

Strategic Communication as One of the Key Tools to Counter Hybrid Threats

Ivan MAJCHÚT^{1*}, František GUBÁŠ¹, Juraj ŠIMKO¹

¹Security and Defence Department, Armed Forces Academy of Gen. M. R. Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovakia

Correspondence: *ivan.majchut@aos.sk

Abstract

This paper explores strategic communication as a key instrument for countering hybrid threats in contemporary democratic states. The author, drawing on conceptual analysis, policy documents and practical case studies, examines the role of strategic communication in strengthening societal resilience, shaping public narratives, and responding to information-based aggression. He defines hybrid threats as multidimensional and adaptive phenomena operating below the threshold of armed conflict, exploiting institutional, psychological and informational vulnerabilities. Simultaneously, he argues that strategic communication, when coordinated, credible and value-based, constitutes an essential component of national security policy. The analysis identifies four core functions – informational, preventive, coordinative and normative – and highlights challenges related to institutional fragmentation, analytical capacity, and ethical dilemmas. Based on the findings, the author formulates normative and practical recommendations for policymakers. He concludes that strategic communication is not only a reactive tool but also a proactive mechanism for narrative resilience and democratic integrity in the age of non-linear conflict.

KEY WORDS: *Strategic communication, key tool, state, hybrid threats, defence.*

Citation: Majchút, I.; Gubáš, F.; Šimko, J. Strategic Communication as One of the Key Tools to Counter Hybrid Threats. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, [https://doi.org/ 10.47459/cndcgs.2026.28](https://doi.org/10.47459/cndcgs.2026.28)

Introduction

In an era of deepening strategic uncertainty, instability, escalating multipolar global rivalry, and unprecedented technological acceleration, the global and regional security environment is fundamentally changing [1]. The traditional understanding of conflict as an open armed clash is giving way to a reality where information operations, psychological campaigns, cyber-attacks, and public opinion manipulation are as effective tools of power as tanks, artillery, or missiles. Hybrid threats, as complex, dynamic, and often subtle forms of hostile action [30], pose a significant challenge to the security systems of democratic states, especially regarding their ability to respond promptly, protect the public sphere, and maintain public trust in institutions [2] [3] [34].

In this context, strategic communication gains increasing importance, becoming not only a tool for government information dissemination but, more importantly, a tool for active resistance against hybrid influence. It is not merely a technical or media discipline, but an interdisciplinary and security-political instrument whose purpose is to shape public awareness, strengthen societal resilience, and narratively counter external and internal attempts to destabilize the democratic order [4] [5].

Hybrid operations, as demonstrated, for example, during the Russian annexation of Crimea, the Covid-19 pandemic, or influence operations related to the war in Ukraine, primarily target the vulnerabilities of the information space, disrupt social cohesion, and erode trust in the state [1]. Strategic communication specifically represents a preventive and reactive mechanism that can significantly contribute to society's resilience against these forms of influence.

Over the last decade, there has been a fundamental shift in the understanding of threats within the political and security practices of states. Linear and identifiable security challenges have been replaced by complex, multi-domain, and non-linear forms of engagement [6]. Hybrid threats, which combine diplomatic, informational, military, economic, cyber,

and psychological tools (the so-called DIMEFIL spectrum), are often characterized by remaining below the threshold of military response and formal securitization, thereby effectively weakening the reactive mechanisms of democratic regimes [7] [31].

Strategic communication, when properly implemented, coordinated, and targeted, can play a pivotal role in anticipating and neutralizing hybrid influences. It's more than just information transfer; it's about purposefully building trustworthy narratives, strengthening societal resilience, preventing polarization, and fostering media literacy among citizens [8] [9].

At the same time, it's a tool that requires inter-sectoral cooperation among government, security forces, academia, media, and civil society. In the context of increasing technological interconnectedness [32], rapid information virality, and the spread of various disinformation [36], conspiracy theories, and hoaxes through social networks [10], strategic communication must become a fundamental pillar of every democratic state's security policy [11].

Despite a growing consensus on the importance of strategic communication in addressing hybrid threats, there's significant variability in its understanding, implementation, and effectiveness evaluation within academic literature and practice [4]. Research attention often focuses either on the military aspects of hybrid operations or on the media and sociological dimensions of communication, while a comprehensive bridge between strategic communication as a security tool and hybrid threats as a systemic challenge remains partially unexplored.

Therefore, this article emphasizes the analytical reflection and conceptual grounding of strategic communication as one of the key tools in the fight against hybrid threats, drawing on multiple analytical dimensions: normative-security, institutional, communication, and political-strategic. The primary goal of the article is to explore how strategic communication can effectively contribute to building state resilience against hybrid threats and to identify its capabilities, limitations, and recommendations for practice.

For these purposes, the article addresses the following research questions:

1. How can strategic communication and hybrid threats be conceptually defined within the contemporary security discourse?
2. What are the main functions and tools of strategic communication in the context of defence against hybrid threats?
3. To what extent can strategic communication strengthen the resilience of democratic societies and support an effective response to hybrid operations?
4. What challenges, risks, and dilemmas arise from the implementation of strategic communication as a national security tool?

From a methodological perspective, the article adopts a qualitative research design, combining conceptual analysis, document analysis, and a critical-discursive approach. The work draws upon the study of primary government documents (e.g., The Concept of Strategic Communication of the Slovak Republic, National Strategy for Countering Hybrid Activities), academic studies, as well as expert research from institutions such as StratCom CoE, NATO, and Hybrid CoE.

The paper is structured into four main chapters. The first is dedicated to the theoretical and conceptual foundations of strategic communication and hybrid threats. The second chapter analyses strategic communication as a tool of state action. The third chapter focuses on its application in the fight against hybrid threats. The fourth chapter identifies challenges, limitations, and recommendations for the effective use of this tool. The conclusion then synthesizes the findings, answers the research questions, and offers an outlook for further research.

2. Theoretical and Conceptual Foundations

Strategic communication and hybrid threats represent two interconnected areas whose significance has rapidly increased in the contemporary security environment. In this new landscape, conflicts are increasingly waged in the realm of narratives, perceptions, informational credibility, and psychological manipulation. While strategic communication is developing as a complex tool of government action and active shaping of the information space, hybrid threats represent a sophisticated and adaptable type of hostile activity that requires precise conceptual understanding.

The term strategic communication is interpreted diversely in the academic literature, reflecting its interdisciplinary nature. It integrates insights from political science, security studies, communication sciences, psychology, and strategic studies [4] [11]. In its broadest sense, strategic communication is understood as the deliberate, coordinated, and long-term activity of government and public institutions aimed at achieving strategic objectives by influencing the perceptions, behaviours, and attitudes of target groups [5] [33].

According to the official Slovak framework, it involves "communication that ensures the transparency, trustworthiness, and openness of the state towards citizens, as well as a unified and timely response to disinformation, polarizing narratives, and influence operations" [9]. Strategic communication also relies on proactivity, coordination, reactivity, value-based anchoring, and long-term planning, thus extending beyond ordinary political communication and PR activities.

On an analytical level, strategic communication can be understood in two ways:

- As a tool of political power and governance, through which the state not only explains its actions but also builds narrative frameworks of reality and creates value ties between the state and society.

- As part of a broader security apparatus, where it plays an important role in building resilience, detecting hostile operations, and neutralizing their impact on society [12] [13].

The concept of hybrid threats emerged in response to the changing nature of conflicts in the 21st century, where military and non-military tools are increasingly intertwined in the struggle for strategic advantage. The conceptual roots of this term trace back to the 1990s, with Robert Walker [14] often cited as one of its earliest users. He has spoken of "hybrid forces" as "flexible formations capable of operating across conventional and special domains." Later, Frank Hoffman significantly elaborated on the concept, warning in 2007 that future conflicts would be characterized by a blend of conventional, irregular, and criminal forms of violence alongside cyber and information operations [6].

A fundamental shift in the understanding of hybrid threats occurred after Russia's annexation of Crimea in 2014. This event demonstrated that power interests could be advanced through a combination of asymmetric tools, influence operations, disinformation, and the exploitation of societal vulnerabilities, with conventional military action playing a secondary, supporting role [1]. In this regard, Ivančik and Nečas state that hybrid activities are characterized by subtlety, legal and narrative ambivalence, and a tendency to operate "below the threshold of war," which significantly complicates their attribution and response [3].

Currently, there are several definitions of hybrid threats that reflect different analytical and strategic approaches. According to the National Strategy for Countering Hybrid Activities, they refer to "covert and overt activities by state or non-state actors, directed against vulnerable elements of a democratic state and society, utilizing combined and synchronized tools—political, diplomatic, informational, military, economic, and intelligence—with the aim of destabilizing, disorganizing, and influencing decision-making." [15].

This approach emphasizes the strategic complexity, diffused nature of actors, and focus on systemic weaknesses of a democratic regime. Hybrid threats are thus characterized by low attributability, the interconnectedness of various domains (cyber, information, diplomatic, military, economic), the use of both legal and illegal means, and an effort to induce a psychological, political, or societal effect [2].

From the perspective of international organizations, NATO [28] defines hybrid threats as "a combination of military and non-military, as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, the deployment of irregular armed groups, and the use of conventional forces." Hybrid methods are employed to blur the lines between war and peace, aiming to sow doubt in the minds of the target population. Their objective is to destabilize and undermine societies.

The European Union [17] uses a broader definition, stating that "hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives. Hybrid campaigns are multidimensional, combining coercive and subversive measures using both conventional and unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion that hinders rapid and effective decision-making."

Given the nature of hybrid threats, which are largely based on manipulating information, creating narrative frameworks, and psychologically influencing the public, strategic communication plays a crucial role as a defensive and preventive state tool. Hybrid operations, by their very nature, do not focus on kinetic confrontation but rather on undermining trust in institutions, questioning facts, and blurring the line between reality and fiction [3] [7] [16].

Strategic communication can respond to these challenges in three fundamental ways:

- a) Proactively – by building societal immunity, resilience, and media literacy through positive narratives, values, and symbols (e.g., the credibility of democratic institutions, the unity of EU and NATO membership).
- b) Reactively – by timely detection and correction of disinformation, half-truths, and manipulative content spreading in the public sphere.
- c) Strategically – through long-term planning, building narrative frameworks, inter-sectoral coordination, and streamlining decision-making during communication crises [5] [7] [9].

There's an inverse relationship between strategic communication and hybrid threats. While hybrid activities aim to weaken a state from within through disinformation, fragmenting public opinion, and undermining legitimacy, strategic communication works in the opposite way—it unifies, strengthens, explains, and restores trust. This contrast between "disintegrating" and "integrating" action is analytically crucial for understanding strategic communication as a tool for ensuring national security.

The concept of narrative conflict also deserves special attention, as the struggle between the state and hybrid actors unfolds at the level of interpreting reality. Narratives about a "failing West," the "EU's double standards," "lost sovereignty," or "being dragged into war" are common examples of hybrid influence. Strategic communication must counter these with its own value-driven, authentic, and inclusive stories.

One of the main challenges in studying strategic communication and hybrid threats is their terminological and analytical ambiguity. Various authors and institutions often use terms like hybrid warfare, hybrid activities, disinformation operations, strategic influence, or information manipulation interchangeably. This leads to dispersed research approaches and methodological inconsistency [18]. Some authors prefer a narrower military framework, while others advocate for a broader political-social understanding of hybrid threats as a multidisciplinary phenomenon [10].

Similarly, strategic communication is often reduced to a crisis public relations tool, without reflecting on its strategic, security, and democratic functions. This reduction leads to underestimating its potential in preventing polarization, building resistance to manipulation, and maintaining social cohesion. Therefore, it's necessary to understand

strategic communication not just as an add-on to security policy, but as an integral part of state resilience, operating across political, informational, and social domains.

From a conceptual standpoint, we can therefore conclude that:

- Strategic communication represents a dynamic, multidimensional, and value-anchored tool whose effectiveness depends on credibility, coordination, and the ability to anticipate threats.
- Hybrid threats constitute a form of non-linear conflict characterized not by a front line, but by a struggle for perception, loyalty, and narrative dominance in the information space.
- The interaction between these two phenomena is asymmetrical and psychological: the state responds to hybrid activities not through kinetic means, but through communicative and narrative ones [2] [4] [7] [10] [12] [16] [19].

This establishes a solid foundation for further analysis of how strategic communication can operationalize its defensive and preventive function in specific security contexts, which will be the subject of the following chapter.

3. Strategic Communication as a Tool for State Defence

From the state's perspective, strategic communication isn't merely a form of public expression; it's a systemic tool for defence, crisis prevention, and building trustworthiness with citizens. In the context of hybrid threats, its importance shifts from a passive informational function towards actively creating narratives that bolster societal resilience against both external and internal disruption [8] [9].

Strategic communication isn't an isolated activity; rather, it's a coordination platform among multiple actors: government institutions (ministries, government, security forces), security and intelligence agencies, and the media, academia, expert community, and civil society. This form of communication extends beyond traditional government PR. Its goal is not only to inform but also to create interpretive frameworks that shape the perception of events and strengthen values like democracy, the rule of law, social cohesion, and geopolitical orientation [5]. It's precisely these values that are often the target of hybrid threats—their questioning, blurring, or devaluation weakens the legitimacy of a democratic regime. Psychologists and scientists who study the influence of human behaviour and decision-making processes believe that critical thinking is a relatively insignificant part of solving everyday situations compared to human spontaneity [20].

Governments that implement strategic communication as part of their national security strategy understand that responding to hybrid activities cannot be solely repressive or technocratic. The fear as a social and political phenomenon is only shaped by power relations, social structures, and broader socio-political dynamics. From a sociopolitical perspective, fear is not solely an individual psychological experience but is shaped and influenced by larger social forces [21]. Actively shaping societal resilience is essential, achieved through trustworthy narratives that not only answer disinformation but also preventatively neutralize it by reducing its effectiveness on target audiences [3] [4] [22].

Strategic communication plays a multi-layered role in state defence. It's not just a tool for relaying information, but also a way to build resilience against hybrid operations, foster internal societal integrity, and enhance the effectiveness of government decision-making in crisis situations [23]. In security practice, its functions can be categorized as follows:

- Informational Function – Ensures accurate, timely, and understandable information for citizens during peacetime, crisis, and war. It prevents the spread of panic, destabilization, and information chaos.
- Coordination Function – Unites the communication activities of various state components into a cohesive framework, preventing inconsistencies, ambiguities, and inter-departmental information failures.
- Preventive Function – Works to increase societal resilience, strengthening media literacy, critical thinking, and social immunity to manipulation.
- Norm-setting Function – Creates narratives that shape the value-based anchoring of society, as well as state identities within the geopolitical and cultural sphere.

From the perspective of operational domains, strategic communication is applied in:

- The political sphere – explaining public policies and state actions.
- The security sphere – countering hybrid threats, disinformation, and cyber-attacks.
- The social sphere – increasing trust in institutions, preventing polarization and radicalization.
- The international sphere – enhancing state reputation, public diplomacy, and strategic positioning.

The main tools of strategic communication include [11] [24]:

- Government press briefings and official communiqués.
- Online platforms and digital communication (web portals, social media).
- Information campaigns, educational programs, and media literacy initiatives.
- Involving both public and private media in crisis communication.
- Analytical and intelligence reports for detecting narrative operations.

In practice, effective strategic communication proves to be flexible, integrated, and supported by thorough analysis of target groups. High-quality communication campaigns leverage insights from behavioural sciences, psychology, linguistics, and media studies—it's not improvisation, but strategic planning based on research and data [4].

In recent years, the concept of resilience has gained prominence in security discourse. It refers to a society's ability to resist, absorb, and adapt to various types of crises, including hybrid threats. In this context, strategic

communication plays a crucial role, acting not as a passive reaction to threats, but as a tool for cultivating resilience even in the pre-crisis stage [8].

Resilience isn't merely about the technical preparedness of state structures; it also encompasses the psychological and social capacity of the populace to avoid panic, manipulation, or distrust towards institutions. Strategic communication contributes to building this resilience through:

- Long-term transparency in government communication.
- A consistent value framework.
- An expert and factual approach to crisis topics.
- Active public engagement and strengthening media literacy.

Part of this effort involves educating the public about disinformation and manipulative techniques, thereby creating a "natural firewall" against hybrid activities. As experiences from the Baltic States, Scandinavia, and Finland show, publicly funded campaigns, media education, and community projects focused on critical thinking significantly bolster societal immunity [19] and social coherence and awareness [29].

However, resilience isn't solely about audience robustness; it's also about the readiness of institutions to communicate during a crisis—and to do so quickly, factually, and without conflicting signals. In this sense, strategic communication is closely intertwined with crisis communication, which forms its reactive component.

Effective crisis communication is that which [23]:

- Prevents an information vacuum.
- Coordinates messages across different ministries.
- Considers the emotional state of the audience.
- Offers solutions and perspective, not just warnings.

Poorly managed communication in crisis situations—for example, during a pandemic, a cyber-attack, or a geopolitical conflict—can undermine state legitimacy and strengthen the effects of hybrid narratives. Conversely, well-managed communication can not only handle a crisis but even strengthen social bonds and increase trust in public institutions.

A clearly defined institutional framework and established competencies are crucial for effective strategic communication. These ensure coordination among various state administration actors. Experiences from Slovakia and Czechia show that without political will, a stable managing centre, and inter-institutional cooperation, strategic communication becomes ineffective or fragmented.

In Slovakia, the government adopted the "Concept of Strategic Communication of the Slovak Republic" in 2023, representing the first comprehensive framework for this area. It defines strategic communication as "coordinated, timely, and targeted use of state communication tools to strengthen societal resilience and protect democratic values" [9]. The document introduces several principles: unity, trustworthiness, transparency, participation, and timeliness.

However, the Concept also identifies several challenges, including:

- Low levels of personnel and analytical capacities.
- Missing methodologies for evaluating communication effectiveness.
- Weak interconnectedness between the security apparatus and communication departments.
- Insufficient integration of strategic communication into crisis management.

The Czech Republic is several years ahead in this area. As early as 2018, the Centre Against Hybrid Threats (CPHH) was established as a specialized workplace within the Ministry of Interior, focusing on analysis, training, and methodological support for public administration bodies. In 2021, the "National Strategy for Countering Hybrid Activities" was adopted, designating strategic communication as a key pillar of national security and promoting a "whole-of-government approach" [15].

A strength of Czech practice is the creation of a communication matrix during crises (e.g., COVID-19, the war in Ukraine), which allows for rapid coordination of messages among individual ministries and targeted information distribution to the public. A weakness, however, remains the persistent distrust of a portion of the public towards official narratives, linked to a long-term absence of media education and a high degree of conspiratorial thinking [25].

Both cases indicate that effective strategic communication requires:

- Strong central governance (e.g., under the Government Office).
- Sufficient analytical and personnel capacities.
- Integrated connection with security forces, crisis management, and local government.

Continuous evaluation of communication campaign effectiveness and adaptation of strategy to target groups.

4. Strategic Communication in the Context of Countering Hybrid Threats

Hybrid threats are currently considered one of the most serious challenges to the security of democratic states. Their essence lies in their ability to combine military and non-military, conventional and unconventional, lethal and non-lethal, regular and irregular forces, tools, techniques, and means [10]. The military forces in a hybrid war are basically responsible for creating and maintaining the conditions required by other entities or in favour of other power tools [35]. Increasingly, the emphasis is placed on the informational and psychological dimensions of conflict. In such an

environment, strategic communication becomes not only a tool for defence and protection but also a form of anticipation and narrative counter-offensive, enabling the timely detection, neutralization, and delegitimization of hostile activities.

Hybrid activities often operate in the so-called "grey zone" between peace and war, where state and non-state actors use disinformation, psychological operations, cyber-attacks, economic pressure, and subversive diplomacy to weaken geopolitical adversaries without formally crossing the threshold of armed conflict [2] [3] [26]. This is precisely why effectively countering these threats requires the ability to respond quickly and credibly. This response shouldn't be merely defensive, but actively shape public perceptions, attitudes, and values. In this context, strategic communication functions as the "first contact" with hybrid activities—not with weapons, but with facts, narratives, and trustworthiness.

In practice, this means that if a hybrid actor seeks to destabilize society through false narratives that question the legitimacy of state institutions, membership in the EU or NATO, or promote conspiratorial and divisive themes, the state must be able to identify these narratives promptly and offer an alternative. This alternative must be not only factually correct but also anchored in values and culture [10]. Such an alternative does not emerge spontaneously; it must be the result of strategic planning, understanding target groups, and coordinated action by public actors. In this regard, strategic communication is more than just a response to threats—it's a form of strategic action aimed at building society's "mental resilience" against subversive influences. An important indicator of strategic communication's significance is its functioning in real crisis situations. One of the most significant examples was the COVID-19 pandemic, which revealed the extent to which state institutions were prepared to communicate a crisis consistently, convincingly, and strategically. The pandemic was accompanied by extensive hybrid activity, including the spread of disinformation about the virus's origin, vaccine effectiveness, the role of international organizations, and the alleged totalitarian nature of government measures. It became evident during this period that inconsistent, uncoordinated, and untrustworthy government communication significantly increases society's vulnerability to manipulative content and alternative narratives that threaten health, social cohesion, and trust in institutions [7] [25]. A similar example could be, especially with an emphasis on the deteriorating international security and political situation, whether the state is addressing the capabilities of domestic industry to provide equipment with weapons systems and other segments of the arms product portfolio [27].

Conversely, countries that relied on a proactively established strategic communication framework, such as Finland, Estonia, and Lithuania, were better able to counter this wave of hybrid threats. In their case, not only institutional preparedness and consistent planning of communication steps played a key role, but also long-term engagement with society—supporting media literacy, educating about disinformation, and active cooperation with the civil sector. Finland's Comprehensive Security Concept, for example, includes strategic communication as one of the fundamental pillars of national security, considering it on par with intelligence and military capabilities [19].

Another pivotal moment for the application of strategic communication was the start of the full-scale Russian invasion of Ukraine in February 2022. Moscow's hybrid activities had been noticeable long before this, particularly through the spread of narratives about the alleged genocide of the Russian-speaking population in Donbas, the need for "denazification" of Ukraine, or the hostile encirclement of Russia by the West [1]. These narratives were massively disseminated through allied media, social networks, various proxy platforms, and diplomatic statements. Their aim was to undermine the unity of the EU and NATO, divide Western public opinion, and legitimize the aggression in the eyes of the international community [16].

In this scenario, strategic communication proved to be of decisive importance—not only for defence but also for public mobilization, shaping international support, and narratively isolating the aggressor. Thanks to centralized and exceptionally effective strategic communication, Ukraine managed not only to maintain the trust of its population but also to create a strong and credible international narrative about defending freedom, sovereignty, and European values. Ukrainian President Volodymyr Zelenskyy and his team utilized modern communication channels—from social media to regular video appeals to the public—to maintain a continuous moral story that provided the world with a framework for identifying with a state attacked simultaneously by hybrid and conventional means.

These cases demonstrate that strategic communication is not merely an "appendage" to crisis management but a constitutive element of national and collective defence. When properly coordinated, supported by analytical data, ethically anchored, and oriented toward a long-term goal, it can not only react to disinformation but also prevent it by creating an information space where truth is credible, facts are distinguishable, and institutions are respected.

An analysis of past experiences shows that the success of strategic communication in combating hybrid threats depends on several key factors. The first is the credibility of the communicating institutions—without it, even factually correct information becomes insufficiently convincing and prone to questioning. Trust, in turn, is the result of a long-term relationship between the state and society, the quality of which is influenced by the transparency, predictability, and consistency of government action.

The second factor is informational speed and coherence. In an environment where disinformation spreads with viral speed and emotional charge, a state cannot respond slowly or ambiguously. The absence of timely and understandable communication creates a narrative "vacuum" that is immediately filled by hybrid actors. Therefore, it's essential for the state to have prepared crisis communication scenarios, trained spokespeople, and an interconnected network of analytical and communication units.

The third factor is knowledge of the target audience. Strategic communication cannot be universal; it must be targeted, culturally sensitive, and segmented according to the communication habits, media consumption, and value orientation of individual groups. For example, young people will be more sensitive to visual and digital content, while

older citizens prefer traditional media. Ignoring these differences leads to ineffectiveness or, worse, to increased public frustration and resignation.

The fourth aspect is ethical integrity. Communication aimed at combating hybrid threats must not itself descend into manipulation, propaganda, or concealment. Successful strategic communication is based on value consistency, respect for the audience, and openness of discourse, which fundamentally distinguishes it from hybrid tactics that operate through deception, polarization, and subversion. Ethics and trustworthiness are not weaknesses, but a key prerequisite for effectiveness.

From the above, it follows that strategic communication is currently one of the few tools capable of acting preventively, reactively, and transformatively at the same time. Its effective use allows not only for defence against hybrid attacks but also for the restoration of trust in the democratic process, the strengthening of informational resilience, and the creation of a culture of dialogue based on facts. However, for this to happen, it must be part of a broader security and societal strategy, not an isolated PR activity.

5. Conclusion

In the context of contemporary security challenges, strategic communication has unequivocally established itself as a crucial tool in the fight against hybrid threats. It possesses not only an informational and political dimension but also a security, normative, and societal one. As the analysis in this article has shown, it is a multidimensional and dynamic instrument that transcends the traditional understanding of government communication. It serves as a strategic pillar in times of uncertainty, polarization, and systemic vulnerability. In an information-saturated environment marked by narrative conflicts, psychological operations, and the mass spread of disinformation, strategic communication is one of the few tools democratic states can employ to counter hybrid threats without jeopardizing their own value-based and legal foundations. The synthesis of findings indicates that strategic communication combines long-term planning, value orientation, narrative creation, crisis management, and civic participation. This makes it a key bridge between security policy and societal resilience. Hybrid activities, which seek to weaken institutions from within, fragment public opinion, and undermine citizen trust, can only be effectively neutralized if the state acts clearly, quickly, ethically, and strategically—precisely within the framework of well-established communication.

In this context, the research questions can be answered as follows:

1. How can strategic communication and hybrid threats be conceptually defined in the contemporary security discourse? Strategic communication in the current discourse is understood as a deliberate, coordinated, and long-term planned state activity that uses communication means to support strategic goals, defend the value framework, and strengthen societal resilience. It's not just about informing but about shaping perceptions and narrative frameworks that give security and political actions legitimacy and clarity. Hybrid threats, conversely, are diffuse, combined, and adaptable forms of hostile activity that exploit the weaknesses of open societies—especially in the informational, cyber, psychological, and social spheres. A key element of hybrid threats is their low attributability and ability to operate below the threshold of military response.

2. What are the main functions and tools of strategic communication in the context of defence against hybrid threats? The main functions of strategic communication can be summarized into four categories: informational (timely and accurate informing), coordinating (harmonizing state communication), preventive (building societal immunity), and norm-setting (shaping society's value framework). Its tools include press outputs, digital platforms, analytical reports, targeted campaigns, community projects, and informal forms of participatory discourse. Successful strategic communication relies on trustworthiness, clear narratives, knowledge of target groups, and the use of behavioural insights.

3. To what extent can strategic communication strengthen the resilience of democratic societies and support an effective response to hybrid activities? Strategic communication has significant potential to strengthen societal resilience, provided it's implemented systematically, long-term, and participatively. It contributes to increasing media literacy, cultivating critical thinking, restoring trust in public institutions, and reducing societal polarization. Furthermore, it supports the state's adaptive capacity to respond to crises caused by hybrid attacks while minimizing the effects of narrative and psychological operations aimed at fragmenting public discourse. Successful communication can not only react but also prevent waves of disinformation by creating a robust and trustworthy information space.

4. What challenges, risks, and dilemmas arise from implementing strategic communication as a national security tool? Implementing strategic communication faces several challenges: insufficient institutionalization, limited personnel and technical capacities, poor coordination among ministries, a lack of analytical tools, and the risk of crossing the line between communication and propaganda. The democratic state confronts complex dilemmas: how to effectively respond to hybrid activities without violating principles of free speech, how to regulate digital platforms without infringing on privacy, and how to create compelling narratives without manipulation. These challenges require ethically grounded, legally precise, and participative approaches that integrate strategic communication into a broader security culture.

From a normative perspective, it's clear that strategic communication can't remain solely within the domain of crisis management or public relations. It must be understood as an integral element of democratic resilience, collective security, and strategic planning. Its importance will grow proportionally with the sophistication of hybrid activities. Therefore, it needs to be firmly embedded in national security policies, supported by interdisciplinary research, and built on cooperation between the state, experts, the media, and civil society.

For future research, several open questions remain. Further investigation is needed into the measurability of strategic communication's effectiveness, its impact on changes in audience behaviour, and the psychological and cultural factors influencing the perception of trustworthiness. Promising areas also include the development of narrative frameworks in the digital space, the use of artificial intelligence in detecting disinformation campaigns, and the evaluation of the impact of ethical dilemmas on communication effectiveness.

In conclusion, strategic communication is an indispensable component of the security architecture of democratic states today. Its power lies not just in words or images, but in its ability to build a resilient society that understands its values, comprehends risks, and is prepared to defend an open and free public space.

Acknowledgements. The paper has been supported by the outputs of the research project "N14200646 - Concept of the Slovak Armed Forces operations in the information domain" funded by the Ministry of Defence of the Slovak Republic through the inter-ministerial sub-program 06E0I-Research and development in support of state defence.

References

1. **Jurčák, V. & Ivančík, R.** The conflict in Ukraine – A Turning Point for Security and Defence of the EU? In *Security Dimensions*, 2023, č. 44, s. 84-101. ISSN 2353-7000. Retrieved from: <https://doi.org/10.5604/01.3001.0054.1744>
2. **Mareš, M., Kraus, J. & Drmola, J.** Conceptualisation of Hybrid Interference in the Czech Republic: How to Make it a Practically Researchable Phenomenon? In *Politics in Central Europe*, 2022, Vol. 18, No. 3, pp. 343-354. ISSN 2787-9038. Retrieved from: <https://doi.org/10.2478/pce-2022-0015>
3. **Ivančík, R., Nečas, P., & Ilaščíková, L.** Attention as a Commodity in the World of Disinformation and Social Media. In *Entrepreneurship and Sustainability Issues*, 2024, Vol. 12, No. 2, pp. 176-192. ISSN 2345-0282. Retrieved from: <https://doi.org/10.9770/k7393698996>
4. **Bērziņa Čerenkova, U. A. & Pamment, J. et al.** Hybrid Threats: A Strategic Communications Perspective. In *NATO Strategic Communications Centre of Excellence*, 2019. Retrieved from: https://stratcomcoe.org/pdfs/?file=/publications/download/2nd_book_short_digi_pdf.pdf?zoom=page-fit
5. **Táborský, J.** *V síti dezinformací*. Praha: Grada Publishing, 2019. ISBN 978-80-271-1066-7.
6. **Hoffman, F.** *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, 2007. Retrieved from: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
7. **Divišová, V.** Strategická komunikace: od reaktivního boje s dezinformacemi po komplexní využití v oblasti národní bezpečnosti a obrany státu. In *Vojenské rozhledy*, 2022, Vol. 31, No. 2, pp. 34-53. ISSN 2336-2995. Retrieved from: <https://www.doi.org/10.3849/2336-2995.31.2022.02.034-053>
8. **Sanders, K. & Caner, M. J.** *Government Communication: Cases and Challenges*. London: Bloomsbury Academic, 2013. ISBN 978-1-849-66612-1.
9. **GOSR.** *Strategic Communication Concept of the Slovak Republic*. Bratislava: Government Office of the Slovak Republic, 2023. Retrieved from: <https://www.stratkom.gov.sk/site/assets/files/6363/ksk.pdf>
10. **Ivančík, R. & Andrassy, V.** On Some Factors Contributing to Belief in Conspiracy Theories. *Academic Journal of Interdisciplinary Studies*, 2023, Vol. 12, No. 3, pp. 16-32. Retrieved from: <https://doi.org/10.36941/ajis-2023-0056>
11. **Blumler, J. G.** Core Theories of Political Communication: Foundational and Freshly Minted. In *Communication Theory*, 2015, Vol. 25, No. 4, pp. 426-438. ISSN 1050-3293. Retrieved from: <https://doi.org/10.1111/comt.12077>
12. **Bolt, N., Stolze, M., Haiden, L. & Althuis, J.** Understanding Strategic Communication. In *NATO Strategic Communications Centre of Excellence*, 2023. ISBN 978-9934-619-40-3. Review of Policy Research, 2024. Retrieved from: <https://stratcomcoe.org/pdfs/?file=/publications/download/Terminology-Report-No3-DIGITAL.pdf?zoom=page-fit>
13. **McGovern, R. & Jones, M. D.** The narrative policy framework and institutions. In *Review of Policy Research*, 2024. Retrieved from: <https://doi.org/10.1111/ropr.12616>
14. **Walker, R. G.** SPEC FI: the United States Marine Corps and Special Operations. In *The NPS Institutional Archive*, 1998. Retrieved from: <https://core.ac.uk/download/pdf/36702547.pdf>
15. **MOCR.** *National strategy for countering hybrid threats*. Praha: Ministry of Defence of the Czech Republic, 2021. Retrieved from: <https://mocr.mo.gov.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf>
16. **NATO.** NATO's approach to counter information threats. In *North Atlantic Treaty Organization*, 2025. Retrieved from: https://www.nato.int/cps/en/natohq/topics_219728.htm
17. **EU.** A Europe that Protects: Countering Hybrid Threats. In *European External Action Service*, 2018. Retrieved from: https://www.dsn.gob.es/sites/dsn/files/hybrid_threats_en_final.pdf
18. **Monaghan, S.** Countering Hybrid Warfare: So What for the Joint Force? In *PRISM*, 2019, Vol. 8, No. 2, pp. 83-98. ISSN 2157- 0663. Retrieved from: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf?ver=2019-09-17-231051-890

19. **Pynnöniemi, K. & Saari, S.** Hybrid influence – lessons from Finland. In *NATO Review*, 2017. Retrieved from: <https://www.nato.int/docu/review/articles/2017/06/28/hybrid-influence-lessons-from-finland/index.html>
20. **Kolomazník, T.** Strategic Communication's Role in Eliminating Disinformation's Impact in Time of Current Geopolitical Challenges. In *Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation*, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.99
21. **Vlasova, O.** War's Shadow: Exploring Multifaceted Strategies in the Politics of Fear. In *Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation*, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.161
22. **Turchenko, Y.** Cross-Cultural Comparisons for the Analysis of Disinformation in a Geopolitical Context: Case of Ukraine. In *Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation*, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.178
23. **Tomandl, J., Čuřík, J., Maršovská, K. & Fojtová, T.** *Krizová komunikace*. Brno: Masarykova univerzita, 2020. ISBN 978-80-210-9636-3.
24. **Ftorek, J.** 2017. *Manipulace a propaganda na pozadí současné informační války*. Praha: Grada, 2017. 200 s. ISBN 978-80-2710-605-9.
25. **Bízík, V., Kosárová, D., Potočňák, A. & Stojar, R.** Empirical Test of the Multi-Dimensional Concept of “Hybrid”. In *Obrana a strategie*, 2022, Vol. 22, No. 1, pp. 75-88. ISSN 1802-7199. Retrieved from: <https://www.doi.org/10.3849/1802-7199.22.2022.01.075-088>
26. **Andrassy, V. & Ondruš, M.** The Gray Zone and Its Place in Security Environment. In *Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation*, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.90
27. **Novák, J., Potužák, L., Blaha M., Šlouf, V. & Drábek, J.** The impact of the deteriorated political and security situation on the financial stability of arms companies operating in an oligopolistic market environment. In *Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation*, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.500
28. **NATO.** Countering hybrid threats. In *North Atlantic Treaty Organization*, 2024. Retrieved from: https://www.nato.int/cps/en/natohq/topics_156338.htm
29. **Keršanskas, V.** Deterrence: Proposing a more strategic approach to countering hybrid threats. In *Hybrid CoE*, 2020, Paper 2. ISBN 978-952-7282-33-5. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf
30. **Kompan, J., Hrnčiar, M. & Brezina, D.** AI in Mobility Support Management in Hybrid Warfare. In: Kabashkin, I., Yatskiv, I., Prentkovskis, O. (eds) *Reliability and Statistics in Transportation and Communication: Human Sustainability and Resilience in the Digital Age*. RelStat 2024. Lecture Notes in Networks and Systems, vol 1337. Springer, Cham., 2025. https://doi.org/10.1007/978-3-031-87532-8_9
31. **Brezina, D. & Kompan, J.** Evaluation of Modern Approaches to Crisis Management. In *Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation*, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. pp. 397-402. DOI: 10.3849/cndcgs.2024.397
32. **Conte, M.M., Roman, F., Sacchet, M., Spinello, E., Molnár, A., Attias, S., Tudorache, P., Kompan, J. & Dolan, A.** Students' perception of international collaboration and cultural Understanding in digitally driven education. *Proceedings of the International Conferences on e-Learning and Digital Learning 2024, ELDL 2024; Sustainability, Technology and Education 2024, STE 2024*, pp. 145-153.
33. **Belan, L. & Petrufová, M.** Behaviour of members of the Slovak republic armed forces in crisis situations. In *Politické Vedy*, 2021, Vol. 24, No. 1, pp. 70-94. ISSN 1335–2741. Retrieved from: <https://doi.org/10.24040/politickevedy.2021.24.1.70-94>
34. **Chovanec, D., Kollár, B., Ristvej, J., Jelšík, J. & Andrassy, V.** Application of artificial intelligence for decision support within crisis management. In: *Modelling and simulation 2025*, Ostend: EUROSIS-ETI, 2025, ISBN 9789492859389. Retrieved from: <https://www.eurosis.org/cms/files/proceedings/ESM/ESM2025contents.pdf>
35. **Kompan, J., Turaj, M. & Vajda, M.** Operational Environment. In: *Hybrid Warfare Reference Curriculum Volume 1 = Compulsory Lectures*, Budapest: Ludovika University Press, 2024, pp. 99-128. ISBN 978-963-653-031-0. Retrieved from: https://doi.org/10.36250/01195_06
36. **Belica, B.** Artificial Intelligence and Disinformation: Opportunity or Threat? In: *Vojenské reflexie*, 2024, Vol. XIX, No. 3, pp. 61-73. ISSN 1336-9202. Retrieved from: <https://doi.org/10.52651/vr.a.2024.3.61-73>.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of CNDCGS 2026 and/or the editor(s). CNDCGS 2026 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.