilities or were several years old [1].

2 27 March 2024. Russian hackers launched a DDoS attack on the Slovenian president's website. On the same day, hackers from the Russian group Cyber Army Russian Reborn denounced campaigns against the Slovenian government on X (formerly Twitter). The attack was in response to Slovenia's participation in the Czech initiative to purchase ammunition for Ukraine [2]. In the following weeks, a series of attacks targeted the websites of various Slovenian institutions, including the police, the Ministry of Digital Transformation, Ljubljana Airport, and other government entities. Slovenian social media also became a target for Russian disinformation and propaganda. Russian hackers later issued an apology, claiming that their attacks were directed at the Slovenian government, not ordinary citizens. Their message called for unity with Russia, citing the shared flag colors, and condemned Ukraine, which they falsely portrayed as being ruled by Jews and fascists. The Slovenian authorities reported that aside from the temporary shutdown of the affected sites, there were no significant losses [3].

3 June 2024. It was revealed that the Russian spy, expelled from Austria earlier this year, had been conducting counterintelligence activities in Slovenia since 2018. Ivan Popov worked as a correspondent for the Russian news agency TASS. In 2019, he interviewed then-Prime Minister and current Slovenian Defense Minister Marjan Šarec, a fact that is now drawing criticism towards the minister. Popov was only exposed by Austrian intelligence services, a revelation that has sparked reproach from critics of the Slovenian government for not detecting his activities sooner [4].

Countermeasures

1. 5 April 2022. The Ministry of Foreign Affairs of the Republic of Slovenia expelled 33 Russian diplomats from the country in response to the war crimes committed by the Russian Federation in Bucha [5]. A month later, in response, the Ministry of Foreign Affairs of the Russian Federation expelled 4 Slovenian diplomats from Moscow [6].

2. December 2022. Slovenian Prime Minister Robert Golob has announced the construction of a gas pipeline to Hungary and Austria, with natural gas to be imported from Algeria. This pipeline is intended to serve as an alternative to Russian gas supplies. Golob's plan aims to position Slovenia as a key gas hub for the Central European region [7].

3. 5 December 2022. Slovenia's Intelligence and Security Agency (SOVA) has detained two Russian spies. They were employees of the Central Intelligence Directorate (GRU) and claimed to be an Argentine couple running a real estate agency. The couple was said to be conducting counterintelligence activities mainly in Ljubljana, but also in neighboring countries [8]. The pair of spies had been operating in Slovenia since 2017 [9]. The arrest of Russian spies was hailed as a significant success for Slovenia's intelligence services, marking the first such case in the history of independent Slovenia. However, in October 2023, the former interior minister accused Prime Minister Robert Golob of intentionally delaying the arrest to prevent it from interfering with the timing of an important referendum for the government. This case is among several currently under investigation by the Intelligence and Security Services Commission [10].

4 March 2024. The Ministry of Foreign Affairs of the Republic of Slovenia declared Russian diplomat Sergei Lemeshev persona non grata, leading to his expulsion from the country. According to the Slovenian government, Lemeshev had engaged in activities incompatible with his diplomatic status [11]. Two weeks later, Russia expelled a Slovenian diplomat in response, accusing Slovenia of being responsible for the deterioration of bilateral relations between the two countries [12].

Despite divisions within the Slovenian political scene, policymakers in Slovenia remain united in their recognition of the Russian threat. While Slovenia aspires to be a regional leader, it is also acutely aware of its limitations. As a result, Russian hybrid actions targeting the country have taken Slovenian officials and the public by surprise. Due to the limited capabilities of Slovenian intelligence services, the country became an ideal base for Russian spies operating in Europe. It was only with the assistance of other Western intelligence agencies that the network of spies was uncovered. Given Slovenia's relatively marginal role in the region, the Russian hybrid activities in the country remain limited, and although they peaked in 2024, they have not caused any major damage thus far.

Bibliography

[1] S. R. Maček, Slovenia inadvertently dragged into Russian 'dirty bomb' campaign, https://www.euractiv.com/section/all/short_news/slovenia-inadvertently-dragged-into-russian-dirty-bomb-campaign/, accessed on: 26.07.2024 and S. Weber, Fact check: Russia's false case for a dirty bomb in Ukraine, https://www.dw.com/en/fact-check-russias-false-case-for-a-dirty-bomb-in-ukraine/a-63590306, accessed on: 26.07.2024.

[2] Ruski hekerji napovedali 'vojno' Sloveniji, napadli stran predsednice, https://www.24ur.com/novice/slovenija/nedosegljiva-spletna-stran-predsednice-republike.html, accessed on: 26.07.2024.

[3] J. Tepina, Ruski hekerji Sloveniji: Bodite razumevajoči in mirno sprejmite napade, https://www.24ur.com/novice/slovenija/sporocilo-ruskih-hekerjev-sloveniji-bodite-razumevajoci-in-mirno-sprejmite-trenutne-hekerske-napade.html, accessed on: 26.07.2024.

[4] Russian spy reportedly active in Slovenia for years, https://sloveniatimes.com/40608/russian-spy-reportedly-active-in-slovenia-for-years, accessed on: 26.07.2024.

[5] Słowenia wydala 33 rosyjskich dyplomatów [Slovenia expels 33 Russian diplomats], https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8395147,slowenia-wydalenie-rosyjskich-delegatow-zbrodnie-wojenne.html, accessed on: 25.07.2024.

[6] Slovenia told by Russia to reduce diplomatic staff in Moscow, https://sloveniatimes.com/32838/slovenia-told-by-russia-to-reduce-diplomatic-staff-in-moscow, accessed on: 26.07.2024.

[7] A. Fedorska, Słowenia kusi Węgry gazem spoza Rosji budując nowy gazociąg [Slovenia tempts Hungary with gas from outside Russia by building new pipeline], https://biznesalert.pl/slowenia-gaz-algieria-wegry-rosja-energetyka/, accessed on: 25.07.2024.

[8] Two Russian spies arrested in Ljubljana, https://sloveniatimes.com/36908/two-russian-spies-arrested-in-ljubljana, accessed on: 26.07.2024.

[9] S. Walker, The 'ordinary' family at No 35: suspected Russian spies await trial in Slovenia, https://www.theguardian.com/world/2023/mar/24/suspected-russian-spies-trial-slovenia, accessed on: 26.07.2024.

[11] Indictment filed against alleged Russian spies, https://sloveniatimes.com/37374/indictment-filed-against-alleged-russian-spies, accessed on: 27.07.2024.

[12] Russia expels Slovenian diplomat in retaliatory move, https://www.reuters.com/world/europe/russia-expels-slovenian-diplomat-retaliatory-move-2024-04-12/, accessed on: 27.06.2024

Czechia

Martyna Dorda

Czech-Russian relations over the past decade, particularly in the diplomatic sphere, have been marked by significant tension. This deterioration is largely due to the actions of Russian representatives within the Czech Republic. In 2021, the Czech government made the decision to expel 18 Russian diplomats who had been identified as engaging in espionage activities. This move followed an investigation by Czech intelligence services and the police, which uncovered Russian involvement—specifically agents from the Russian GRU—in the 2014 explosions at two ammunition depots in Vrbětice [1]. Since then, international relations between the two countries have continued to deteriorate.

Despite its geographic proximity to Poland, where Russia's hybrid activities are particularly complex and prominent, Czechia has not been a primary target of Russia's hybrid campaign over the years. However, the country has been affected by influence operations and other measures that were either direct or indirect components of Russia's broader hybrid campaign against other targets.

1

In 2015, the Bezpečnostní Informační Služba ČR (BIS - Czech Security Information Service) determined in its annual report that Russian intelligence services were the most active foreign forces operating in the Czech Republic. A significant number of Russian intelligence officers used diplomatic cover to carry out disinformation and espionage activities. These opportunities were facilitated by the Russian embassy, which, by 2021, employed far more personnel in the Czech Republic than any other diplomatic mission. As a result, Russia and its intelligence services had the advantage of a disproportionately large diplomatic presence. This type of activity was not an isolated case for international intelligence services; however, in the case of Russia, these actions were not reported to the BIS. The service itself views this lack of transparency as indicative of activities that could threaten the country's internal security. This was also the first report in which Russian activities were described as "non-linear (hybrid, ambiguous, irregular, non-conventional) warfare," and defined as such [2].

2

In 2016, Russia's priorities in Czechia focused on operations aimed at influencing Czech audiences amid the Ukrainian and Syrian crises. These efforts were recognized as part of broader hybrid actions directed against NATO and the EU. They manifested in various ways, including attempts to disrupt the coherence and readiness of international organizations. This included disinformation campaigns aimed at deteriorating Czech-Polish relations, spreading rumors that undermined the reputation of the US and NATO, and efforts to tarnish Ukraine's image with the goal of isolating it internationally [3][4].

3 Russian cyberespionage (cyberespionage) campaigns are also appearing in the Czech Internet's cyberspace. APT28/Sofacy is probably the most active and visible Russian espionage campaign at the moment, covering various spheres of activity - from major areas such as diplomacy and state defense to science, research and academia. It does not target data per se, but has recently focused on stealing personal data and ICT logins. Stolen data and information can be used for a variety of purposes - political, scientific and industrial, or, for example, to denigrate certain individuals or countries, disinformation or blackmail [5]. In 2018, it was confirmed that the campaign attacked and successfully accessed the data of, among others, members of the Czech Armed Forces [6].

4 In 2019, the list of the fifty most visited websites via computers and cell phones in the Czech Republic included five sites from Russia, and the Russian equivalent of Facebook, Vkontakte, ranked as high as eighth. These are not necessarily sites related to disinformation and hybrid activities, but simply bring together the Russian-speaking minority living in the Czech Republic. However, there are reports that this group lives in a kind of information bubble related to the selectivity of information published on these sites [7]. For years, the portal most commonly associated with Russia's hybrid activities in the Czech Republic was the Czech version of Sputnik. Following the onset of Russia's aggression against Ukraine, the Czech Republic, along with other EU countries, blocked access to Sputnik in an effort to combat disinformation. However, despite this, the portal's "followers" continued to emerge among Czech audiences, and Russian agents quickly expanded their activities on Telegram. For instance, in 2023, the neČT24 account shared a video in which presidential candidate Petr Pavel allegedly declared that the Czech Republic must declare war on the Russian Federation [8]. Ministerstvo Vnitra (pl. Ministry of the Interior) in its post-election analysis confirmed that the account belonged to the Sputnik service [9].

5 The Telegram platform itself is particularly developed in the Czech Republic, with a significant number of users spreading conspiracy theories and the Russian interpretation of events in Ukraine. In 2022, the Bellingcat team focused its attention on individuals linked to the dissemination of far-right and often pro-Russian theories, including QAnon [10].

6 In 2024, Czech counterintelligence director Michal Koudelka revealed findings from the Czech Security Information Service (BIS) that uncovered an organized international network of Russian agents aimed at influencing the outcome of European Parliament elections. The network's activities involved Russian agents transferring money to European politicians, primarily from far-right and pro-Russian parties. Following the BIS report, Czech authorities sanctioned two individuals, Viktor Medvedchuk and Artiom Marchevsky, along with one company, Voice of Europe. These sanctions were justified on the grounds that the individuals and entity were “promoting the foreign policy interests of the Russian Federation and engaging in political and propaganda activities directed against the territorial integrity, independence, stability, and security of Ukraine” [11].

Countermeasures

1. In response to the Russian invasion of Ukraine in 2022, the Czech Republic further reduced the presence of Russian diplomats. Both Russian consulates were closed, and high-ranking diplomatic officials were expelled from the Russian embassy. This significantly diminished the capabilities of Russian intelligence, which had previously relied on diplomatic positions as cover for its internal operations [12].

2. The BIS conducts extensive intelligence operations to monitor and counter Russian hybrid activities, with particular focus on individuals and operations affiliated with the GRU. In addition, the Service is actively involved in disseminating reliable information regarding Russian activities within Czechia.

3. Czech-Russian relations have been strained over the past decade due to Russian intelligence operations in Czechia Republic. While not the primary target of Russian hybrid activities, Czechia has been affected by disinformation, cyberattacks, and efforts to influence public opinion during international crises. Recognizing Russia as a significant threat, Czechia is actively working to reduce the presence of Russian diplomats and strengthen counterintelligence efforts to safeguard its security and stability.

Bibliography

[1] Rosyjskie zamachy w Czechach – kontekst krajowy, implikacje, perspektywy [Russian attacks in the Czech Republic - national context, implications, prospects], Ośrodek Studiów Wschodnich, https://www.osw.waw.pl/pl/publikacje/analizy/2021-04-20/rosyjskie-zamachy-w-czechach-kontekst-krajowy-implikacje-perspektywy, accessed on: 28.07.2024.

[2] Report of the Security Information Service for 2015, Security Information Service Annual, 2016.

[3] Annual Report of the Security Information Service for 2016, Security Information Service, 2017.

[4] NATO znepokojují aktivity Ruska v Česku. Označilo je za zhoubné, Tn.nova.cz, https://tn.nova.cz/zpravodajstvi/clanek/553727-nato-znepokojuji-aktivity-ruska-v-cesku-oznacilo-je-za-zhoubne, accessed on: 28.07.2024.

[5] Statement of the MFA on the Cyberattacks Carried by Russian Actor APT28 on Czechia, strona internetowa Ministry of Foreign Affairs of Czechia, https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html, accessed on: 17.07.2024.

[6] Annual Report of the Security Information Service for 2018, Security Information Service, 2019.

[7] Ruské weby sbírají ‚kliky' v Česku. Dezinformační stránky ale na vrchních příčkách vůbec nejsou, strona internetowa Lidovky.cz, https://www.lidovky.cz/domov/ruske-weby-sbiraji-kliky-v-cesku-dezinformacni-stranky-ale-na-vrchnich-prickach-vubec-nejsou.A190816_190321_ln_noviny_rkj, accessed on: 17.07.2024.

[8] Rusko se pokusilo zabránit zvolení Petra Pavla. Šířilo o něm lživé video, soudí ministerstvo vnitra, strona interntowa Forum.24.cz, https://www.forum24.cz/rusko-se-pokusilo-zabranit-zvoleni-petra-pavla-sirilo-o-nem-lzive-video-soudi-ministerstvo-vnitra, dostęp: 18.07.2024.

[9] Souhrn poznatků k českým prezidentským volbám 2023, Ministerstvo Vnitra ČR, https://www.mvcr.cz/chh/clanek/souhrn-poznatku-k-ceskym-prezidentskym-volbam-2023.aspx, accessed on: 17.07.2024.

[10] Telegram je nový dark web. Pro Čechy jde téměř o neomezenou cestu ke konspiračním teoriím, strona internetowa Hlidacipes.org, https://hlidacipes.org/telegram-je-novy-dark-web-pro-cechy-jde-temer-o-neomezenou-cestu-ke-konspiracnim-teoriim/, accessed on: 18.07.2024.

[11] Czechy ujawniają sieć szpiegowską Rosji w UE. Przeszukania także w Polsce [Czechia reveals Russia's spy network in EU. Searches also in Poland], Euractiv.pl, https://www.euractiv.pl/section/polityka-zagraniczna-ue/news/czechy-ujawniaja-siec-szpiegowska-rosji-w-ue-przeszukania-takze-w-polsce/, accessed on: 28.07.2024.

[12] Annual Report of the Security Information Service for 2022, Security Information Service, 2023.

Austria

Martyna Dorda

The Republic of Austria has remained a formally military-neutral country since 1955 under its Constitution and the State Treaty (German: Die Unterzeichnung des Staatsvertrags). Today, this neutrality is becoming increasingly problematic to maintain in the face of international developments [1]. In recent decades, Austria has maintained strong relations with Russia, particularly in economic and industrial sectors. Notably, in 2018, Austria extended its agreement with Russian energy giant Gazprom for gas supplies until 2040. Politically, in 2016, the leader of the Freiheitliche Partei Österreichs (FPÖ, or Freedom Party of Austria) signed an agreement to co-opt the ruling Russian political party, United Russia (Единая Россия, Jedinaja Rossija). Despite this, when Russia invaded Ukraine in 2022, Austria officially maintained a neutral stance, particularly in military terms. Some FPÖ politicians even advocated for a complete dissociation from the conflict. However, as an EU member state, Austria complied with sanctions against Russia proposed by the European Union [2]. The Austrian government also recognized some Russian diplomats as persona non grata and in the later months of 2022 and 2023 expelled as many as 8 diplomats for behavior incompatible with their diplomatic status [3]. Despite this, Austria remains in close economic and industrial relations with Russia in terms of Russian gas imports and with Austrian companies still operating in Russia.

Russia had been engaging in hybrid actions against Austria long before 2022. Notably, in 2014, prior to the annexation of Crimea by Russian forces, there was an increasing presence of campaigns promoting the concept of a Greater Russia within the online space.

1 After 2014, Russian hybrid activities in Austria were particularly evident in the form of cyberattacks. In May 2023, following the leak of the so-called “Vulkan files,” [4] the Bundesministerium für Inneres (BMI - Ministry of the Interior) issued an announcement that it had registered an increased number of Russian cyberattacks since the Russian invasion of Ukraine began. Despite the information contained in the “Vulkan files” on Russian disinformation campaign strategies and hacking attacks by the Sandworm group, the ministry pointed out that there is no more accurate information there that would be helpful, and announced that: “Companies and authorities must continue to invest in their IT security and protect themselves from potential attacks” (own translation) [5].

2 Austrian websites are not as frequent a target for Russian troll factories or bots, but portals that spread pro-Russian disinformation still emerge in the virtual space. One example is the blog "Ukrainian Expat," which appears in targeted ads on platforms like X (formerly Twitter) from users around Vienna who follow legitimate news portals. The alleged author of the blog, "Anna," is a Russian-speaking Ukrainian currently living in Serbia. She claims to engage critically with events in her homeland, but uses Russian propaganda language. For instance, she writes about the "persecution of ethnic Russians" in Ukraine since the 2014 Donbas war. The blog’s source code reveals the use of a "geotargeting plugin," indicating that the content is tailored to the recipient’s location [6]. Such accounts are often suspended or disappear from online platforms, only to reappear in a new form after some time.

3 Jan Marsalek, of Austrian descent, was a key figure in one of the largest financial scandals in German history. As a member of the board of directors of Wirecard, he was responsible for overseeing the company's international operations, particularly in the Asia-Pacific region, where massive financial fraud took place. In 2020, Wirecard declared bankruptcy when it was discovered that €1.9 billion was missing from its balance sheets. Marsalek was suspected of being involved in falsifying financial records and facilitating the movement of funds. After the scandal broke, Marsalek fled and is believed to have gone into hiding in Russia or Belarus, where he reportedly maintained contacts with Russian intelligence services.

In 2023, The Wall Street Journal reported that Marsalek had worked as an agent for Russian intelligence for nearly a decade. His activities reportedly included supporting the Wagner Group and providing Moscow with information on German intelligence services. Western intelligence agencies believe that while heading Wirecard, Marsalek helped organize payments for Russia's military intelligence services (GRU) and foreign intelligence services (SVR), and provided them with details about Wirecard's clients, which included German intelligence services and the Bundeskriminalamt (BKA). Additionally, Marsalek is accused of being involved in the reconfiguration of Yevgeny Prigozhin's business empire in Africa..

4 Austria recognizes disinformation as one of Russia's hybrid action techniques. After the invasion of Ukraine, along with other countries, the EU decided against halting the broadcasting activities of Russian state media on its territory. Even before that, Russian portals were spreading messages aimed at controlling the narrative against Russian imperialist actions, including on the following topics:

-Portraying Russia and Ukraine as historically one country,
-Allegedly exposing the Russian-speaking population in Donbas to atrocities by Ukrainians,
-Calling the invasion and war a "Special Operation" aimed at denazification of Ukraine [7].

Countermeasures

1. Due to growing global threats and Russian hybrid activities, the Austrian government has decided to revise its die nationale Cyber-Sicherheitsstrategie (ÖSS - National Cybersecurity Strategy) for the first time in 10 years. Austria's cybersecurity efforts now focus on early detection of threats and preventing them from escalating [8].

2. Austrian Defense Minister Klaudia Tanner wants to strengthen the country's defenses not only against military attacks, but also against hybrid attacks[9]. A similar stance is taken by a document that is an Austrian analysis of international security policy Risikobild 2024 - Welt aus den Fugen [10].

3. Austrian institutions, both governmental and from the third sector, conduct research and studies on Russia's hybrid activities, are involved in the publication of thematic reports and conduct fact-checking against disinformation. Among others, the Austrian Center for Intelligence, Propaganda and Security Studies (ACIPSS), or the Austria Instituts für Europa- und Sicherheitspolitik (AIES).

Despite Austria's military neutrality and internal disagreements over its stance in response to Russian aggression, the Austrian government is clearly aware of the hybrid threats posed by Russia. However, Austria continues to import Russian gas and allow business dealings with Russia, despite actions such as expelling Russian diplomats and imposing sanctions. This creates a noticeable dualism in Austria's policy toward Russia, marked by a lack of consistent and decisive action.

Bibliography

[1] D. Imwinkelried, Wehe den Kritikern, die Österreichs Neutralität infrage stellen, NZZ.ch, https://www.nzz.ch/international/oesterreich-der-ukraine-krieg-und-die-neutralitaet-ld.1733922, accessed on: 18.07.2024.

[2] Auswirkungen des Konflikts in der Ukraine auf Österreich, verteidingungspolitik.at, https://verteidigungspolitik.at/auswirkungen-des-konflikts-in-der-ukraine-auf-%C3%96sterreich, accessed on: 18.07.2024.

[3] Österreich weist zwei russische Diplomaten aus, Zeit.de, https://www.zeit.de/politik/ausland/2024-03/oesterreich-russland-diplomaten-ausgewiesen-spionage, accessed on: 28.07.2024.

[4] 'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics, The Guardian, https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics, accessed on: 29.07.2024.

[5] Innenministerium: Vermehrt russische Cyberangriffe, strona internetowa Saltsburgen Nachrichten, https://www.sn.at/politik/innenpolitik/innenministerium-vermehrt-russische-cyberangriffe-136440850, accessed on: 29.07.2024.

[6] J. Denkmayr, J. Melchar, Russische Fake News erreichen Österreich, Kleine Zeitung, https://www.kleinezeitung.at/politik/aussenpolitik/18219147/mutmassliche-russische-fake-news-nun-auch-in-oesterreich, accessed on: 29.07.2024.

[7] M. Zinkanell, Die russische hybride Kriegsführung. Im Kontext des Angriffskriegs gegen die Ukraine, AIES Austrian Institute for European and Security Policy STUDY, Bundesministrum Landesverteiding, No. 2023/3, 2023.

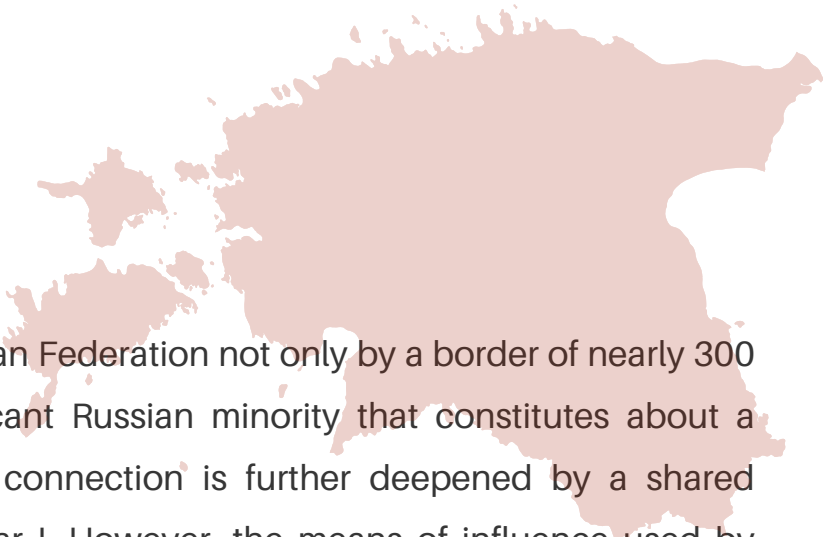
[8] Bundeskazleramt, Österreichische Sicherheitsstrategie, bundeskazleramt.gv.at, https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/sicherheitsstrategie.html, accessed on: 29.07.2024.

[9] L. Mahnke, Risiko 'sehr hoch': Österreich warnt vor Angriff aus Russland, Merkur.de, https://www.merkur.de/politik/konfliktherde-oesterreich-bundesheer-bericht-risikobild-warnung-frieden-krieg-verteidigung-zr-92804346.html, accessed on: 29.07.2024.

[10] Bundesministerium für Landesverteidigung (BMLV), Risikobild 2024 – Welt aus den Fugen, 2024.

Estonia

Antonina Sołtysiak



Estonia is connected to the Russian Federation not only by a border of nearly 300 kilometers but also by a significant Russian minority that constitutes about a quarter of the population. This connection is further deepened by a shared history, dating back to World War I. However, the means of influence used by Russia today are vastly different from those employed over a century ago. With technological advancements, cyberattacks have become a prominent tool, and Russia has developed a cadre of highly skilled hackers capable of breaching the systems of many countries, including government websites. Estonia, too, has been a target, with historical ties from the Soviet era often serving as a point of contention and a justification for attacks. The catalyst for future cyber assaults came in 2007, when Russia launched its first major cyberattack against Estonia's internet infrastructure.

In response to the 2007 cyberattacks, Estonia rapidly developed its cybersecurity infrastructure. Today, it is regarded as one of the most advanced countries in terms of digital defense and is largely immune to external cyber threats. Additionally, the NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn in 2008, further solidifying Estonia's leadership in cybersecurity in Europe. This robust cybersecurity framework proved invaluable, particularly after the outbreak of the war in Ukraine. Russia has since intensified its hybrid operations, not only targeting the front lines but also focusing on countries that openly support Ukraine. While hybrid threats have become a constant challenge, Estonia has managed them effectively. Despite the frequency of these attacks, they do not disrupt the daily lives of Estonians, as they are continually repelled and often remain unseen.

In **April 2007**, following the Estonian government's decision to relocate a Soviet soldier monument from downtown Tallinn to a military cemetery, widespread protests erupted, primarily led by pro-Russian activists. The situation escalated on April 27, when a series of massive cyberattacks targeted government and public websites. The attacks, which lasted for 22 days, mainly involved denial-of-service (DDoS) tactics, restricting access and flooding sites with spam. In response, the Estonian government took the unprecedented step of closing the country's digital borders, limiting traffic to its websites. This marked the first significant cyberattack on Estonia's national security, highlighting the vulnerability of critical digital infrastructure [1].

In **August 2022**, Estonia faced a massive cyberattack targeting around 200 government and private institution websites. The attack followed the Estonian government's decision to move a historic Soviet Tu-34 tank from the center of Narva to the Estonian Military Museum. This decision sparked protests, particularly from the Russian minority in Estonia, who felt that the relocation was an attempt to "blur" a piece of history. In response, the Russian hacking group Killnet launched a cyberattack that primarily aimed at disrupting access to various websites and compromising data flow. While the attack caused significant inconvenience by impeding website access, it did not result in major damage or data breaches [2].

September 2023 Distributed Denial-of-Service (DDoS) attack on the website of Estonian rail carrier Elron. At the time of the attack, the site was down for 24 hours, making it impossible to purchase tickets both online and on the train [3].

4. March 2024 - An attack by Russian hackers on Estonian government websites, including The Police and Border Guard Board, The Tax and Customs Board and the Ministry of Justice. The attack, which lasted for two days, made it much more difficult to access many official sites for many basic matters, such as filing documents. Estonia, however, thanks to its advanced computer security measures, quickly dealt with the problem, and the attack did not cause any permanent damage to the system [4].

Countermeasures

1. Establishment of Estonia's “data embassy” in Luxembourg [5].

2. The Estonian government has invested in and nurtured education and programs for children over the years to familiarize them with technology. Such programs are also in place for older people. Tallinn is betting on education and preparing the public to quickly detect and deal with manipulation [6].

3. Establishment of the Estonian Department of Information System (RIA)

Bibliography

[1] How a cyber attack transformed Estonia, BBC News, https://www.bbc.com/news/39655415, accessed on: 29.07.2024.

[2] Estonia repels cyberattacks claimed by Russian hackers, Al Jazeera, https://www.aljazeera.com/news/2022/8/18/estonia-says-it-repelled-cyber-attacks-claimed-by-russian-group, accessed on: 29.07.2024.

[3] RIA on Elron cyberattack: It is likely that it will happen again, ERR News, https://news.err.ee/1609108433/ria-on-elron-cyberattack-it-is-likely-that-it-will-happen-again, accessed on: 29.07.2024.

[4] Massive cyberattack on Estonian gov't institutions, TVP World, https://tvpworld.com/76379715/estonian-govt-institutions-targeted-in-largest-cyber-attack-in-countrys-history, accessed on: 29.07.2024.

[5] Data Embassy- e- Estonia, e- Estonia, https://e-estonia.com/solutions/e-governance/data-embassy/, accessed on: 29.07.2024.

[6] How Russian threats in the 2000s turned Estonia into the go-to expert on cyber defense, CNN Business, https://edition.cnn.com/2021/06/18/tech/estonia-cyber-security-lessons-intl-cmd/index.html, accessed on: 29.07.2024.

Financed by the National Institute of Freedom
under the Solidarity Corps program –
Support for volunteer organizations in NGOs.

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

NIW
Narodowy Instytut Wolności
Centrum Rozwoju Społeczeństwa Obywatelskiego

Program Wspierania i Rozwoju Wolontariatu Długoterminowego na lata 2018–2030
Korpus Solidarności