Received: 15.3.2023 Accepted: 15.5.2023 Published on-line: 25.6.2023
Available from: www.obranaastrategie.cz doi: 10.3849/1802-7199.23.2023.01.049-073

ONE THREAT - MULTIPLE RESPONSES
Countering Hybrid Threats in V4 Countries

JEDNA HROZBA - VÍCE ZPŮSOBŮ REAKCE
Čelení hybridnímu působení v zemích V4

Josef Procházka[a], Pavel Vinkler[b], Krisztián Jójárt[c], Zoltán Szenes[d], Artur Gruszczak[e], Matej Kandrík[f]

Abstract

The new dynamics in the global security environment accompanied by the renewal of great power competition and its impact on security provision of Central European countries brought new challenges, especially in countering hybrid threats. The article embraces the outcome of a multilateral research analysing countering hybrid threat policies in the Czech Republic, Hungary, Poland, and Slovakia. The goal of the article is to discuss and explain the four nations' policies towards the mitigation of the hybrid challenges and their complexity. Those national approaches are comprehensively assessed in four case studies and their main commonalities and key differences are discussed. The conclusion is that although the V4 countries have the same conceptual theoretical basis, the policies against the hybrid threat differ. The authors propose more efficient way ahead at the national level and the improvement of coordination between the V4 countries.

Abstrakt

Nová dynamika v globálním bezpečnostním prostředí doprovázená obnovením velmocenské konkurence a její dopad na bezpečnost středoevropských zemí přinesly nové výzvy, zejména v čelení hybridním hrozbám. Tento článek přináší výstupy multilaterálního výzkumu analyzujícího politiku čelení hybridnímu působení v České republice, Maďarsku, Polsku a na Slovensku. Cílem článku je diskutovat a vysvětlit politiky čtyř národů v rámci této oblasti

[a] University of Defence, Brno, Czech Republic
E-mail: josef.prochazka@unob.cz. ORCID: 0000-0001-8180-397X.
[b] Charles University, Prague, Czech Republic
E-mail: vinkler.pav@gmail.com. ORCID: 0000-0003-2795-7518.
[c] University of Public Service, Budapest, Hungary
E-mail: jojart.krisztian@gmail.com.ORCID: 0000-0002-3172-3274.
[d] University of Public Service, Budapest, Hungary
E-mail: szenes.zoltan@uni-nke.hu. ORCID: 0000-0003-1686-2273.
[e] Jagiellonian University in Kraków, Poland
E-mail: artur.gruszczak@nj.ed.pl. ORCID: 0000-0002-3450-8377.
[f] Strategic Policy Institute, Bratislava, Slovakia
E-mail: kandrik@stratpol.sk. ORCID: 0000-0001-8265-0960.

a jejich složitosti. Tyto národní přístupy jsou komplexně hodnoceny ve čtyřech případových studiích a jsou diskutovány jejich hlavní společné rysy a klíčové rozdíly. Závěrem je, že ačkoli země V4 mají stejný koncepční teoretický základ, jednotlivé politiky se liší. Autoři navrhují efektivnější postup na národní úrovni a zlepšení koordinace mezi zeměmi V4.

Keywords

Hybrid threats; Czech Republic; Hungary; Poland; Slovakia; national policies; crisis management system.

Klíčová slova

Hybridní působení; Česko; Maďarsko; Polsko; Slovensko; národní politiky; systém krizového řízení.

Introduction

The strategic proximity of the Visegrad four nations (V4) is underlined by close collaboration within the group established in February 1991 in the aftermath of the democratization process in this region. Their common interests, when seeking cooperation in the areas of NATO and EU, were in the heart of the project in that time.[1] Moreover, there is a legacy of some similarities in history, strategic culture, and state functioning. Additionally, all V4 nations are developed countries and enjoy favourable level of security. According to the Global Peace Index, Czech Republic ranked 8th, Hungary 13th, Poland 25th and Slovakia 25th among 163 countries.[2] Perhaps this relative prosperity and security also contributes to the fact that the V4 countries' policy against hybrid threats is not as advanced as the security environment, especially Russia's aggressive threat, would justify.

In terms of hybrid threats, V4 countries adopted the NATO strategy on countering hybrid threats in 2015.[3] They also implement the joint framework on countering hybrid threats: a European Union Response.[4] All V4 nations support and benefit from the developing cooperation between the EU and NATO, with no less than 74 common actions stipulated in the framework of the three Joint Declarations of 2016, 2018, and 2023.[5] The EU has taken important steps to improve its capacity to counter hybrid threats and enhance the EU's resilience, including by introducing chemical and cyber sanctions regimes. It has strengthened cooperation with NATO on hybrid and cyber security as well. Moreover, member states are pooling intelligence through the Hybrid Fusion Cell. All V4 countries are involved in the activities of the European Centre of Excellence for Countering Hybrid Threats in Helsinki established as an outcome of 2016 EU Joint Framework for Countering Hybrid Threats.[6] All these elements create favourable conditions for identification and sharing valuable lessons especially at the policy level decision making among those four nations. Both security and defence provisions in general and countering hybrid challenges in particular have a significant potential to benefit from these experience and knowledge.

[1] USIAK, Jaroslav: Visegrad Group as Institution for Central European Cooperation: Ups and Downs of Small International Organisations. Revista Unisci, 2020, vol. 54, October, pp. 9-28.

[2] Global Peace Index 2022: *Measuring peace in a complex world*. Institute for Economics and Peace (IEP), Sydney. [online] [cit.2023-11-03] Available from: https://search.issuelab.org/resource/global-peace-index-2022-measuring-peace-in-a-complex-world.html

[3] RÜHLE, Michael and ROBERTS, Clare: Enlarging NATO's toolbox to counter hybrid threats. *NATO Review*, 19 March 2021. [online] [cit.2023-11-03] Available from: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html

[4] European Commission (2016): *Joint communication to the European parliament and the Council. Joint Framework on countering hybrid threats: a European Union response*. [online] [cit.2023-11-03] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

[5] The European Union's Global Strategy Three Years On, Looking Forward. [online] [cit.2023-11-03] Available from: https://www.eeas.europa.eu/sites/default/files/eu_global_strategy_2019.pdf

[6] Finnish Government (2017): *European Centre of Excellence for Countering Hybrid Threats established in Helsinki*. [online] [cit.2023-11-03] Available from: https://valtioneuvosto.fi/en/-/10616/eurooppalainen-hybridiuhkien-osaamiskeskus-perustettiin-helsinkiin

Research Objective

The research objective is to assess the states' policy approach towards countering hybrid threats in V4 countries. The article aims at examining strategies and relevant secondary documents in terms of convergence between strategic approaches to hybrid threats and policy responses worked out by state actors in each V4 country. It applies deductive reasoning to test the following tentative argument (a research hypothesis): V4 states share a common position on hybrid threats at the strategic level yet differ over ways and means of effective coping with those threats, especially on the level of national security institutions and crisis management systems.

We use the Hybrid CoE's definition as a basis for our research: "The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military terms." We were inspired by John Gerring's case study concept[7] to validate a research hypothesis focusing on conceptualization, measurement, causality, and policy documents research. We choose the V4 countries as four cases and use mainly the descriptive method of analysis helping identify commonalities and different approaches in countering hybrid threats at the policy level. The rationale behind source selection was led by the anticipated purpose of the analysis, which is to develop a strategic overview of V4 countries national approaches to countering hybrid threats. Thus, in the first round of collecting data, all security strategic documents of all four states were considered, to provide the basic understanding of the cases. Consequently, in the second round, various documents, both primary and secondary, providing context behind the identified approaches were studied, including legislative documents of the countries, scientific journals and media articles accessible via internet. In some cases, interviews were used as well. This research also employs an interpretive political analysis approach.[8] It is based on a qualitative content analysis of official documents issued in V4 states in the years 2013–2022. Those documents embrace strategies (general and sectoral), relevant legal acts, reports of competent state institutions, and official statements. Content samples were carefully selected according to their concurrence with the three key variables and in conjunction with hybrid threats.

In the explanatory part of the research, the comparative analysis method served as an inspiration. The comparative framework of Muray and Viotti[9] for defence policy analysis allowed to establish two comparative criteria which served as a baseline for our research: (1) threat perception and strategic approach towards countering hybrid threats; (2) crisis management system with a focus on countering hybrid threats. We place these two key variables in a strategic security environment to get better understanding in each case. Moreover, in the final discussion we have decided to compare our findings in six areas: (1) perception of a hybrid threat, (2) strategy approach, (3) policy approach, (4) institutional arrangement, (5) approach towards cyber domain and (6) whether there were any comprehensive security reviews conducted in the analysed countries.

[7] GERRING, John: *Case Study Research. Principles and Practices*. Cambridge University Press, 2007.

[8] SCHWARTZ-SHEA, Peregrine and YANON, Dvora: *Interpretive Research Design: Concept and Process*. New-York, Abington. Routledge, 2013.

[9] MURRAY, Douglas, J. - VIOTTI, Paul V.: Introduction. In Murray, Douglas, J. – Viotti, Paul V. (eds.): *The defense policies of nations: a comparative study*. Baltimore: The John Hopkins University Press, 1994. pp. xviii-xxiv.

Firstly, by perception of hybrid threat we understand how the V4 countries are defining hybrid threats in their government level strategic and conceptual documents. In our research, we have analysed all still valid security related strategic documents. Secondly, by strategic approach we mean whether there were any specific government level strategies or conceptual documents approved in V4 countries in last years, focusing directly on the topic of countering hybrid interference. The timeframe here starts in 2014, when the agenda of countering hybrid interference started to be emphasized. In the policy approach part we focus on what are the main approaches described by V4 countries in their government level security documents that might be considered, in line with the definition of the Hybrid CoE, as a way to counter hybrid interference. The timeframe again starts in 2014. In the institutional arrangement part we describe what are the main institutions on the strategic level tasked to deal with countering hybrid interference. The approach towards cyber domain was identified as a separate comparison area because the cyber domain is usually considered as a part of the wider hybrid continuum, however, due to historical developments it has evolved into a separate policy agenda. Given this context, we were interested how the cyber domain is approached in V4 countries on the policy level.

Finally, by the comprehensive security reviews we mean documents on the strategic level (approved by government), which aim to asses vulnerabilities in the security system of the analysed countries as a whole. Their existence is an important signal of horizontal approach towards security policy because of the comprehensive and multidomain nature of hybrid threats. We considered only documents released after 2014.

The analysis scope is constrained by the extent of the scientific article. Further research might focus also on other aspects of states' policy, e. g., the cooperation and support of the state to non-state organizations often considered as important actors for countering hybrid threats policy.[10] However, the two chosen criteria set the baseline, which, if missed, would leave the rest of the states' activities broadly ineffective.

Literature Review

It is important to emphasize the relevance of the research in the context of other studies. As explained further in the text, the topic of countering hybrid threats, although by far not new, became highly visible after the Russian aggression against Ukraine in 2014. Despite this fact and despite gradual development of national policies in this area, dedicated research focusing on the approach of the V4 countries is limited. One of the existing examples is the study by Mareš and Paďourek,[11] who are dealing with threats of the Russian influence and terrorism in V4 countries. The authors focus on threats perception, analysing national security strategies. The study is important in its wide approach, looking at all V4 countries together. However, despite the fact that the Russian influence is one of its topics, it does not assess the institutional set up and does not provide further context in this area, since it is not its aim.

[10] WIGEL, Mikael: Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. *International Affairs*, 2019, vol. 95, no. 2, pp. 255 – 275.

[11] MAREŠ, Miroslav and PAĎOUREK, Jan: The Threats of Russian Influence and Terrorism within National Security Strategies of the Visegrad Four, *The Journal of Slavic Military Studies*, 2020, vol. 33, no. 2.

We can also find relevant studies looking directly at national perspectives of the problem. These texts, however, often focus only on one part of the hybrid spectrum. A good example is the work of Václav Štětka, Jaromír Mazák, and Lenka Vochocová, focusing on the disinformation sphere in the Czech Republic.[12] The authors describe threats in the information domain and also touch some of the institutional problems the state has with countering disinformation. Similarly, we can find a partial information on countering hybrid threats in Slovakia in the study by Kira Harris focusing on the threat of the Night Wolfs Motorcycle club, which is one of the tools in the Russian hybrid toolbox.[13] Thirdly, we can mention the study of Aleksandra Gasztold and Przemysław Gasztold, who analyse Polish counter terrorism system from the point of view of its usefulness for countering also hybrid threats.[14]

The aim of all of the mentioned studies was to look at one specific aspect of the hybrid threats continuum, however, there is so far no research available comparing the situation in all four countries of the V4 and trying to understand local differences. Thus, given the limited amount of research, the value of the article is that it brings a detailed overview and comparison of V4 countries approaches and their development in last years. The overview provided by this research can serve as a basis for further work in this field.

Although the article does not cover the developments of the Russian military invasion in Ukraine in 2022, we refer to it when possible during the discussion of the hybrid threat theory.

From Hybrid Threats to Hybrid War: Conceptual Basis

The problem of hybrid threats first appeared in the military literature, which immediately gave the war (only military) dimension a broader interpretation of the concept. These approaches mainly focused on the military "means" side of the strategic formulation, as the hybrid threat theory began to gain civil attention in the international literature after the Russian involvement in the 2016 American elections.[15] One of the first mentions of hybrid warfare in scholarly literature can be found in William J. Nemeth's thesis titled Future war and Chechnya: a case for hybrid warfare.[16] Nemeth works with the idea of a so-called hybrid society combining various traits of modern and premodern societies. These can be found in devolving states characterized by a high level of violence, instability, and a mixture of

[12] ŠTĚTKA, Václav, MAZÁK, Jaromír, & VOCHOCOVÁ, Lenka: Nobody Tells us what to Write about: The Disinformation Media Ecosystem and its Consumers in the Czech Republic. *Journal of the European Institute for Communication and Culture*. 2021, vol. 28, no. 1.

[13] HARRIS, Kira: A Hybrid Threat: The Night Wolves Motorcycle Club, *Studies in Conflict & Terrorism*. 2021.

[14] GASZTOLD, Aleksandra and GASZTOLD, Przemysław: The Polish Counterterrorism System and Hybrid Warfare Threats, *Terrorism and Political Violence*. 2022, vol. 34, no. 6.

[15] POMERANTSEV, Peter and WEISS, Michael: *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Interpreter, Institute of Modern Russia, 2019. [online] [cit.2023-11-03] Available from: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf ; ROGOZIŃSKA, Agnieszka: Non-military dimension of the hybrid war in Ukraine. *Środkowoeuropejskie Studia Polityczne*, vol. 2, June 2019, pp. 173-194.

[16] NEMETH, William J.: *Future War and Chechnya: A Case for Hybrid Warfare*. Naval Postgraduate School, 2002.

societal and religious relations typical for traditional and modern societies. Hybrid societies are engaged in hybrid warfare, which Nemeth explores through a case study of the Chechen insurgency during the first and the second war in Chechnya. This leads to his understanding of hybrid warfare as a specific form of total guerilla warfare.[17]

By analysing the 2006 Lebanon war and military thinking on modern warfare of the late 1990s and early 2000s, Frank G. Hoffman constructed his concept on hybrid war. He incorporates a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.[18] Hoffman defines hybrid threat as purposeful and tailored violent application of advanced conventional military capabilities with irregular tactics, terrorism and criminal activities, or combination of regular and irregular forces, operating as part of a common design in the same battlespace. In his own words, he was intellectually influenced by concepts such as the fourth generation of warfare, netwars, compound wars or Chinese "three warfares" (legal, psychological, and media) approach. Hoffman's conceptualization of both hybrid warfare and hybrid threat can be understood as a challenge on the military-operational level rooted in transforming the broader battlefield environment.[19]

Not widely known is the fact that NATO elaborated on hybrid threats prior to the Ukrainian crisis in 2010. In the Bi-Strategic Command Input to a New NATO Capstone Concept, we can find the following definition: "*Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and unconventional means adaptively in pursuit of their objectives.*"[20] While Hoffman's work triggered a rather rich discussion and received a fair portion of praise and criticism in the following years, concepts of hybrid threats and war reached a new level of significance since the 2014 events of the Russian annexation of Crimea and subsequent war in eastern Ukraine, and particularly in the current Russian and Ukrainian war. For instance, the US National Military Strategy 2015 formally accepted the hybrid conflict and threats as part the conflict continuum.

According to Fridman, since the mid-2000s, three major and different phenomena have been titled as a hybrid war. The first one is the original Hoffman's concept covering the operational level of incorporation of various conventional and unconventional warfare modes. The second one is the NATO's understanding of hybrid war as a threat continuum, including conventional and unconventional methods, mixing hard and soft power. The third one is the Russian conceptualization of hybrid warfare (gibridnaya voyna).[21] Hybrid warfare in its original sense (i.e., as it was understood by Frank G. Hoffman and others) was seldomly discussed in the Russian military literature before 2014. Gibridnaya voyna gained momentum, however, after it had become the preferred term of Western observers to label the Russian politics after 2014. Despite of (or maybe due to) the Western claims that the Kremlin is conducting hybrid warfare against Ukraine and others, Russian scholarly works and

[17] Ibid.

18 HOFFMAN, F. G.: *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007.

[19] FRIDMAN, Ofer: Russian "Hybrid Warfare": Resurgence and Politicization. New York/Oxford: Oxford University Press, 2018.

[20] NATO: *NATO's Warfighting Capstone Concept*. 2010. [online] [cit.2023-11-03] Available from: https://www.act.nato.int/nwcc

[21] FRIDMAN, Ofer: *Russian "Hybrid Warfare": Resurgence and Politicization*. New York/Oxford: Oxford University Press, 2018.

statements of prominent Russian political and military figures are consistent in the regard that it is the West, not Russia, which uses a hybrid strategy.

Nevertheless, both the Russian and the Western understandings concur that the hybrid warfare's centre of gravity lies not in the military domain but in a wide spectrum of non-military spheres.[22] Hybrid war in the Russian perspective however – while it clearly foresees the limited and covert use of military force in the early period of the conflict – can take the form of an open military confrontation, as we witness in the war in Ukraine today.

The Czech Republic's Response to Hybrid Threats

Threat perception and strategic approach towards countering hybrid threats

In the Czech Republic, countering hybrid threats became an indispensable part of the security policy discourse after the annexation of Crimea and beginning of the war in eastern Ukraine in 2014.[23] As a reaction to the paradigm shift in the security environment, the government approved the Security Strategy of the Czech Republic 2015. It emphasizes new trends in security environment including hybrid threats, when it states that *"threats to the security of allies may be of the classical military nature or they may take the vague form of hybrid warfare."* Moreover, the strategy mentions the hybrid issue as one of the main threats the country will face in the future, stating that *"some states seek to achieve a revision of the existing international order and are ready to pursue their power-seeking goals through hybrid warfare methods."*[24]

The document understands hybrid threats as a combination of conventional and non-conventional military means with non-military tools (propaganda using traditional and new media, disinformation intelligence operations, cyber-attacks, political and economic pressures, and deployment of unmarked military personnel). It attributes it both to state and non-state actors seeking to carve out for themselves exclusive spheres of influence by means of destabilizing the neighbouring countries and taking advantage of local conflicts and disputes.[25]

Since the adoption of the new Security Strategy, the issue of hybrid threats has become part of every strategic security document, stressed in the chapters that describe trends in the security environment. For example, the Defence Strategy 2017 recognizes that Russia has executed hybrid operations against NATO nations and EU Member States, including targeted disinformation activities and cyber-attacks.[26]

[22] SCHMID, Johan: Hybrid warfare on the Ukrainian battlefield: developing theory based on empirical evidence. *Journal of Baltic Security*. 2019. No. 1.

[23] PROCHÁZKA, Josef, KARAFFA, Vladimír, FRANK, Libor, Adaptace obranné politiky a strategie ČR na nové bezpečnostní hrozby, *Vojenské rozhledy*, 2015. Vol. 24 (56), No. 3, pp. 8–2.

[24] Ministry of Foreign Affairs of the Czech Republic. *Security Strategy of the Czech Republic. 2015.* [online] [cit.2023-11-03] Available from: https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf

[25] Ibid.

[26] Ministry of Defence of the Czech Republic. *The Defence Strategy of the Czech Republic*. 2017. [online] [cit.2023-11-03] Available from: https://www.army.cz/images/id_8001_9000/8503/DefenceStrategy2017.pdf

Despite not being specifically mentioned, aspects of hybrid threats are also part of the annual report of the Czech Republic's intelligent service Security Information Service – BIS. E.g., in its public report from 2020, the BIS describes current Russian actions as "*often unconventional concepts when pursuing its interests*".[27] Similar approach is used in the 2021 report.[28] It describes the tools Russia uses in the Czech Republic, which are usually considered to be part of the hybrid interference toolbox (e.g., cyber-attacks, influencing of Russian-speaking community, spreading manipulative information). BIS mentions some of these tools in connection with the activities of the People's Republic of China as well.

As a direct reaction to the worsening security situation in Europe, the Czech Government conducted a comprehensive audit of the state of national security. The outcome in its public version released in 2016 covers 10 areas pointed out as the potentially most vulnerable. One of these chapters also addresses hybrid threats.[29] As a follow-up on tasking based on one of the actions from the consecutive action plan, the Ministry of Defence was invited to elaborate a stand-alone strategy on countering hybrid threats. The main objective was to outline a comprehensive policy document for the whole government response to this threat complexity. The document was approved by the government in April 2021. It provides a necessary conceptual framework for the elaboration of an action plan to implement measures accordingly.[30] The action plan was approved by the government on November 22, 2021. It translates the principles of the strategy into a specific set of actions aiming towards: (1) enhancement of the resilience of state, society and its critical infrastructure, (2) strengthening coordination between state institutions, and (3) further developing states' reaction capabilities. The plan should be implemented by the end of 2023, when its review and possible update can be expected.

Crisis management system: is hybrid considered?

The state's basic duty is to ensure the Czech Republic's sovereignty and territorial integrity, the protection of its democratic foundations, and the protection of lives, health, and property.[31] The security of the Czech Republic is ensured by its armed forces, the armed security corps, rescue corps, and emergency services. State authorities, bodies of the self-governing territorial units, and private companies and individuals are obliged to participate in safeguarding the Czech Republic's security.

The Czech Republic exercises a holistic approach to its security as the evolving security environment has become more challenging and complex in recent years and the line between peace and war continues to blur, with disinformation and subversion posing serious challenges and driven in part by new and emerging technologies. The 2017 Defence Strategy provides a unifying framework for strengthening and securing the defence of the Czech

[27] BIS: Annual Report of the Security Information Service for 2019. 2020. [online] [cit.2023-11-03] Available from: https://www.bis.cz/public/site/bis.cz/content/vvz-2019-web-en-k-publikaci.pdf

[28] BIS: Annual Report of the Security Information Service for 2020. 2021. [online] [cit.2023-11-03] Available from: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf

[29] Ministry of Interior of the Czech Republic (2016): *National Security Audit*. [online] [cit.2023-11-03] Available from: https://www.mvcr.cz/cthh/soubor/national-security-audit.aspx

[30] Ministry of Defence of the Czech Republic. *National Strategy for Countering Hybrid Interference*. Praha, 2021. [online] [cit.2023-11-03] Available from: https://mocr.army.cz/assets/informacni-servis/zpravodajstvi/national-strategy---aj-final.pdf

[31] Constitutional Act No. 110/1998 on the Security of the Czech Republic

Republic and the Armed Forces' capability and capacity. At the same time, it creates a solid groundwork necessary for enhancing the overall resilience of the government bodies and agencies, local administration and citizens against the negative impacts of the unstable security environment.

The primary function of the national defence system is to prepare, manage, coordinate, and support activities of the relevant authorities, forces, and assets to ensure the defence of the Czech Republic. This includes early detection, prediction, and evaluation of potential threats, including hybrid threats.[32] The main authority responsible for conducting the security policy of the Czech Republic is its government. Within the structure of the government office, the National Security Council (BRS) is established. It is a standing body of the government responsible for the coordination of the Czech Republic's security.[33] It consists of the Prime Minister, who is also the Chair of the Council, Minister of Interior, Minister of Defence, Minister of Foreign Affairs, Minister of Industry and Trade, Minister of Transport, Minister of Health, and Minister of Agriculture.[34]

One of the outcomes of the National Security Audit was the establishment of the dedicated working group (WG) by the BRS focusing on countering hybrid threats on 8 March 2017. The members of the WG are all from the ministries which have seats in the BRS. In addition, representatives of the Secretariat of the BRS, Czech National Bank, State Office for Nuclear Safety, National Cyber and Information Security Agency, Security Information Service, Office for Foreign Relations and Information, Military Intelligence, the Police of the Czech Republic, and the Military Attaché to the Government Office are involved. The WG represents a platform for an interdepartmental exchange of information and the coordination of countering hybrid threats.[35] The WG was further enhanced on 19 October 2021, when the BRS established the position of the coordinator for countering hybrid interference who formally became the chairman. Thanks to these changes, the responsibilities in the agenda of countering hybrid interference at strategic level were clarified and formalized. The WG can now adopt its conclusions based on the approval of more than half of all its members. Those can serve as the recommendations to the Chairman of the BRS (the Prime Minister).

In 2022, one more key actor to the security system coordination was added. The government approved on its meeting on 21 December the establishment of the National Security Advisor (NSA). Its role is to coordinate different agendas within the security system, including countering hybrid threats, when it should closely cooperate with the coordinator for countering hybrid interference. In February 2023, the NSA was also tasked with coordinating

[32] Ministry of Defence of the Czech Republic. *The Defence Strategy of the Czech Republic*. 2017. [online] [cit.2023-11-03] Available from: https://www.army.cz/images/id_8001_9000/8503/DefenceStrategy2017.pdf

[33] Vláda České Republiky: Usnesení Bezpečnostní rady státu ze dne 19. října 2021 č. 41. [online] [cit.2023-11-03] Available from: https://www.vlada.cz/assets/ppov/brs/pracovni-vybory/hybridni-hrozby/usn-41-21.pdf

[34] Vláda České Republiky: *Statut Bezpečnostní rady státu*. 2018. [online] [cit.2023-11-03] Available from: https://www.vlada.cz/assets/ppov/brs/Statut-BRS-rijen-2018.pdf

[35] Vláda České republiky: Usnesení Bezpečnostní rady státu ze dne 21. prosince 2020 č. 42 ke Změně usnesení Bezpečnostní rady státu ze dne 8. března 2017 č. 9, k Odborné pracovní skupině Bezpečnostní rady státu pro hybridní hrozby. [online] [cit.2023-11-03] Available from: https://www.vlada.cz/assets/ppov/brs/cinnost/zaznamy-z-jednani/usn-42-20.pdf

the agenda of countering foreign information interference.[36] By all these responsibilities, the NSA becomes one of the key actors in the system of countering hybrid threats of the Czech Republic.

At the operational level, the Centre Against Terrorism and Hybrid Threats (CTHH – recently renamed as CHH) was established in 2016 and works within the structure of the Ministry of Interior. Its mission is to provide specialized analytical and communications expertise and monitor threats directly related to internal security, "*which implies a broad array of threats and potential incidents related to terrorism, soft target attacks, security aspects of migration, extremism, public gatherings, violation of public order and different crimes, but also disinformation campaigns related to internal security.*"[37]

Advancement of digitalization of the Czech Republic and hybrid threats create continually growing demands on cyber security. The Government of the Czech Republic enhanced its capability and capacity to protect its interests in increasingly contested cyber domain by several measures. First, the legal system was modernized[38] and national cyber security strategy formulated and updated on regular basis.[39] It allowed to design modern cyber security architecture embracing the formation of the National Cyber and Information Security Agency. Furthermore, the National Cyber Operation Centre and Cyber Forces Command within the Ministry of Defence reinforce the overall Czech Republic cyber domain resilience.

Given the intermixture of internal and external security threats, preparing citizens for national defence calls for a combination of military and civilian approaches. Systematic approach to the preparation of civic population and the reinforcement of societal resilience of the Czech Republic is addressed by the Concept on Defence Preparation of Inhabitants.[40] It supports a wider array of activities with the focus on young population activities including NGOs.

[36] Vláda České republiky: *Agendu bezpečnostních aspektů boje proti vlivům cizích mocností přebírá národní bezpečnostní poradce*. February 15th, 2023. [online] [cit.2023-11-03] Available from: https://www.vlada.cz/cz/agendu-bezpecnostnich-aspektu-boje-proti-vlivum-cizich-mocnosti-prebira-narodni-bezpecnostni-poradce-203036/

[37] Ministerstvo Vnitra České republiky*: Centre Against Terrorism and Hybrid Threats*. 2021. [online] [cit.2023-11-03] Available from: https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx

[38] Parliament of the Czech Republic (2014): Act No 181/2014, on cyber security.

[39] Government of the Czech Republic: *National Cyber Security Strategy of the Czech Republic*. 2021. [online] [cit.2023-12-03] Available from: https://www.nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf

[40] Government of the Czech Republic (2019). *The Concept on Defence Preparation of Inhabitants 2019-2024.* [online] [cit.2023-12-03] Available from: https://mocr.army.cz/images/id_40001_50000/46088/Koncepce_p____pravy_ob__an___k_obran___st__tu_2019-2024.pdf

Hungary's Counter Hybrid Warfare Policy

Threat perception and strategic approach towards countering hybrid threats

Awareness of both the public and the government about the challenge of hybrid warfare emerged slowly in Hungary as the interviews conducted at the Prime Minister's Office, the Ministry of Defence, the Ministry of Foreign Affairs, and the Counter-Terrorism Information and Crime Analysis Centre in 2021 and 2022 have shown. It became evident only after the Russian interference in the US and French presidential elections of 2016 and 2017 that Hungary must protect its sovereignty against foreign destabilization attempts. Although the Hungarian experts[41] quickly recognized the challenge of hybrid warfare following Russia's aggression against Ukraine in 2014, the government did not voice its concern – at least publicly – until 2017. The official perception was that Hungary could become a target of a complex hybrid threat primarily due to its place and role in the alliance system.[42] While only great powers with appropriate potential can pose complex hybrid threats, it cannot be ruled out that certain elements of hybrid threats (e.g., cyberattacks) will challenge Hungary's security. The detection and elimination of hybrid threats is primarily within the national authority, while the international community should be ready to provide help upon request. Due to the complexity of hybrid threats, countering hybrid threats requires a whole-of-government approach, the preparation of society and an integrated defence management system to tackle the problem.

This two-step approach was reflected in the 2020 National Security Strategy (NSS), which defined hybrid warfare as hostile actions below the threshold of war which can destabilize the country, weaken the government's ability to act, break the political stability and the social cohesion and limit the state's capability to pursue its interests internationally (National Security Strategy of Hungary, 2020). The strategy identifies the following hybrid threats: coordinated and widespread (1) diplomatic activity, (2) information and intelligence operations, (3) financial and economic pressure, (4) financial speculative attacks, and (5) military threats coupled with the above. The new National Military Strategy (NMS) of 2021 further specifies hybrid threats, mentioning (1) conscious and active influence of domestic and international public opinion, (2) manipulation of information channels and social media platforms, (3) incitement of social, political, and economic instability, (4) taking advantage of crises, and (5) the use of military and economic-financial aid as a tool to exert pressure and influence[43] (para 68).

[41] PORKOLÁB, Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? (Hybrid Warfare: a new form of warfare or an old acquaintance?) *Hadtudomány (Hungarian Military Science)*. 2015. Vol. XXV., No. 3-4; RESPERGER, István: *A válságkezelés és a hibrid hadviselés. (Crisis Management and Hybrid Warfare)*. Budapest: Dialóg Kiadó (National University of Public Service /NUPS/ Press). 2018; RÁCZ, András: *Oroszország hibrid háborúja Ukrajnában (Russia's Hybrid War in Ukraine)*. KKI tanulmányok. (Institute for Foreign Affairs and Trade Studies) 2014. No. 1; SZENES, Zoltán: Military Security Today. New Threats, New Wars, New Theories. In: Géza Finszter, István Sabjanics (Eds), *Security Challenges in the 21.th Century*. Budapest: Dialóg Campus.

[42] SIMICSKÓ, István: A hibrid hadviselés előzményei és aktualitásai. (Antecedents and Consequences of Hybrid Warfare). Hadtudomány (Hungarian Military Science), 2017. No. 3-4.

[43] Government Decree No. 1393/2021. (VI.24.) on Hungary's National Military Strategy. 2021. [online] [cit.2022-20-06] Available from: https://hirlevel.egov.hu/2021/06/27/a-kormany-1393-2021-vi-24-korm-hatarozata-magyarorszag-nemzeti-katonai-strategiajarol/

The strategies, however, do not name any country as a potential perpetrator of hybrid warfare and threat to Hungary, thus making implementation of defensive measures and effective response problematic. On the other hand, if we read between the lines, some countries are implicitly recognizable. The NSS names illegal mass migration as a potential tool of hybrid warfare, for instance, which implicates those countries that can use this method to exert pressure (e.g., Turkey or Russia through its presence in Libya and Syria) – states with which the Hungarian government otherwise cultivates good relationship. Similarly, when the document mentions new "opportunities and challenges" deriving from the rapid technological development such as 5G wireless network, it is easy to identify China.

Both strategies emphasize the need to strengthen resilience against hostile intelligence activity, the coordination among member states as well as between member states and international organizations, first and foremost NATO and EU. The new National Military Strategy dedicates an entire subchapter to the strengthening of the ability for international cooperation. This is one of the reasons why Hungary joined the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in 2019.

The first element of hybrid threats that the Hungarian government recognized was the cyber domain.[44] However, it took half a decade to build a cyber defence system in accordance with international requirements. The evolving EU and NATO policies in this field had a direct impact on Hungary's approach. Hungary's cyber strategy[45] was instantly published after the EU's Cyber Security Strategy of 2013.

The creation of the country's cyber defence system consequently paved the way for today's counter-hybrid policy. Following the build-up of the system of cyber defence, the Hungarian government aimed to strengthen the country's resilience. The COVID-19 pandemic facilitated this goal further as it shed light on the lacking capacities, and the problems in international cooperation, that emphasized the need to rely on one's own forces and resources. Enhancing resilience is stipulated by both the national security and military strategy. According to the NSS, "defence against weapons of mass destruction, terrorism, cyberattacks, hybrid operations and disasters alike demand an increase in Hungary's national resilience" (NSS 2020, para 175.). To serve this goal, it is inevitable to develop the infrastructure of civil protection and a whole-of-government national defence administration (NSS, para 30). The National Military Strategy points out the interrelation between resilience and deterrence and underlines the importance to improve the conditions of host nation support for allied forces. It also holds crucial the military support of civilian authorities in various emergency situations (NMS, 2021, para 30).

National resilience is defined by the new Act XCIII of 2021 on defence and security as the ability of the population, economy, and the state to forecast and prevent threats and dangers, mitigate risks, and manage the consequences and solve the tasks of recovery. To this belong the tasks of maintaining internal and external security, ensuring the national defence and national security interests of the state against natural or man-made disasters, pandemics, attacks or hostile attempts harming or endangering the stability of the state. It also underlines the importance of the two-step strategy elaborated in the National Security

[44] The National Security Strategy of Hungary. Safe Hungary in a changing world. Government Decree No. 1163/2020. 2020.[online] [cit.2022-20-06] Available from: https://nbsz.gov.hu/docs/NBS_MK_2020_81_1163.2020_Korm.hat.pdf

[45] Government Decree of 1139/2013. (III.21.) on Hungary's Cyber Defence Strategy. 2013. [online] [cit.2022-20-06] Available from: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf

Strategy, namely, the need to enhance resilience in accordance with the obligations of the alliance. The law determines the following elements as part of national resilience: a) ensuring the state's functioning determined by the Constitution, uninterrupted governance, and work of crucial government services, b) building an energy system and energy security solutions flexible and adaptive to the challenges, c) ability to effectively control the mass-scale movement of persons, d) system of basic healthcare flexible and adaptive to the challenges, ensuring the work of vital infrastructure satisfying the basic needs of the society, e) ability to manage situations threatening with mass-scale personal injuries, f) creation and operation of info communication and transportation infrastructure flexible and adaptive to the challenges, and g) high level of professionalism and dedication on behalf of the security and defence organs' personnel. It is not hard to recognize the NATO and EU requirements in the above enumeration of tasks.

Crisis management system and decision-making

Hybrid challenges, risks, and threats have impact on the established system of crisis management in Hungary. It is fair to say that these challenges help the country move away from the current scattered system of crisis management and replace it with a new complex one. After the 1989 regime change in Hungary, basically two systems of crisis management evolved: one for solving the tasks of defence against external military attack, and one for handling situations that pose threat to internal security, mainly in natural disasters. Both sets of missions are specified in the Constitution and cardinal laws. The problem lies in the fact that the two systems (external and internal defence) use the same institutional framework, resources, and capabilities but for different purposes, in different locations and hierarchical set-ups, and in varying structures, operational order and cooperation. The government changes the modus operandi from crisis to crisis and the National Security Cabinet is not directly involved in operational management. Hybrid warfare represents an extraordinary challenge to this system as the various types of threats are interconnected with each other. Consequently, countering hybrid threats requires flexibility and joint response on behalf of multiple branches. This is the reason, why experts advise the integration of the existing systems.[46] Also, hybrid threats cannot be handled in the framework of special legal order as they generally emerge in the form of a so-called below the threshold crisis. To handle this problem, the Act XCIII of 2021 was approved, which gradually created conditions to move further the institutional development and better peacetime and crisis decision-making system to deal with hybrid threats.

The act on the harmonization of defence and security activities of 2021 supports the aim to establish an integrated crisis management structure. It prescribes the foundation of the high level national defence and security forum to advise on the matters of national resilience on a whole-of-government level. The forum was established in July 2022 with the name of Defence Council, chaired by the Prime Minister and entitled to discuss all (state and non-state alike) issues of security and defence (including hybrid threats) and make recommendations for governmental and state reforms. This operational body is different from the current National Security Cabinet, which is subordinated to the government. The law authorizes the government to cooperate with bodies not under the supervision of the

[46] KESZELY, László. A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modellje. (A possible Governance model for Comprehensive Action against Hybrid Conflict) *Honvédségi Szemle (Hungarian Military Review)*. 2020. No. 4, pp. 24-48.

government, such as civil organizations, religious communities, and charity organizations, who participate in the fulfilment of defence and security tasks on a voluntary basis. For the sake of operative control, a National Situation Reporting Centre was also established in October 2022. These measures improve the system of crisis management, including the coordinated response to hybrid threats.

Poland

Strategic approach to countering hybrid threats

The concepts of hybrid warfare and hybrid threats were introduced to the official strategic and doctrinal discourse in Poland in the mid-2010s. It is worth mentioning a collected academic volume published already in 2011 by the National Security Bureau (an advisory body to the President of the Republic of Poland in matters of security and defence) concerning the features of asymmetry and hybridness in contemporary conflicts.[47] Unfortunately, it did not have a significant repercussion for strategic thinking and threat perception.

The National Security Strategy adopted in 2014 did not refer to hybrid threats, even though it was released after the outburst of the crisis in Ukraine. A substitute of the term "*hybrid war*" was employed in the document: "*military activities below the threshold of classical war*".[48] This may be attributed to Gen. Stanisław Koziej, the then Head of the National Security Bureau, who coined that formula for a description of a new type of limited military operations which are „*covertly arranged, politically timed and shielded by a screen of disinformation and propaganda", encompassing thereby "information warfare, provocative demonstrations organised by 'useful idiots', secret operations conducted by special forces similar to 'the little green men' in Ukraine."*[49] Nonetheless, the term "hybrid war" appeared in an online BBN Mini-Lexicon of New Security Terms (published by the National Security Bureau in 2015) and was defined as "*war simultaneously integrating various possible means and methods of violence, including regular and irregular armed activities, operations in cyberspace, as well as economic, psychological and propaganda activities etc."*[50] That working definition was devoid of conceptual sharpness and clarity, despite some efforts

[47] SOKALA, Witold and ZAPAŁA, Bartlomiej (eds): *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*. Warszawa: Biuro Bezpieczeństwa Narodowego, 2011.

[48] NSS RP (2014). National Security Strategy of the Republic of Poland 2014. National Security Bureau, Warsaw 2014.

[49] KOZIEJ, Stanisław: *NATO's Strategic Defence in the new "hybrid cold war"*. Pułaski Policy Paper. 2019, No. 6. [online] [cit. 2022-20-06] Available from: https://pulaski.pl/en/pulaski-policy-paper-s-koziej-natos-strategic-defence-in-the-new-hybrid-cold-war/ ; KOZIEJ, Stanisław. *NATO still needs an answer as Russia tests thresholds in East*. Austrian Economics Center. 2015. November 5. [online] [cit.2022-20-06] Available from: https://www.austriancenter.com/nato-still-needs-an-answer-as-russia-tests-thresholds-in-east/

[50] (Mini)Słownik BBN: Wojna hybrydowa (Hybrid warfare). In: *(Mini)Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*. [online] [cit.2021-17-07] Available from: https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html

undertaken in 2015 by the National Security Bureau in cooperation with the National Defence University in the form of conferences devoted to the nature of hybrid war.[51]

The political change in 2015, the electoral victory of the Law and Justice Party (PiS) in the presidential and parliamentary elections marked an important shift in strategic thinking and organisation of the national defence system of the Republic of Poland. The national-conservative ideology of the ruling party was reflected in the first comprehensive assessment of the state of national security and the Polish armed forces. The Strategic Defence Review carried out in 2016 was based on a widespread criticism of the previous strategies and policies based on "*unrealistic assessment of the security environment*".[52] It contained a catalogue of threats and risks to Poland's security and defence but – surprisingly – hybrid threats were not included. The aggressive policy of the Russian Federation was at the top of the list, followed by the uncertain situation in Ukraine, global security threats, and technological, economic, and social threats.[53]

The Strategic Defence Review resulted in the adoption of the Defence Concept of the Republic of Poland[54] in May 2017. No mention of hybrid threats can be found in that document, although a reference to "*hostile activities below the threshold of an armed conflict*" may be interpreted as a substitute of the term "*hybrid war*". It specifically describes Russia's aggressive stance. The Defence Concept unambiguously assumes that "*Russia is ready to destabilize the internal order of other states and to question their territorial integrity by openly violating international law. Russia's actions are often camouflaged and conducted below the threshold of an armed conflict. […] Russia is also likely to provoke proxy wars in various parts of the world to exert pressure on the Western countries. […] Moscow uses instruments allowing it to decrease NATO's advantage of forces by conducting cyber-attacks or threatening the use of force against individual states […].*"

At that time, theory and strategy of hybrid war and hybrid threats specified cybersecurity and cyber threats as typical and essential parts of hybrid conflicts. This was reflected in the National Framework of Cybersecurity Policy for the years 2017-2022,[55] adopted by the Polish government in 2017. One of the objectives of cyber security policy was to enhance the capacity to counteract cybercrime, including cyberespionage, incidents of a terrorist nature, and hybrid threats. It was pointed out that the increasing frequency of attacks of a hybrid nature requires the development of better deterrence and defence capabilities, including the improvement of resilience and acquiescence of ability to respond quickly and effectively to cyberattacks.[56] The latest cybersecurity strategic document[57] points to the role of the ICT sector in increasing the capacity to counteract events of a hybrid nature, including those of

[51] KOLODZIEJCZYK, Rafał: Hybrid war – a potential threat to Poland, Studia i Materiały. *Miscellanea Oeconomicae*. 2017, Vol. 21, No. 4, part II.

[52] SPO: *Strategiczny Przegląd Obronny* 2016. 2016. [online] [cit.2021-17-07] Available from: https://www.gov.pl/attachment/0c73f870-a276-49d7-8f22-e49873d63b90

[53] Ibid.

[54] DCRP: *The Defence Concept of the Republic of Poland*. Warsaw: Ministry of National Defence, 2017.

[55] NFCPRP: *National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022*. 2017. [online] [cit.2022-17-03] Available from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf

[56] Ibid. pp. 22

[57] CSRP: Cybersecurity Strategy of the Republic of Poland for 2019–2024. [online] [cit.2022-17-03] Available from: https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8

a terrorist nature. It is worthwhile to mention that hybrid threats are not defined in the cybersecurity strategies and their meaning is intuitively taken for granted.

A more substantive approach to hybrid threats was presented in the domestic crisis management system. A National Plan for Crisis Management, adopted in 2017 and updated in 2020, based on a classified report on national security threats, mentioned "hybrid activities" as one of the 19 categories of occurrences of natural and man-made origins which require activation of the national crisis management system. In that adocument, hybrid activities were defined as "*actions carried out by state and/or non-state actors in a planned and coordinated manner, often spread over a long period of time, combining various means of pressure from and dependence on a potential aggressor. They may entail political, economic, legal, military and social measures, including the use of national, ethnic and religious minorities and various social communication channels.*"[58]

The National Security Strategy of 2013 was substituted in May 2020 by a new document which articulated the strategic outlook presented by the PiS government. Regarding hybrid threats, however, it did not add up anything to the previous strategic documents. It still associated hybrid threats with Russia's active measures and aggressive policy, claiming that: "*the Russian Federation carries out activities below the threshold of war (of hybrid nature)*".[59] Interestingly, more attention was dedicated to resilience. It was included in the Pillar I of the strategy, which refers to security of the state and its citizens, yet also mentioned the cybersecurity, economy, and information domains. The 2020 National Security Defence set a clear objective: "[*To] build the state's resilience to threats, including hybrid ones, ensure the universal nature of civil defence and protection of the population as well as build-up and maintain the capacity to recover the necessary resources.*"[60]

Institutional framework for countering hybrid threats

The association of hybrid threat with military and non-military activities below the threshold of war had two important implications. Firstly, the tackling of those threats focused primarily on defence and deterrence capabilities generated and developed in the military domain, both domestically and internationally. Secondly, the crisis management system incorporated hybrid activities into a complex set of natural and man-made threats without assigning appropriate competences and tasks to specific institutions. However, recent appointments to key posts in the national crisis management system have indicated a shift of emphasis to civil protection and defence. This suggests that hybrid activities seem to determine the entire crisis management system given that they address a whole range of threats and risks, spanning from ethnic and cultural tensions, disruptions to critical infrastructural networks and economic sanctions to disinformation, cyberattacks and terrorist incidents.[61]

[58] NPCM: Krajowy Plan Zarządzania Kryzysowego. Aktualizacja 2020, part A. p. 48. [online] [cit.2022-17-03] Available from: https://www.gov.pl/attachment/581d0989-0bae-4e8a-8fdb-e2ca5385ac19

[59] NSSRP: National Security Strategy of the Republic of Poland 2020. p. 7. [cit.2022-17-03] Available from: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

[60] Ibid. p. 15.

[61] NPCM: Krajowy Plan Zarządzania Kryzysowego. Aktualizacja 2020, part A. p. 47. [online] [cit.2022-17-03] Available from: https://www.gov.pl/attachment/581d0989-0bae-4e8a-8fdb-e2ca5385ac19

Concerning defence and deterrence capabilities, the Polish Army plays a key role in reacting to threats to the state, its territory and population. The 2020 National Security Strategy points to the need of developing "*operational capabilities of the Polish Armed Forces, in particular of the Special Operations Forces, to combat threats, including hybrid ones and to conduct counterterrorist operations during all possible extraordinary states and in states of defence readiness.*"[62] The singling out of the Polish Special Operations Forces (POLSOF) is meaningful: this component has gained invaluable experience in regional conflicts as part of international coalitions formed under the aegis of the United Nations, NATO, and the United States. From Haiti to Afghanistan and Syria, POLSOF has proved its effectiveness, high level of professionalism and "jointness", especially within the NATO alliance.

In April 2016, the Law and Justice government decided to adopt a concept of territorial defence and, after amendments to the Act on Common Defence Duty, in 2017, a new branch was established within the Polish army: Territorial Defence Forces (TDF). Their mission was to cultivate the tradition of the Polish resistance movement of the World War II and prepare to hamper hostile activities, especially of hybrid nature. The protection of critical infrastructure and assistance to the population in crisis circumstances were also included in the catalogue of TDF's tasks. Those forces are voluntary, organised in 17 regional brigades, and commanded by professional officers. The latter usually come from the Special Operations Forces, which brings the whole idea of territorial defence and resistance closer to the doctrine of irregular warfare.

The impact of the Alliance's mechanisms and resources is underlined also in crisis management. The 2020 National Security Strategy advocated for an adjustment of the national crisis management system to NATO Crisis Response System "*through extending it also to the field of political and military conflict and allowing for smooth transition from the state of peace to the state of crisis and war, as well as ensuring that it provides effective tools to prevent and combat threats, including hybrid ones.*"[63] As mentioned above, a transversal perspective on hybrid threats makes the crisis management system somehow permeated by elements of those threats and therefore embedded in the organisational structure of that system. A key institution, the Government Security Centre (RCB), is responsible for the management of the entire system, threat assessment, alerting and early warning, and emergency response. RCB is led by a director appointed by the Prime Minister, currently a former officer of POLSOF and a former member of TDF Command. The RCB director is a secretary of the Government Crisis Management Team for an Early Identification of Hybrid Threats which is aimed at monitoring hybrid threats, assessing risk of crisis situations, and preparing proposals of a response to hybrid threats and coordination of relevant government actions.

[62] NSSRP: National Security Strategy of the Republic of Poland 2020. p. 19. [online] [cit.2022-17-03] Available from: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

[63] NSSRP: *National Security Strategy of the Republic of Poland 2020*. p. 13. [online] [cit.2022-17-03] Available from: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

Slovakia

Threat perception and strategic approach towards countering hybrid threats

Slovakia acknowledges hybrid threats as a significant security challenge inherently connected and subsequential with the nature of the contemporary security environment. As elsewhere, the term itself came into broader attention of Slovak security policy pundits, think-tankers, and media in 2014/2015 as a descriptive term for Russian actions in the annexation of Crimea and following the war in eastern Ukraine. The way of the term "*hybrid threats*" into the official vocabulary of Slovak security and defence-related institutions and representatives took longer. One of the very first uses of the term in official documents can be found in the Annual Report of Slovak Intelligence Service 2016.[64] The report contains a brief paragraph mentioning the Act on Slovak Information Service and Strategic Focus of Slovak Intelligence Service as two major documents defining SIS tasks and agenda regarding hybrid threats. While the report did not define the term itself, it listed espionage, terrorism, extremism, cyber-attacks, organized crime, foreign influencing, or energetic security as fundaments of nexus like hybrid threats.

The official definition of hybrid threats can be found in the 2017 update of the Crisis Management Terminology Dictionary issued by the National Security Council of the Slovak Republic. "*Hybrid threat is a set of coercive and subversive activities, conventional and unconventional, military and non-military methods, which state and non-state actors use to achieve specific goals without a formal declaration of a war.*"[65] A significant milestone in building understanding and awareness about hybrid threats in Slovakia is tied to the National Security Strategy and National Defence Strategy 2017, which were praised by the expert community, approved by the government, nevertheless, the parliament never approved it, which lead into the "Schrödingerian status" of both documents. In the national security strategy, the case of Ukraine is directly used as an illustrative example of hybrid threats. The above-described definition is employed and extended by direct mentions of paramilitary groups, cyber-attacks, espionage, or influence operation employed by state and non-state actors. As goals of hybrid influencing are mentioned: society polarisation; decreasing trust, legitimacy, and actionability of state institutions; democratic constitutional order; and public support for fulfilling international obligations of the Slovak Republic.[66] The document also promised to create and implement a dedicated concept for building resilience against hybrid threats and deepening the collaboration with relevant NGOs while actively supporting the development of civil society in general. This can be understood as the first, if still not explicit, mention of the so-called whole-of-the-society approach while countering hybrid threats. The National Defence Strategy from 2017 is less eloquent about hybrid threats than the National Security Strategy. Yet, it mentions specific preparation, capabilities building,

[64] Slovak Intelligence Service: *Annual Report 2016*. The Slovak Intelligence Service, 2017. [online] [cit.2022-12-11] Available from: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti-2016.html

[65] Security Council of Slovak Republic: *Terminological Dictionary of Crisis Management*. The Security Council of Slovak Republic. 2017. [online] [cit.2022-12-11] Available from: https://www.vlada.gov.sk/data/files/7616_terminologicky-slovnik-uprava260919.pdf

[66] Ministry of Defence of Slovak Republic: *Defence Strategy of Slovak Republic*. The Ministry of Defence of Slovak Republic. 2017. [online] [cit.2022-12-11] Available from: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2017/640

and collaboration of the armed forces with other armed security corps, crisis management, and other related agencies against hybrid influencing.[67]

A truly cornerstone document in Slovak context regarding hybrid threats is the Countering Hybrid Threats Concept of the Slovak Republic from 2018. The Concept is the first official document wholly dedicated to hybrid threats. It assessed the character of the security environment and level of Slovakia's preparedness, defined basic pillars and goals of the Concept, and outlined the needed institutional framework for effective and efficient countering hybrid threats. The document also stressed the international dimension of hybrid threats in the context of targeted weakening EU and NATO cohesion and solidarity between members, directly opposing the vital national interests of Slovakia as main potential vectors of hybrid influencing are mentioned propaganda, support of local radicals and extremists, marginalized minorities, dependency on energetic supplies, information, and cyber infrastructure.[68]

In 2021, Slovakia updated all top-level security documents: National Security Strategy, National Defence Strategy, National Military Strategy, and National Cyber Security Strategy. All these documents employ the term hybrid threats repeatedly. The 2021 National Security Strategy describes state and society preparedness effectively and in a coordinated manner react to hybrid threats, including disinformation, as a strategic security interest. Again, the weakening of the democratic order and support for Slovakia's membership in the EU and NATO are mentioned as primary goals of hybrid influencing against Slovakia.[69] The National Defence Strategy of 2021 recognized the strengthening of state resilience by military and non-military means. It declared firm determination to react on hybrid influencing against Slovakia's sovereignty and territorial integrity even under the threshold of usual reaction.[70] The National Cyber Security Strategy 2021-2025 defines cyberspace as a vital hybrid domain, where attacks on critical infrastructure, cyber espionage, cyber criminality, or cyber-attacks can occur as a component of a hybrid threat.[71] Even the National Military Strategy 2021 considers hybrid influencing as a severe threat and dedicates much space to this issue within the text. Hybrid threats are considered an escalation factor within scenarios of possible armed attack or armed conflict through targeted disinformation campaigns, local paramilitaries, extremist groups, weaponized migration, cyber-attacks, irredentism, and

[67] Ibid.

[68] Office of the Government of Slovak Republic*: Countering Hybrid Threats Concept*. The Office of the Government of Slovak Republic. 2018. [online] [cit.2022-12-11] Available from: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf

[69] Ministry of Foreign and European Affairs of Slovak Republic: *Security Strategy of Slovak Republic*. The Ministry of Foreign and European Affairs of Slovak Republic. 2021. [online] [cit.2022-12-11] Available from: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf

[70] Ministry of Defence of Slovak Republic: *Defence Strategy of Slovak Republic*. The Ministry of Defence of Slovak Republic. 2021. [online] [cit.2022-12-11] Available from: https://www.mosr.sk/data/files/4286_obranna-strategia-sr-2021.pdf

[71] National Security Authority of Slovak Republic: *National Cyber Security Strategy 2021 -2025*. 2021. [online] [cit.2022-12-11] Available from: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf

separatism. Moreover, the document pays extra attention to potential hybrid influencing against the armed forces, their capabilities, capacities, morale, and cohesion.[72]

While these top-level national security documents do not mention any specific hybrid threats sources explicitly, contextually, it is rather clear that Russia, China, or the broader area of the Middle East are meant. More open in attributing hybrid threats are Annual Reports of Slovak Intelligence Services. Reports from 2018, 2019 and 2020 repeatedly mention Russia and China as examples of significant hybrid influencing sources. Russian campaigns are discrediting EU and NATO while presenting Russia as a good, long-term friend of Slovakia. This messaging is amplified by well-networked pro-Russian civil society organizations, so-called alternative media, and pro-Russian activists and sympathizers. China aims to present its political regime and economy as positive examples by creating and influencing think tanks, media, cultural exchange organizations, and other similar entities to project its influence. These activities often have a coordination background in Chinese secret services.[73]

Assessing the strategic approach towards hybrid threats in Slovakia, one can reasonably describe the current Slovak national approach as solid and rather well-developed. All the current top-level national security and defence strategies fully acknowledge hybrid threats as real and serious national security issues. These documents offer quite a clear official definition, identically define major vectors of potential hybrid influencing and vulnerabilities. Also, they openly stress the importance of international level and dedication for a comprehensive approach, including the private sector and civil society as important actors in countering hybrid threats.

Institutional and processual framework for countering hybrid threats

While on the strategic and conceptual levels, Slovakia managed to develop a solid and well-developed approach regarding hybrid threats in recent years, the institutional setup and processual framework are somehow lagging. As the Concept for fighting hybrid threats of the Slovak Republic states, there is no single state institution explicitly tasked with hybrid threats agenda. No resort holds the necessary material, technical or personal capacities to cover the whole area sufficiently. Therefore, close cooperation and collaboration are necessary across all state and public administration and private sector, and civil society.

The Concept describes a basic institutional framework with the task assigned to listed stakeholders. The Situation Centre at the Government Office of the Slovak Republic (SITCEN) serves as the national contact point for hybrid threats. Aside from its core analytical, monitoring, and information tasks for the Prime Minister Office, SITCEN functions as an official national point of contact for inquiries with international partners, representing Slovakia at the Helsinki Hybrid Centre of Excellence or EU Hybrid Fusion Cell within the EU Intelligence and Situation Centre. The National Security Analytical Centre (NSAC) is a

[72] Ministry of Defence of Slovak Republic: *Military Strategy of Slovak Republic*. The Ministry of Defence of Slovak Republic. 2021. [online] [cit.2022-12-11] Available from: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2021/235

[73] Slovak Intelligence Service: *Annual Report 2018*. The Slovak Intelligence Service. 2019. [online] [cit.2022-12-11] Available from: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti-2018.html ; Slovak Intelligence Service: *Annual Report 2019*. The Slovak Intelligence Service. 2020. [online] [cit.2022-12-11] Available from: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti-2019.html ; Slovak Intelligence Service: *Annual Report 2020*. The Slovak Intelligence Service. 2021. [online] [cit.2022-12-11] Available from: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html .

specialized collaborative workplace of Slovak Intelligence Service with the direct active participation of Military Intelligence, National Security Authority, Ministry of Foreign Affairs, General Staff of Armed Forces, Police, Criminal Office of Financial Administration, and the SITCEN. The NSAC also serves as a national cooperation centre for hybrid threats with the responsibility to evaluate information and suspicious activities based on suggestions coming from state institutions, legal and physical entities. In case of need, the NSAC can prepare a special report for law-authorized recipients.[74]

Aside from SITCEN and NSAC, other important stakeholders can be identified. As the so-called "leading group", we can name the Ministry of Foreign Affairs, Ministry of Defence, National Security Authority, Slovak Intelligence Service, Military Intelligence, and the Armed Forces. All these institutions already created or create dedicated structures for dealing with hybrid threats. By the end of 2021, the National Action Plan for Countering Hybrid Threats, prepared under the MoD guidance, was presented. The main goal established in this document is to provide a clear-cut set of tasks specifying both institutional and processual issues.[75] Simultaneously, the Interior Ministry has prepared the National Project for the Building of Resilience and Capacities Against Hybrid Threats. The European Social Fund project is boosting capacities of analytical and strategic communication units in the Ministry of Interior, Ministry of Foreign Affairs, Ministry of Defence, and the Office of the Government (Ministry of Interior).

Though on the working level and in selected areas the Slovak approach against hybrid threats has been getting more concrete shapes, it still lacks a clearly identified and acknowledged actor responsible for the overall coordination on the policy planning and decision-making levels. Another issue is the outdated National Security System Concept from 2003, a core document for defining goals, actors, agenda, and tasks for ensuring the security of the Slovak Republic. Updating this document to the realities and needs of 2021, including hybrid threats, is of utmost importance and a prerequisite for the creation effective, efficient, well-connected, and truly comprehensive approach against hybrid threats. Also, the COVID-19 experience has revealed shortcomings and incompetence of the state to carry out a systematically proactive communication, limiting at least the reach and consequences of disinformation campaigns. Strategic communication has often been mentioned as a tool for countering disinformation but, except for the MFA, not much has been practically done. The implementation or, better to say, creation of a system of countering hybrid threats in Slovakia is now in development stages and faces several complex challenges.

[74] Office of the Government of Slovak Republic: *Countering Hybrid Threats Concept*. The Office of the Government of Slovak Republic. 2018. [online] [cit.2022-12-11] Available from: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf

[75] Ministry of Defence of Slovak Republic: *Defence Strategy of Slovak Republic*. The Ministry of Defence of Slovak Republic. 2021. [online] [cit.2022-13-11] Available from: https://www.mosr.sk/data/files/4286_obranna-strategia-sr-2021.pdf

Discussion and Conclusions

The comparative analysis demonstrates the V4 countries' political will and effort for countering hybrid threats. The urgency of this matter relates mainly to the aftermath of the Ukrainian crisis in 2014. We can see it in the publication dates of strategic documents of the V4 countries where this agenda is mentioned. The dynamic in the security environment reinforced by the increasing competition among global powers and the ongoing military Russian war against Ukraine provide impetus for further recalibration of existing policies including hybrid threat areas, capabilities and capacities of national security architecture, and decision making in all V4 nations.

Although the concept of hybrid threats appeared in the national state documents (national security strategy, national military strategy, national cybersecurity strategy, concepts for fighting hybrid threats, action plans and programs), the V4 countries (Czech Republic, Hungary, Poland, Slovakia) have understood hybrid threats rather as a political problem of strategic level. In broader sense, the measures taken by these nations aim toward higher level of interagency coordination and improvement of existing processes and security architecture. The adjustments of the V4 nations' operational capabilities and capacities reflect mainly the pressing requirements of maintaining reliable cyber security within the heavily contested cyber and information domain of the four societies.

It is also interesting to follow the development of the agenda of countering hybrid threats alongside another important agenda: cyber security. This is because both of these exist separately in all V4 states, despite the fact that the cyber realm is, by nature of the hybrid threat's definition, one of its defined domains. We can explain this development by the quick need to respond to the growing threats in cyber space, which were emphasized with greater intensity much earlier than the issue of countering hybrid threats. Developments at the level of the Council of the EU also contributed to this two-way approach, where a working group for Cyber Issues was firstly created, to be supplemented by the Horizontal Working Party for Enhancing Resilience and Countering Hybrid Threats several years later. The V4 countries, which are all EU member states, had to reflect this development in their approaches.

The criticality of effective mitigation of hybrid threats in all V4 countries seems to comprise the resilience of national institutions, private sector, and civic society. It means to elevate the whole of government to the whole of society approach to security provision. Based on the outcome of this research, it seems to be a challenge for all V4 nations for the foreseeable future.

The V4 policy documents underline the fact that the employment of proxy forces and government actors disguised as non-governmental organizations as well as the activity of covertly state-funded and controlled criminal and terrorist groups has increased in the new type "grey zone" conflicts. The employers of these means, particularly Russia and to some extend China, exploit modern technology to extend their hybrid operations to the fields of economy, media, cyberspace and to manipulate public opinion.

The Central European countries share the same view about the content of hybrid threats: the attacker / challenger / adversary threatens the sovereignty or viability of the country when trying to weaken the target country in a political, diplomatic, economic, financial, energy, information domain, or military field. During hybrid warfare, the hostile actor aims to inflict hurdles and harm to the countries, create crisis, and decrease their capacity to operate and fulfil their interest through the coordinated use of military and non-military means, state and non-state actors. The separate or combined use of the elements of offensive measures might be capable of influencing, disturbing, undermining internal order, or forming the public opinion without resorting to the employment of conventional military force.

Although all V4 states agree to strengthen the fight against hybrid threats at national level, national policies differ in threat perception, strategy formulation, and policy making, and in the way how to strengthen the security architecture and its capabilities and capacities. It is also found that each country considers different areas to be important regarding to sectoral approach. The first pace of development for cyber threats was easily identifiable, followed by the resilience of countries in the second tier. Poland assigns a remarkably strong role to the military element in the protection against hybrid threats, while in other countries the ministries of the interior, security services, and state bodies play a stronger role. All countries are lagging in the areas of strategic communication, economic, and financial spheres,[76] protection of institutions, companies, and citizens. It is particularly thought-provoking how vulnerable the population is due to Russian disinformation campaigns and the lack of a centrally dedicated strategic communication body to fight against disinformation. This is a very strong, common shortcoming in V4 countries tackling foreign hybrid threats, but this varies from country to country for domestic political reasons and does not allow for uniform action.

[76] Although in the economic and financial spheres we can see gradual improvements given by the need to implement the EU Foreign Direct Investments screening directive.

Table 1: Summary of the comparative analysis in V4 countries

	Czech Republic	Hungary	Poland	Slovakia
Hybrid threat perception	Complex (military, non-military instruments, state and non-state actors, media, disinfo, cyber, political, diplomatic, and economic pressure)	Stress on destabilisation, influence of public opinion in HUN and abroad, use of proxy forces and fictive NGO under state control	Complex (political, economic, legal, military, social, etc. actions carried out by state and/or non-state actors in a planned and coordinated manner)	Complex (military, non-military instruments, state, and non-state actors) with explicit focus under the threshold of war)
Strategy	National Strategy for Countering Hybrid Interference, NSS 2015, NDS 2017	None NSS 2020, NMS 2021	None Strategic Defence Review 2017, NSS 2020	Concept for fighting with hybrid threats of Slovak republic 2018
Policy	Whole of Society to some extent – societal resilience is addressed. Resilient Society 4.0 (Cyber domain)	Cyber societal law on resilience (2021) and National resilience and Recovery Plan (2021), integrated crisis management system established (2022)	Transversal perspective connecting the crisis management system with the national defence Comprehensive defence concept (2017)	Whole of Society approach is reflected in strategic documents
Institutional arrangement	National Security Council, led by Government Office; Centre against terrorism and hybrid threats under Ministry of Interior (2016)	Integrated crisis management system (ICMS) established in 2022	Government Security Centre (RCB) for crisis management;	National Security Council; National Security Analytical Centre, Governmental Situation Centre Various dedicated units at MFA, NSA and MOD and MI (2022)
Cyber domain	National Cyber and Information Security Agency, 2014. National Cyber Security Architecture.	Cyber Defence Strategy 2013 – international cooperation; New Law 2015, National Cybersecurity centre (2015) – centralisation of all bodies, plus CERT)	National Cybersecurity System; Cybersecurity Centre; National Framework of Cybersecurity Policy (2017), Cybersecurity Strategy (2019)	National Security Authority
Reviews, audits	National Security Audit 2016.	No information available	No information available	None, although Intelligence Services Report 2018, 2019, 2020, and 2021 are relevant

All V4 countries agree that the purpose in hybrid attacks is not to reach the threshold of war, which was a mistake, considering the 2022 Russo-Ukraine war. We found that it is equally important for all V4 countries to cooperate with NATO and EU after the crisis in Ukraine, even though we see improvements in the case of two countries (Hungary and Slovakia), which cannot be abstracted from the current war in Ukraine. There is also similarity that these international organizations play conceptual, initiating, and supportive role in the case of V4 countries examined. Although the perception of hybrid threats is very similar, the countries still differ in whether they name or do not name a particular country as a real hybrid threat. In this respect, the Czech Republic and Poland directly mention Russia as a threat, while the other two countries (Hungary and Slovakia) just conclude this indirectly. The differing perceptions of hybrid security are essentially the same as the general security perception of V4 countries and they are in line with the NATO and EU requirements as well as the principles of the Hybrid CoE hybrid threats concept. But in the Polish case, it is difficult to explain why the national hybrid warfare policy was evolving so slowly in the light of the declared Russian threat. It is also interesting that only the Czech Republic (Strategy for Countering Hybrid Threats, 2021) and Slovakia (Concept for Fighting against Hybrid Threats 2018) have specific hybrid-threat-related policies. In Hungary this work has just started, in Poland this policy dissolves in a comprehensive defence concept (2017).

The crisis management system against hybrid threats, on the other hand, shows colourful picture. There is a general tendency to try to integrate the command and control into the Prime Minister Office (Hungary, Slovakia), while in the other two countries (Czech Republic, Poland) this role rests with the Ministry of Defence. The development of the institutional system against cyber threats is progressing well, enjoying concrete recommendations from NATO and EU. The importance of cyber defence as the element of hybrid threat protection coincides with the state and civic experience of the V4 countries and shows perhaps the best results in this area which can be demonstrated for the alliances and the public very well.

The requirements of NATO and EU (e.g., point of contact system) help the countries develop the similar institutional system in both civil and military sphere, giving an opportunity for fruitful intra-cooperation among the four countries. In recent years, building state and country resilience came to the fore, and concrete measures were taken to strengthen it. In Hungary, the first national resilience plan was developed in 2021. All countries work to develop military capabilities (e.g., special operation forces, cyber defensive and offensive forces) in line with NATO requirements. Overall, however, it can be concluded that the anti-hybrid policies, the institutional system, the availability of resources, the crisis management leadership and system differ from country to country in many respects as the pandemic experience has shown. Much remains to be done to achieve the ideal goal “The European Quartet – One Melody” like in V4 tourism.