Political-Strategic Perspectives of Hybrid Warfare in the Czech Republic

Gabriel Olegário

Graduado em Relações Internacionais na Universidade Federal de Santa Catarina e graduando em Ciência Política na Universidade de Hradec Králové, na República Tcheca. Participou do Grupo de Pesquisa e Extensão em Segurança Internacional e Defesa (GESED). Pesquisador voluntário do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea (GEPPIC-UFSC).

Graciela de Conti Pagliari

Professora Associada da Universidade Federal de Santa Catarina. Doutora em Relações Internacionais pela Universidade de Brasília (2009). Mestre em Relações Internacionais pela Universidade Federal do Rio Grande do Sul (2004), Graduada em Direito pela Universidade do Vale do Rio dos Sinos. É autora do livro O Brasil e a Segurança na América do Sul e co-autora do Guia de Defesa Cibernética na América do Sul.

Abstract

Since the first conceptualization of Hybrid Warfare by Hoffman in 2007, the term has been used by politicians and academics to refer to a new concept of war strategy. Therefore, the use and definition of the term are important, considering the growing literature in the academic field after 2014, with the annexation of Crimea by Russia. This paper aims to demonstrate the political-strategic perspectives of the Czech Republic on the issue of Hybrid Warfare, demonstrating the tendency to securitize hybrid threats. Later, a detailed analysis of information warfare is done due to the relevance of the cyber dimension and the importance of disinformation as a hybrid threat in the security environment of the Czech Republic. It is concluded that strategic responses centered only on the State may be insufficient, and a joint effort with society is necessary to pursue the objective of the "Resilient Czech Society 4.0".

Keywords: Hybrid Warfare; Czech Republic; Hybrid Threat; National Strategy Defense.

Resumo

Perspectivas Político-Estratégicas da Guerra Híbrida na República Tcheca

Desde a primeira conceituação de Guerra Híbrida em 2007, o termo tem sido usado por políticos e acadêmicos para se referir a um novo conceito de estratégia de guerra. Portanto, o uso e definição do termo é importante, considerando a crescente literatura no campo acadêmico após 2014, com a anexação da Crimeia pela Rússia. Este artigo tem como objetivo demonstrar as perspectivas político-estratégicas da República Tcheca sobre a questão da Guerra Híbrida, demonstrando a tendência de securitizar ameaças híbridas. Uma análise mais longa sobre a guerra de informação é feita devido à relevância da dimensão cibernética e à importância da desinformação como ameaça híbrida no ambiente de segurança da República Tcheca. Conclui-se que as respostas estratégicas centradas apenas no Estado podem ser insuficientes, sendo necessário um esforço conjunto com a sociedade para atingir o objetivo da "Sociedade Checa Resiliente 4.0".

Palavras-chave: *Guerra Híbrida; República Tcheca; Ameaça Híbrida; Estratégia Nacional de Defesa.*

Artigo recebido: 25.07.2022
Aprovado: 18.10.2022
https://doi.org/10.47906/ND2022.163.03

Introduction

The security issues of the 21st century have been under a rapid socio-technical transformation and increasing fragmentation of political power and authority, establishing hybrid warfare as one of the main State concerns. Therefore, Cavelty and Wenger (2022) maintain that hybrid threats will enlarge in complexity and political significance due to the technological developments that have been shaping the relationship between politics and technology.

The drawback of this article deals with hybrid threats that States are facing under these rapid transformations in society and the recognition of cyberspace as an operational domain in 2016 by NATO (Czech Republic, 2021b). Therefore, the main aim of this article is to identify the developments of hybrid warfare in the current Czech Republic's political-strategic perspective and to select and analyze one hybrid threat relevant in the Czech Republic's context. With that being said, the next chapter delves into the definition of Hybrid Warfare and Hybrid Threat to set the ground for this article.

Definition of Hybrid Warfare

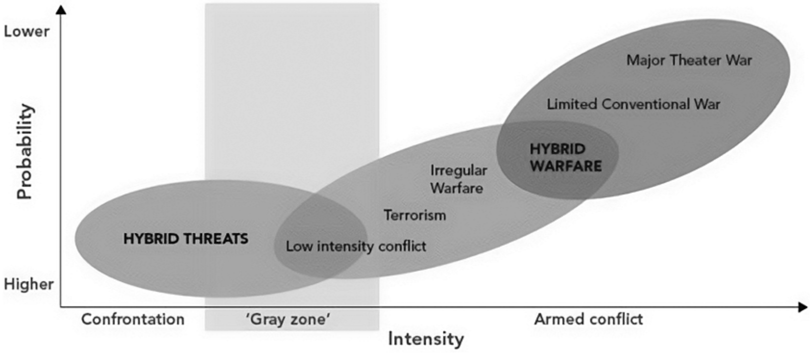
The concept of Hybrid Warfare is wide and subjective to interpret how technological development influences the relationship between the State and Warfare. Thus, formulating a precise definition of Hybrid Warfare is important for both civil society and government national security bodies, especially in the formulation of policies and legislation that encompasses a concept that is still under construction and constantly changing (Clarke and Knake, 2010). One of the first strategists to write about the topic, Hoffman (2009) maintains that seeking a proper definition for the concept of Hybrid Warfare is essential because it facilitates the improvement of policies and defense strategies centered on hybrid threats to better prepare for different internal and external vulnerabilities.

The concept of Hybrid Warfare and Hybrid Threats can be conflicting due to the diversity of possible overlapping definitions, mainly because it is a concept that is still being constructed and modified. The situation is complicated also by the fact that the concept of hybrid warfare or hybrid threats has no legal definition (Łubiński, 2022; Berzins, 2022). As Hoffman referred to in his pivotal work: "Hybrid Warfare incorporates a range of different models of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder" (Hoffman, 2007, p. 14). Thus, hybrid warfare presumes a combination of civilian and military activity, which reaches significant intensity and could result in some level of violence. Interestingly, it has to be noted that many non-western international relations scholars oppose the existence of such a concept, for example, when Russian scholars talk about the same topic they use terms known as new generation warfare and non-linear warfare (Wither, 2016).

Additionally, an important differentiation is the concept of hybrid threat, as the European Centre of Excellence for Countering Hybrid Threats refers to: as "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 means" (Hybrid CoE, 2022). In other words, the threats could be any phenomenon that could undermine or harm the interests and values protected by the State. Furthermore, due to the hybrid aspect diminishing boundaries between civilian tools and military weapons, hybrid threats have a lower intensity and take place in the "gray zone" compared to hybrid warfare (Filipec, 2022, p. 5).

The image below differentiates both concepts visually, conceptualizing the probability and intensity of a conflict in those terms. Therefore, there is a difference between managing a hybrid threat and hybrid warfare, the same way terrorism and irregular warfare are in the same continuum of conflict, however, they require different tactics to tackle it.

Image 1
Hybrid Warfare and Hybrid Threats



Source: Hoffman (2009).

To understand how Hybrid Warfare and Hybrid Threats are intertwined with the Czech Republic's security environment, we shall proceed to the next subsection.

Czech Republic's strategic environment

The Czech Republic (as well as Central European countries) redirected its geopolitical values after the Cold War, starting a process of *westernization* (Cadier, 2019). According to Cadier (2019), this process of *westernization* is best known as the *return to Europe*, a transition embracing liberal democracy, capitalism, and Euro-Atlantic political structures that were seen as contemporary solutions to 90's geopolitical issues. Thus, there is a historical background to explain Czech Republic's pathway to westernization. To summarize, since 1993, the Czech Republic's security environment has been developing three main pillars in the form of challenges. The first concerns the adequacy of Western European patterns of change in the Czech security environment and changes in domestic, economic, and social transformation policies. The second is related to the implementation of the defense policy, which most of the time encounters difficulties because it is not being adequately financed, resulting in a defense sector that has insufficient resources and the lag of defense capabilities. The third pillar is associated with the evolution of the concept of the Armed Forces of the Czech Republic, more specifically, the role of the Armed Forces was primarily the defense of the national territory which contemporaneously becomes (after the 1990s) Expeditionary Forces that has in its core the principle of collective defense and provider of know-how for international crisis management (Czech Republic, 2015).

Three main tendencies can be retrieved from the Security Strategy of the Czech Republic (2015), the first trend concerns that the risks of invasions or direct military conflicts against the Czech Republic are low, however, the possibility of using force in conjunction with NATO allies or EU members cannot be ruled out. This point is underpinned by the general decline in security and stability on the flanks of Europe and in the EU's neighboring countries which can take the form of threats of a classical military nature or the form of Hybrid Warfare. Furthermore, the increasing dependence of the Czech state and society on technology generates vulnerabilities (Czech Republic, 2015).

The second trend is in line with the first since the Czech Armed Forces are increasingly preparing to transform themselves into Expeditionary Forces due to the lack of internal use of military force. Thus, the second trend is that the security environment of the Czech Republic is defined beyond national and the EU borders, recognizing that any global conflict could affect the Czech Republic. The Security Strategy of the Czech Republic (2015) states that "one of the characteristic aspects of the current environment is that our security can be directly affected by the instability and conflicts existing far beyond the borders of Europe" (Czech Republic, 2015, p. 10). Moreover, the Czech Republic encompasses a much wider spectrum of crisis management with a combination of military and civilian tools, in addition to diplomatic, legal, and economic means (Czech Republic, 2015).

The third trend is associated with the growing ambition of some actors around the Czech security environment ready to use military force in pursuit of their interests at the expense of stability in other countries. Therefore, according to the Security Strategy of the Czech Republic,

> The aspirations of these actors are associated with a substantial increase in their military capabilities, including offensive cyber capabilities, weapons of mass destruction, and their means of delivery, and with their growing demand for essential raw materials, activity in financial markets, struggle for influence in strategic areas and increasingly aggressive promotion of its political ambitions in international forums [...] In addition, another consequence of the aspiration of these actors is the destabilization of the strategic environment of NATO, the EU, and the Czech Republic, resulting in conflicts that violate human rights, including political, social and environmental rights. Such actors (state or otherwise) normally violate the international order and basic principles of international law in the pursuit of power (Czech Republic, 2015, p. 10).

After the elucidation of the Czech Republic's security environment, we shall continue with how the official Czech documents strategically perceive Hybrid Warfare and Hybrid Threats.

The Czech Republic's political-strategic perspectives

As detailed above, the Czech Republic relies on the *westernization process* and this leads the Czech Republic to affirm explicitly or implicitly in the documents that membership in NATO and the EU is the best guarantee for the National Security of the Czech Republic. According to the 2017 Defense Strategy, we observe that

> The Defence Strategy is based on the applicable national law regulating defense, particularly the Czech Constitution, international treaties, and relevant Acts. It stems from the Security Strategy of the Czech Republic and reflects NATO's Strategic Concept, the EU's Global Strategy, and other relevant national, international and allied documents (Czech Republic, 2017, p. 6).

This strategy strongly emphasized security threats that did not pose greater risks to the Czech Republic itself but were associated with a degree of risk to NATO members. In practice, this means that international terrorism has become the number one security threat, with the proliferation of weapons of mass destruction in second place, which was not the primary agenda for the national defense of the Czech Republic in 2017 (Kriz, 2021). However, as NATO and the EU have been preparing to increase the resilience against hybrid warfare in their official documents, the instability created by the 2022 Ukrainian-Russian war will likely increase the significance of hybrid warfare and threats to the NATO/EU members as well as the Czech Republic (The economist, 2022). The concept of Hybrid Warfare not only gained some popularity in public opinion, but hybrid campaigns or hybrid threats gained relevance after 2012 in the main security documents of the Czech Republic such as Security Strategy of the Czech Republic (2015), Defence Strategy of the Czech Republic (2017), National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025, the National Strategy to Combat Interference Hybrid as well as official reports from the Czech Republic's intelligence agency. To find a satisfactory answer regarding The Czech Republic's political-strategic perspectives, the next subsections go further into the document's details.

Security Strategy of the Czech Republic (2015)

The introduction to the Security Strategy of the Czech Republic (2015) document cites that "In today's crisis-ridden world, the Czech Republic naturally has to face a huge number of challenges. Economic and social development is our main and immediate concern" (Czech Republic, 2015, p. 3). Therefore, the Czech Republic understands that immediate concerns (economic and social development) will only progress if strategic interests are promoted as such,

> security and stability, especially in the Euro-Atlantic area; preventing and managing local and regional conflicts and mitigating their impacts; maintaining the UN's global stabilising role and increasing its efficiency; strengthening the cohesion and efficiency of NATO and the EU and retaining a functional and credible transatlantic link; reinforcing the NATO-EU strategic partnership, including the strengthening of cooperation in the complementary development of defence and security capabilities; developing the OSCE's role in the prevention of armed conflicts, in democratisation and in building mutual confidence and security; a functioning and transparent conventional arms control regime in Europe; supporting and developing regional cooperation; supporting international stability through cooperation with partner countries; supporting democracy, fundamental freedoms, and the principles of the rule of law; safeguarding internal security and protecting the population; safeguarding the Czech Republic's economic security and strengthening the competitiveness of the economy; safeguarding the Czech Republic's energy, raw-material and food security and an appropriate level of strategic reserves; safeguarding the Czech Republic's cyber security and defence; preventing and suppressing security threats affecting the security of the Czech Republic and its allies (Czech Republic, 2015, p. 8).

The Security Strategy of the Czech Republic (2015) that is currently in force was adopted in the context of various hybrid threats such as the annexation of Ukraine by Russia as well as the cyberattacks on the Baltic countries (Czech Republic, 2015). Learning the lessons from a lack of a joint response against both events, the Security Strategy of the Czech Republic (2015) brings a perspective that focuses on international cooperation, as the "weakening of the cooperative security mechanism and of political and international legal commitments in the area of security" (Czech Republic, 2015, p. 13).

Although Russia is not explicitly mentioned in this document, the idea is developed from the recent strategies used by Russia, the document states that revisionist States might use hybrid instruments to achieve their goals such as

> 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) (Czech Republic, 2015, p. 13).

Yet, a very important remark is the affirmation of the volatile nature of the present security threats and the requirement to have a broad-based approach to security, combining military and non-military tools to defeat hybrid threats. Therefore, the document affirms that "The Czech Republic develops tools for promoting its security interests at the national level as well as through active engagement in multilateral and bilateral relations". The purpose of having such a broad-based approach is due to the abstract nature of threats that might occur, taking into account the development of new technologies and consequently new threats.

The Defence Strategy of the Czech Republic (2017)

In the Defence Strategy of the Czech Republic (2017), the Czech Republic seeks to achieve a comprehensive security approach that goes beyond the framework of pure military security, following the same tendency in the Security Strategy of the Czech Republic (2015). Moreover, the comprehensive security approach is a core principle of NATO and the EU that is also affirmed in the Defence Strategy of the Czech Republic (2017) with the aim of ensuring

> the defence of its sovereignty and territorial integrity, primarily within the framework of NATO's collective defence as set out in Article 5 of the Washington Treaty. Nevertheless, the Czech Republic's membership of international organisations does not free it from its primary responsibility of defending its own national territory. Autonomously, and in cooperation with other states, the Czech Republic maintains and develops,

> in line with Article 3 of the North Atlantic Treaty, its individual and collective capacity to resist an armed attack. The defence policy of the Czech Republic is based on the country's membership of NATO and the EU, and benefits from the provision of home defence and security while, in turn, committing the Czech Republic to adequately contribute to the development of the collective defence of other member countries (Czech Republic, 2017, p. 15).

In the 2017 Defense Strategy, the threat of the Russian Federation and its imperialist ambitions against the Czech Republic and the West is explicit, and the document continuously develops the foreign and security policy orientation that the Czech Republic has followed since 1993, namely pro-Western and anti-Russia orientation, ties to the transatlantic security partnership and building the security dimension of the European integration.

> Since 2012, the security situation in Europe has significantly deteriorated. In Eastern Europe, the Russian Federation blatantly carries out its power ambitions, including through use of military force. In doing so, the Russian Federation violates the norms of international law, including the territorial integrity of its neighbouring states. It has executed hybrid operations against NATO nations and EU Member States, including targeted disinformation activities and cyber-attacks (Czech Republic, 2017, p. 7).

As stated in the Defense Strategy document, the Czech Republic is responding by increasing the defense budget at the expense of the instability of its strategic environment. Still, it is claimed that the

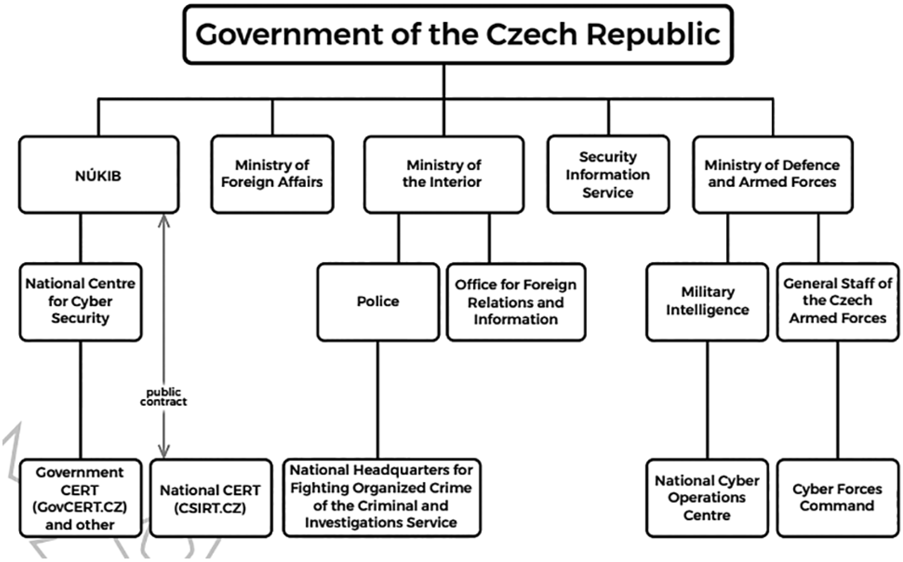
> response to the deteriorating security environment, the Czech government has begun to increase defence funding. The most pressing task is to redress the consequences of the slump in the level of defence capabilities, and the personnel, technology and material negligence that had built up over the previous years, and to develop the Czech Armed Forces so that they are able to fulfil their tasks (Czech Republic, 2017, p. 7).

Another feature described is the national defence system interlinked with the allied structures. The primary function of the national defence system is "to prepare, manage, coordinate and support activities of the relevant authorities, forces, and assets in order to ensure the defense of the Czech Republic. This includes early detection, prediction, and evaluation of potential threats, including hybrid threats" (Czech Republic, 2017, p. 16). Importantly, the operational activities are provided for and controlled by the President of the Czech Republic, Parliament and the Government of the Czech Republic, working and advisory bodies, ministries and other central government authorities.

Czech Republic National Cyber Security Strategy 2021-2015

According to the Czech Republic National Cyber Security Strategy 2021-2015 document, the Czech government has been funding and renewing its cybersecurity strategy against the variety of threats that the cyber dimension has been producing. Therefore, the scheme below demonstrates how Cyber Security is ensured by the Czech Republic, demonstrating that cyberspace is one of the most recent and vulnerable dimensions due to the lack of preparation States have to securitize technology.

Image 2
Ensuring Cyber Security in the Czech Republic


Government of the Czech Republic
NÚKIB
Ministry of Foreign Affairs
Ministry of the Interior
Security Information Service
Ministry of Defence and Armed Forces
National Centre for Cyber Security
public contract
Police
Office for Foreign Relations and Information
Military Intelligence
General Staff of the Czech Armed Forces
Government CERT (GovCERT.CZ) and other
National CERT (CSIRT.CZ)
National Headquarters for Fighting Organized Crime of the Criminal and Investigations Service
National Cyber Operations Centre
Cyber Forces Command

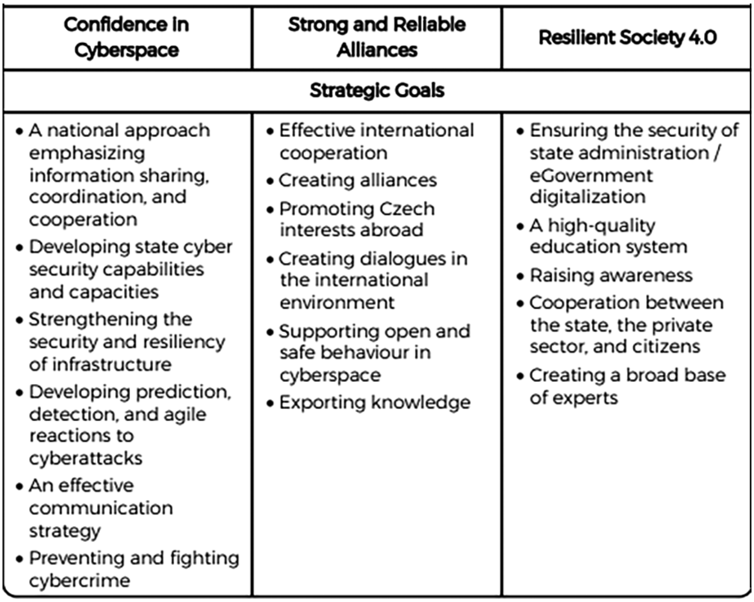
Source: Czech Republic (2021b, p. 8).

According to the document, each unit shown in the figure above has a specific function, mainly specified in the document that complements the National Cybersecurity Strategy of the Czech Republic 2021-2015 called the Action Plan for the National Cybersecurity Strategy of the Czech Republic 2021-2015. For didactic purposes, the Action Plan will not be analyzed, as the most important result is to understand the complexity of cyber protection networks and the primary role of the government of the Czech Republic in ensuring cyber security.

The Czech Republic Cyber Strategy (2021b) can be structured and summarized in three main points: a) confidence in cyberspace, b) strong and reliable alliances and c) Resilient Society 4.0. The three points correspond with the future of the strategic direction of the coming years. The overview of "The Czech Republic will have a resilient society and infrastructure, will act confidently in cyberspace and will actively confront the entire spectrum of threats while strengthening reliable alliances" (Czech Republic, 2021, p. 21).

Thus, considering the three points mentioned in the document, the summary of the strategic objectives can be found in the table below,

Table 1
Strategic objectives according to the National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025



Confidence in Cyberspace	Strong and Reliable Alliances	Resilient Society 4.0
Strategic Goals		
• A national approach emphasizing information sharing, coordination, and cooperation • Developing state cyber security capabilities and capacities • Strengthening the security and resiliency of infrastructure • Developing prediction, detection, and agile reactions to cyberattacks • An effective communication strategy • Preventing and fighting cybercrime	• Effective international cooperation • Creating alliances • Promoting Czech interests abroad • Creating dialogues in the international environment • Supporting open and safe behaviour in cyberspace • Exporting knowledge	• Ensuring the security of state administration / eGovernment digitalization • A high-quality education system • Raising awareness • Cooperation between the state, the private sector, and citizens • Creating a broad base of experts

Source: Czech Republic (2021, p. 21).

Therefore, the strategic objectives are focused on the resilience of the State against cyber vulnerability, both in terms of hardware and social issues (Czech Republic, 2021). Following the broad-based approach to counter hybrid threats, society (ordinary internet users) needs to get used to protecting itself, recognizing possible threats, and understanding the dynamics of cyberspace. This is precisely why the document states that it will invest in primary and secondary education to modernize the country's educational system and also invite sectors of society to participate in courses on digital hygiene to improve digital resilience, especially positions that demand knowledge and use of the internet with sensitive data (Czech Republic, 2021).

National Strategy to Combat Hybrid Interference

Hybrid Interference has become a relevant security matter and the National Strategy to Combat Hybrid Interference defines the objectives and determines the essential defense capabilities for the protection of the national interests of the Czech Republic. Such a document has a strong appeal for the comprehensive security proposed by NATO and the EU, as it focuses on a wide variety of security threats, in addition to human security (Czech Republic, 2021a).

Thus, the document states that hybrid threats can include the overt or discreet influence of political structures and the decision-making process in politics, courts, police, military, media and public opinion. The opponents' objectives would be to destabilize or divide Czech society and diminish the trust that citizens have in the country's institutions (Czech Republic, 2021a).

Still, the hybrid threats that can affect the economic interests of the Czech Republic, and the strategic sectors that the Czech Republic cites are dependence on strategic resources from foreign countries, such as oil, natural gas, and nuclear fuel. Therefore, the Czech Republic states that it will guarantee the defense of the opening of the economy and its orientation towards exports, foreign investments, and loans that are in strategic sectors of the economy or that lead to strategic dependence on its suppliers (Czech Republic, 2021a). In addition to the dependence on strategic resources for the development of the Czech economy, it is also necessary to understand that hybrid threats can manifest through technologies such as 5G networks and artificial intelligence used by the private sector (Czech Republic, 2021a).

Other risks also concern corruption, links between diplomacy, the private sector, espionage, and the interest of foreign powers in the Czech Republic. Hybrid threats can include the mobilization of interest groups (defined by religion, ethnicity, nationality, or language) or criminal groups acting against the security interests of the Czech Republic and violating public order. Hybrid interference that seeks to delay or paralyze decision-making processes in the defense and security domain also poses a risk. This includes NATO collective defense and EU defense and political cooperation (Czech Republic, 2021a).

The hybrid threat of informational warfare and (dis)information in the Czech Society

Since the concept of warfare has existed in human societies, it has always been connected with information. Therefore, decisions and actions of any nature can be understood in informational terms. For example, controlling the flow of information and its characteristics can represent an important factor in influencing the behavior of certain targets, and consequently can be weaponized to achieve political goals (Filipec, 2019).

The democratic system in the Czech Republic has alleged asymmetrical vulnerabilities and is characterized by uncertainty about the impact of disinformation, leading to an increase in the securitization of information. Furthermore, the empirical evidence is short related to foreign disinformation campaigns having a substantial long-term effect on public discourse and public policy, and the potential macro effects on policy-making and psychological influence are difficult to understand and prove (Štětka, Mazák and Vochocová, 2021).

According to the Czech intelligence service, the Czech Republic has become a laboratory for the Russian Hybrid War (Bezpecnostní Informacni Sluzba, 2020). It is important to remember that due to the geographical situation of the Czech Republic and its past, 'less Europe' automatically means 'more Russia'. To some extent, Rychnovska and Kohut (2018) affirm that Russia's policy of inflicting fear is in the national interest, and one of the goals that Russia has is to gain more support for its foreign policy through the use of the disinformation strategy (Rychnovska and Kohut, 2018).

One of the dangers of defining disinformation is to similarly conceptualize "fake news", "misinformation", "coordinated inauthentic behavior" and "propaganda" in the same category due to the amount of news misusing these terms. For the majority of news consumers, this difference might be not that relevant, however, Ó Fathaigh, R. & Helberger, N. and Appelman, N. (2021) maintain that this constellation of different concepts is the defining political communication topic of our time, which most likely will increase over time. A clear definition of those terms is essential to any State that fancies creating cyber strategies and defensive capabilities.

In fact, there are various definitions and overlapping concepts which may significantly vary in different contexts, and the Czech Republic is no different. A primary definition by the High-Level Expert Group of Fake News and Online Disinformation of the European Commission affirms that "Disinformation… includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for-profit" (De Cock Buning, 2018, p. 3). That is the reason why the definition above has some critical criteria as a) deception, b) potential for harm, and 3) an intent to harm. It thus excludes deceptive messages that may cause harm without the disseminators' knowledge (misinformation) and non-deceptive messages intended to harm others (e.g. hate speech).

To summarize those three critical criteria, disinformation is misleading information that has the purpose to be intentionally misleading, intentionally providing manipulated content, and therefore intentionally creating false beliefs. Disinformation is still informational nonetheless, taking into account the nature of the phenomenon (De Cock Buning, 2018).

Moreover, the Czech Ministry of Interior distinguishes between disinformation, understood as a "systematic and intentional spread of false information mainly by state actors or its affiliates against foreign states or media with the aim to influence decision-making or opinions of those, who adopt decisions" and misinformation which refers to "incorrect or misleading information, which is not spread systematically nor with the intention to influence decision-making or the opinions of those who adopt decisions" (Czech Republic, 2019).

Quoting one of the most influential Czech politicians, former President, and Philosopher Václav Havel: "It is a natural disadvantage of a democracy that it ties the hands of those who wish it well, and opens unlimited possibilities for those who do not take it seriously" (Havel, 1971, p. 12). Therefore, it is evident that democracies have a shortcoming in tackling disinformation, and Central and Eastern European countries might have specific factors that make it even more difficult. After those necessary definitions, the next subsection deals with countering information warfare and (dis)information in the Czech Society

Countering information warfare and (dis)information in the Czech Society

To a certain extent, democratic countries have more barriers to counter information warfare as they try to find a balance between freedom of expression and protection of one's basic rights, as censorship is not acceptable in the Czech constitution. To delve further into the Czech Republic's perspective, foreign disinformation campaigns were assessed as a serious threat to internal security and one of the recommendations to combat these forms of hybrid warfare was to "establish departments within relevant government institutions for the assessment of disinformation campaigns and other manifestations of foreign power influence" (Czech Republic, 2016, p. 61).

Thus, a response by the Czech government to this problem was the establishment of the Center against terrorism and hybrid threats (Centrum proti terorismu a hybridním hrozbám) in 2017. However, one of the points and difficulties that States have is to fight disinformation at the expense of basic rights, such as the right to expression, leading the current president of the Czech Republic, Milos Zeman, to suggest that the Center would infringe on freedom of expression (Reuters, 2021).

This is exactly why the Czech Republic finds barriers to penalizing disinformation, as such a term does not exist in the Czech legislative system. As there is no specific term for disinformation, the Czech Republic has different crimes that can be typified as disinformation, as in the Penal Code, Chapter II criminal offenses against liberty, privacy and personal rights and confidentiality only in the case of § 181 violation rights of others, § 184 defamation, § 345 false accusations, § 355 defamation of the nation, race, ethnicities or other groups of people, § 356 instigation of hatred against groups of people or the suppression of rights and freedoms, § 357 spreading news §364 incitement to criminal offenses, § 365 approval of criminal offenses, § 404 expressing sympathies for movements that seek to suppress human rights and freedoms in accordance with act nº 40/2009 (Filipec, 2019).

The National Cyber and Information Security Agency maintains in the National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025 that

> the Strategy's main actors are the state's security services and other public administration bodies. However, the Strategy also supports and informs other parts of Czech society to enable them to better understand the state's actions when facing cyber threats and risks [...] leaving cyber security solely to the Czech state is not enough, however. Every institution, private company, and individual has their role and can positively contribute to cyber security. The Czech Republic must therefore set up and support a cyber security policy that will consistently incorporate all of society into cyber security processes and thus increase its resilience to cyber threats (Czech Republic, 2021, p. 3).

In other words, there is a glimpse into what the Czech Republic considered as proper cyberdefense capabilities: a tendency to decentralize the securitization of information through the increase of resilience of the civil society, the private and the public sectors. Furthermore, the key strategy against disinformation is resilience in the Czech society, more specifically, to increase the capacity to recover as fast as possible from difficulties or toughness (Czech Republic, 2021).

According to the National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025, "the central challenge for the Czech Republic in this area is to concentrate not only on current cyber security threats but also to acquire the ability to adapt to the new and constantly changing security environment" (Czech Republic, 2021, p. 6). Therefore, there is a flexible tendency for adopting defense policies along the way, proving that the Czech Republic maximizes its capacities and constantly seeks new strategies against future cyber threats.

With that being said, the securitization of information warfare or disinformation happens primarily with the emergence of a new network of professionals composed of think tanks and journalists who manage to reach the public and influence policy-makers. Thus, this network is formed by professionals from different fields connecting different institutions. One of the examples is European Values and the Ministry of Interior of the Czech Republic, which have working connections and develop policies together (Rychnovska and Kohut, 2018).

The European Values initiated a series of reports about the Kremlin, and consequently, the expert endorsement was published to legitimize the aggressive policies of the Russian government. Another point is to analyze how the Ministry of the Interior was influenced, legitimizing the activities of European Values and bringing the whole problem of disinformation to the forefront of media attention (Rychnovska and Kohut, 2018).

Also, according to Rychnovska and Kohut (2018), there are different networks that have different audiences in information warfare debates. For example, while the Prague Security Studies Institute (PSSI) think tank mainly communicates with domestic and international civil society and private actors, European Values has a much closer relationship with the Czech Republic's security apparatus.

Still, the relationship between politicization and securitization of disinformation complicates the possibilities of responses by the Czech government, however, the addition of independent institutions creates new measures that can be adopted in different contexts counting on the potential social mobilization, in addition to just creating untrustworthy media blacklists, selecting individuals who share pro-Russian propaganda, fact-checking tools or digital education (Rychnovska and Kohut, 2018).

Therefore, comprehending the limitation of the Czech government in fighting disinformation, and how this limitation gave space for non-governmental organizations to enter as agents fighting disinformation is a must. Consequently, the decentralization of the fight against disinformation can be one of the solutions for the Czech Republic to continue with its democratic and transparent narrative, giving space for non-governmental organizations to filter information that matches reality.

Conclusion

To conclude, this article demonstrated the strategic responses and the capacity that the Czech Republic has against hybrid threats that are related to its strategic environment (which has been changing since 1993). In other words, the State's inability to securitize all technological advances creates different responses and strategies against hybrid threats, such as the strengthening of the concept of resilience among all parts of society, in addition to the use of independent organizations that can be used strategically against disinformation.

Furthermore, the concept of Hybrid Warfare and the underlying hybrid threats are still constantly changing, and the metamorphic nature of the results of this work is possible. Therefore, when we analyze disinformation in Czech society, we infer that democracies may have obstacles to censoring and filtering information that will pass through digital media. At last, it is analyzed that in order to tackle disinformation, the decentralization of the strategy against disinformation can be an efficient response, such as the joint work between independent organizations such as think tanks and the Czech government.

References

Berzins, V. (2022). 'Hybrid warfare: weaponized migration on the eastern border of the EU?' *The Interdisciplinary Journal of International Studies*, 12(1), 3-19. Available at: https://130.225.53.24/index.php/ijis/article/view/6992 (Accessed: 21 February 2022).

Cadier, D. (2019). 'The geopoliticisation of the EU's Eastern Partnership'. *Geopolitics*, 24(1), pp. 71-99. DOI: 10.1080/14650045.2018.1477754

Czech Republic. Bezpečnostní informační služby (2020). VÝROČNÍ ZPRÁVA 2020. Available at: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf (Accessed: 21 February 2022).

Czech Republic. Minister of Interior (2016). National Security Audit. Available at: http://www.mvcr.cz/cthh/soubor/national-security-audit.aspx (Accessed 9 February 2022).

Czech Republic. Ministry of Defence of the Czech Republic (2015). Security Strategy of the Czech Republic. Available at: https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf (Accessed: 21 February 2022).

Czech Republic. Ministry of Defence of the Czech Republic (2017). THE DEFENCE STRATEGY OF THE CZECH REPUBLIC. Available at: https://www.army.cz/assets/en/ministry-of-defence/strategy-and-doctrine/defencestrategy2017.pdf (Accessed: 21 February 2022).

Czech Republic. Ministry of Defence of the Czech Republic (2021a). NATIONAL STRATEGY FOR COUNTERING HYBRID INTERFERENCE. Available at: https://www.army.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf (Accessed: 21 February 2022).

Czech Republic. National Cyber and Information Security Agency (2021b). National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025. Available at: https://nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf (Accessed: 21 February 2022).

Czech Republic. Ministry of Interior (2019). 'Definice dezinformací a propagandy'. Available at: https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx Accessed 6 February 2022

De Cock Buning, M. (2018). *A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation*. Luxembourg: Publications Office of the European Union. Available at: https://hdl.handle.net/1814/70297

Filipec, O. (2019). 'Towards a disinformation resilient society?: The experience of the Czech republic' *Cosmopolitan Civil Societies: an Interdisciplinary Journal*, 11(1), pp. 1-26. DOI: https://search.informit.org/doi/10.3316/informit.327461541708193

Filipec, O. (2022). 'Multilevel analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threats'. *Central European Journal of Politics*. DOI: 10.24132/cejop_2022_1

Havel, V. (1971). Spiklenci. *Václav Havel Library*. Available at: https://archive.vaclavhavel-library.org/Archive/HavelWork?eventType=Dramatick%C3%BD%20text&eventYear=1971# (Accessed 9 February 2022).

Hoffman, F. G. (2009). *Hybrid threats: Reconceptualizing the evolving character of modern conflict*, Vol. 240. Washington: Institute for National Strategic Studies, National Defense University.

Kříž, Z. (2021). 'The security perception and security policy of the Czech Republic, 1993-2018'. *Defense & Security Analysis*, 37(1), pp. 38-52. DOI: 10.1080/14751798.2020.1831231

Łubiński, P. (2022). 'Hybrid Warfare or Hybrid Threat–The Weaponization of Migration as an Example of the Use of Lawfare–Case Study of Poland'. *Polish Political Science Yearbook*, 51, pp. 1-13. Available at: https://rep.up.krakow.pl/xmlui/bitstream/handle/11716/11174/Lubinski_Hybrid_warfare_or_hybrid_threat_the_weaponization_of_migration.pdf?sequence=1&isAllowed=y (Accessed: 21 February 2022).

Ó Fathaigh, R., Helberger, N. and Appelman, N. (2021). The perils of legally defining disinformation. *Internet Policy Review*, 10(4). DOI: 10.14763/2021.4.1584. 2021

Reuters (2017). Czech "hybrid threats" centre under fire from country's own president. Available at: https://news.trust.org/item/20170104185631-56r53 (Accessed 9 February 2022).

Rychnovská, D. and Kohút, M. (2018). The battle for truth: mapping the network of information war experts in the czech republic. *New Perspectives*, 26(3), 57-87. DOI: 0.1177/2336825X1802600304

Štětka, V., Mazák, J., and Vochocová, L. (2021). "Nobody Tells us what to Write about": The Disinformation Media Ecosystem and its Consumers in the Czech Republic. *Javnost-The Public*, 28(1), pp. 90-109. DOI: 10.1080/13183222.2020.1841381

Hybrid CoE (2022). The European Centre of Excellence for Countering Hybrid Threats, 'Countering Hybrid Threats'. Available at: https://www.hybridcoe.fi/ (Accessed: 21 February 2022).

The Economist (2022). What is hybrid war, and is Russia waging it in Ukraine? Available at: https://www.economist.com/the-economist-explains/2022/02/22/what-is-hybrid-war-and-is-russia-waging-it-in-ukraine (Accessed: 21 February 2022).

Wither, J. K. (2016). Making sense of hybrid warfare. *Connections*, 15(2), pp. 73-87. Available at: https://www.jstor.org/stable/26326441?casa_token=taWB4vxTxu8AAAAA:yeXZdcrKrVlNv0K1eTq0Aie47OVcWgdl0bIHv_2bkiuU9oHV81IgNx8ZqK94Oyk309KNUuxsJaypGD7lfdxFiwiww2JOh2dD5-xE5vSUUE-GRqAuwaCl (Accessed: 21 February 2022).