POLITICAL COMMUNICATION IN THE CONTEXT OF HYBRID THREATS: A STRATEGIC RESOURCE FOR NATIONAL SECURITY

Roman Shykhutskyi
Applicant, Mykhailo Dragomanov National University of Ukraine, Ukraine
e-mail: r.shykhutskyi@meta.ua, orcid.org/0009-0008-5840-8232

Summary

The article examines political communication in the context of hybrid threats and the full-scale war against Ukraine, viewing the information space as a critical battlefield of contemporary confrontation. It demonstrates that communication is no longer merely an auxiliary tool but has evolved into a strategic resource of national security, shaping the legitimacy of decisions, mobilizing public support, and influencing the international reputation of the state.

The theoretical framework is grounded in approaches that conceptualize hybrid warfare as a synergy of military and non-military methods of influence, including cyberattacks, information campaigns, and economic pressure. Within this configuration, the cognitive dimension becomes especially significant, as the creation of an alternative reality through manipulative narratives and microtargeting complicates the distinction between a state of war and "normal" politics.

The Ukrainian case highlights the systematic and large-scale nature of informational aggression aimed at delegitimizing institutions and polarizing society. At the same time, coordinated strategic communications have enabled the alignment of messaging across governmental bodies, the development of a unified narrative, and the maintenance of both internal cohesion and external support.

Methodologically, the article employs an interdisciplinary toolkit: discourse and content analysis to identify semantic constructs and recurring themes; case studies to trace the dynamics of crisis campaigns; surveys and statistical modeling to measure effects; network analysis to pinpoint nodes of information dissemination; and disinformation monitoring using AI algorithms to detect anomalies in content propagation.

Practical recommendations are structured around three key areas: prevention, coordination, and response. They include principles of transparency, accuracy, and timeliness; continuous information dissemination to avoid creating a "vacuum"; institutionalization of fact-checking and debunking mechanisms; development of value-driven and inclusive narratives; partnerships between the state, civil society, media, and opinion leaders; and enhanced collaboration with social media platforms.

Key words: political communication, hybrid threats, strategic communications, disinformation, information security, national security, crisis management, information warfare.

DOI https://doi.org/10.23856/7126

1. Introduction

Russia's full-scale aggression against Ukraine has turned the information space into a critical battlefield of hybrid confrontation, where classical approaches to political communication have lost much of their effectiveness. The state is compelled to explore new models of response and the development of resilient communication strategies.

Large-scale disinformation campaigns and manipulative narratives erode public trust in state institutions, deepen social polarization, and weaken society's ability to achieve cohesion. In this context, political communication evolves from a mere tool of information dissemination into a vital component of national security.

At the same time, there is a lack of comprehensive methodologies for assessing the effectiveness of communication strategies and ensuring coordination between state and non-state actors. This gap underscores the need for in-depth research that integrates institutional, technological, and social dimensions of political communication development.

2. The correlation between hybrid threats and political communication

The concept of hybrid threats emerged in political science and security studies in the early 21st century as a response to the changing nature of armed conflicts and the transformation of interstate relations. In the works of Frank Hoffman, one of the first theorists of this phenomenon, hybrid threats are defined as a combination of traditional and non-traditional forms of violence, including conventional military operations, terrorist attacks, cyberattacks, and large-scale information campaigns. According to Hoffman, it is the synchronized use of these diverse tools that creates a multidimensional pressure effect, undermining an opponent's resilience *(Hoffman, 2007).*

In the scholarly works of Peter Mansoor, particular emphasis is placed on the integrated nature of hybrid threats, where military force is closely intertwined with psychological influence, information attacks, and disinformation. This approach blurs the line between war and peace, creating a climate of perpetual instability. In this context, information campaigns are seen as a key component of hybrid strategies, enabling covert manipulation of public sentiment *(Mansoor, 2012).*

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki offers an even broader definition of the term, encompassing information attacks, cyber intrusions, economic pressure, and manipulation of energy resources. NATO documents also interpret this phenomenon as a complex of military and non-military methods aimed at undermining stability and weakening the defensive capacity of states. This confirms that the modern understanding of hybrid threats goes far beyond the boundaries of traditional military paradigms *(Hybrid CoE, 2023).*

The informational and communicative component of hybrid threats is of strategic importance because it shapes the cognitive environment necessary to achieve political and military objectives. Its essence lies in the creation of an alternative reality that alters not only citizens' knowledge but also their emotions and behavior. This enables actors to achieve large-scale effects without the direct deployment of significant military resources.

Hybrid actors actively leverage modern data processing technologies, algorithmic targeting, and big data analytics, allowing for highly personalized influence that often remains imperceptible to individuals. In such conditions, people become targets of information attacks without realizing the manipulative nature of the content they consume *(Borgesius, 2018).*

A distinctive feature of hybrid threats is their transnational character. Information campaigns transcend national borders, shaping international discourse and influencing the positions of partners and public opinion abroad. As a result, the informational dimension of hybrid operations acquires a global scope, complicating containment efforts and necessitating coordinated responses among states.

3. Strategic communications in the context of hybrid threats

Strategic communications in the context of hybrid threats become an independent battlefield where the legitimacy of political decisions, the mobilization of public support, and the formation of a state's international image are determined. Control over information flows is no less critical than control over territories. Through communication strategies, opponents can be delegitimized, resources mobilized, and the image of the enemy constructed *(Koch, 2024).*

One of the most striking examples of hybrid warfare in the 21st century is Russia's aggression against Ukraine. The Kremlin employs information as a systematic instrument of its military-political strategy: spreading myths about the "protection of Russian-speaking populations," conducting smear campaigns against Ukrainian institutions, and leveraging propaganda channels at the international level. This demonstrates that the informational and communicative dimension is not a supplementary but a fundamental element of modern warfare, influencing outcomes as decisively as military power *(Barovska, 2016).*

A telling example of the use of information strategies in contemporary political processes is the campaign surrounding the United Kingdom's exit from the European Union. During the 2016 referendum, strategic communications became the primary tool of competition between supporters and opponents of Brexit. The mass dissemination of manipulative messages on social media, the use of false economic data regarding EU membership, and appeals to emotional factors such as national identity illustrated how the information sphere can directly shape political decisions with far-reaching international consequences *(Bastos & Mercea, 2017).*

In the context of hybrid warfare, political communication simultaneously serves as a vulnerable target of attacks and a strategic resource for resistance. Modern digital technologies allow adversaries to conduct large-scale manipulative campaigns aimed at delegitimizing state institutions, undermining trust in political leadership, and exacerbating internal social divisions. The vulnerability lies in the fact that any message in the open information space can be distorted, taken out of context, or integrated into hostile disinformation narratives.

At the same time, political communication is a key tool for enhancing state resilience against hybrid threats. Strategic communications enable the coordination of messaging across various political and governmental institutions, the alignment of narratives, and timely responses to information attacks.

This coordination fosters social unity, strengthens trust in state institutions, and enhances citizens' ability to resist external manipulation. Thus, political communication functions as a protective shield, safeguarding the information space while consolidating society.

One of the most dangerous manifestations of information aggression is the spread of disinformation, fake news, and manipulative narratives designed to delegitimize democratic processes and create an atmosphere of general distrust. Under such conditions, an effective state communication policy can not only neutralize hostile propaganda but also shape the public agenda. When built on the principles of transparency, openness, and dialogue with the public, it becomes a vital factor in reinforcing political stability and fostering social cohesion *(Bukanov, 2025).*

4. Political communication as a social phenomenon

In the era of digital media, political communication has acquired a new meaning, as information technologies have radically transformed the speed, scale, and forms of interaction between authorities, the media, and society. Social networks have created conditions for direct

communication between political actors and citizens, which, on the one hand, has made politics more accessible but, on the other, has complicated the control over the quality and accuracy of content. The digital environment has facilitated the instant dissemination of information, the formation of networked communities, and new forms of political mobilization, significantly reshaping the public sphere.

At the same time, digital communication has made the public space highly vulnerable to manipulation. Algorithmic mechanisms of social platforms incentivize the spread of sensational or emotionally charged content, deepening processes of polarization and societal radicalization. Disinformation, bot farms, synthetic media, and targeted fake content have become tools used by both domestic political actors and external players seeking to undermine democratic institutions *(Vosoughi, Roy, & Aral, 2018).*

The vulnerability of the public sphere is further exacerbated by the effect of information bubbles, within which users mostly interact with like-minded individuals. Such segmentation of the communicative space reduces critical engagement with information, complicates intergroup dialogue, and creates favorable conditions for manipulative narratives. In this environment, political communication transforms into a field of informational confrontation that shapes the quality of democracy and the level of societal resilience to hybrid threats.

5. Methods of political communication

The methodological foundation for studying political communication in the digital age is shaped by its interdisciplinary nature, integrating approaches from political science, sociology, psychology, information technology, and cybersecurity. This methodological complexity enables the analysis of multi-level communication processes, the identification of hidden mechanisms of manipulation, and the assessment of how information flows influence public opinion formation.

In social sciences, the concept of "methodology" encompasses several dimensions. Broadly, it refers to a system of principles and approaches to organizing scientific research. In a more reflexive sense, methodology represents knowledge about the very process of inquiry, allowing researchers to understand how they construct and verify their theoretical frameworks. In the socio-humanitarian sciences, methodology holds particular significance, as it not only serves as a tool for data collection but also as a means for critically interpreting complex and multidimensional social phenomena *(Tarielkin & Tsykyn, 2010).*

The field of qualitative research methods in political communication is particularly valuable, as it allows the exploration of deeper meanings and hidden structures of political interaction. By applying these approaches, researchers can analyze not only facts and messages but also the contexts in which they arise, enhancing the interpretative depth of scientific analysis. Such methods focus on uncovering the symbolic and cognitive dimensions of political processes.

Discourse analysis is one of the key tools in this regard, as it makes it possible to study the language of political texts, speeches, and media narratives within their social and ideological dimensions. This method helps identify hidden ideologemes, semantic constructs, and rhetorical strategies that shape the perception of political reality, demonstrating how language is used as a tool of power and influence *(Khudolii, 2014).*

Content analysis provides a systematic examination of large volumes of textual or media information, allowing researchers to extract key themes, track changes in communication practices, and identify strategies used by political actors. This method is particularly important in

the context of information wars, where the mass repetition of messages significantly shapes public opinion *(Bataieva, 2018)*.

The case study method focuses on analyzing specific campaigns, electoral processes, or crisis situations. Its application helps trace the dynamics of political communications in particular contexts, identify key factors behind success or failure, and derive generalized conclusions applicable to broader political processes. This approach is especially useful for examining non-standard or unique cases *(Elstub & Pomatto, 2022)*.

Public opinion surveys allow researchers to measure levels of support for political actors, evaluate the effectiveness of communication strategies, and identify shifts in societal attitudes across different socio-demographic groups. When combined with carefully designed sampling and accurate data collection tools, this approach provides a scientifically grounded picture of political processes and enables predictions about their future trajectories.

Statistical analysis serves as a key tool for processing large datasets, enabling the identification of hidden correlations, patterns, and trends in electoral behavior. Techniques such as regression and factor analysis, clustering, and modeling provide deeper insights into the relationships between informational influences and citizens' political preferences.

Network analysis is an emerging and promising direction that opens new opportunities for studying political narratives and communication structures. It enables the identification of key nodes of information dissemination, the mapping of influential actors, and the analysis of the architecture of information flows. This approach is particularly valuable for understanding coalition dynamics, the mechanisms of propagandist message spread, and the formation of information bubbles that create isolated informational environments for users *(Zaiets, 2024)*.

Disinformation monitoring holds special methodological significance, becoming a key tool in the context of hybrid threats. It involves tracking false messages, analyzing information flows, detecting bot networks, and identifying the dynamics of manipulative campaigns. The integration of machine learning algorithms and artificial intelligence technologies allows for the detection of anomalies in content distribution and enhances the effectiveness of protecting democratic processes.

In conclusion, the methodological framework for the study of political communication emerges as an integrated system that combines classical methods of social sciences with innovative digital tools. It allows researchers to capture the multidimensional nature of political communication, enhance scientific reflexivity, and effectively respond to modern challenges such as information wars, crises of trust, and the radicalization of public attitudes.

6. Practical recommendations for the development of political communication in crisis situations

Political communication in crisis situations must be grounded in clear principles, with transparency, accuracy, and timeliness being paramount. Providing society with verified information in an accessible and understandable form minimizes the risk of panic and reduces the effectiveness of manipulative influences *(Ostapenko, 2012)*.

Consistency and coherence in messaging across different state institutions foster public trust, while regular updates prevent the emergence of an information vacuum often exploited by hostile actors. Incorporating empathy as a principle ensures that the emotional state of society is acknowledged, strengthening solidarity and resilience.

In the context of hybrid threats, strategies to counter disinformation are of particular importance. Preventive communication creates a stable informational background, reducing

the persuasiveness of manipulative content. Real-time fact-checking acts as a tool for social verification, helping restore balance and trust. Reactive rhetoric aimed at promptly debunking false messages enhances the adaptability of the communication system *(Arcos, Brandt, Fernández-García, & Gil-Ortega, 2022).*

Collaboration between state and non-state actors is a key condition for effectively countering hybrid threats. State institutions provide strategic coordination, regulatory frameworks, and long-term policy development, while civil society organizations and independent journalism ensure public oversight, media literacy, and factual analysis. Social networks, serving simultaneously as channels for spreading disinformation and platforms for debunking it, require tailored mechanisms of regulation and structured cooperation with civil society.

An important area of focus is the construction of resilient narratives rooted in national identity, democratic values, and principles of solidarity. Such narratives not only counter destructive informational influences but also promote positive scenarios of societal development. Their inclusiveness ensures that the interests of diverse social groups are considered, creating a sense of shared purpose and strengthening public trust.

Influence scenarios in crisis conditions can have both destructive and constructive effects. While disinformation campaigns can fuel panic, radicalization, and distrust, effective communication strategies can transform a crisis into an opportunity for consolidation and the development of critical thinking. Achieving this requires systematic forecasting based on sociological monitoring, digital audience analysis, and continuous media space tracking.

Opinion leaders and influencers play a significant role in this process, as they can reach narrow and localized audiences, forming horizontal trust networks. Their involvement in communication campaigns amplifies the resonance of official messages and enhances the effectiveness of countering manipulation *(Hlynskyi & Donets, 2025).*

Ultimately, political communication in the context of hybrid threats is not merely a response tool to disinformation but a strategic resource for ensuring national security and societal resilience. The integration of preventive and reactive strategies, coordination between state and non-state actors, and the development of coherent narrative systems enable democratic societies to maintain stability amid informational turbulence.

7. Conclusions

Political communication in the context of hybrid threats and the full-scale war against Ukraine has acquired strategic importance, becoming one of the key tools for ensuring national security. Its effectiveness depends on the state's ability to coordinate information flows, build resilient narratives, and respond swiftly to disinformation attacks. The integration of preventive and reactive communication strategies enables the maintenance of societal cohesion, the strengthening of governmental legitimacy, and the formation of a favorable international image of the state.

Ukraine's experience demonstrates that a combination of technological solutions, cross-sectoral cooperation, and transparency in communication is the foundation of societal resilience to informational challenges. Building partnerships among state institutions, civil society, the media, and opinion leaders creates a synergy of efforts, reducing the vulnerability of the information environment to manipulation.

Further academic research should focus on developing unified models for evaluating the effectiveness of strategic communications, analyzing the impact of algorithmic technologies on the formation of societal narratives, and studying the interaction between public and private

actors in countering disinformation. These efforts will help refine evidence-based approaches to building communication strategies capable of enhancing the resilience of democratic institutions and strengthening national security.

References

1. Hoffman, F. (2007). Conflict in the 21st century: The rise of hybrid wars. Arlington: Potomac Institute for Policy Studies. Retrieved from https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
2. Mansoor, P. R. (2012). Introduction. In W. Murray & P. R. Mansoor (Eds.), Hybrid warfare (pp. 1–17). Cambridge. https://doi.org/10.1017/cbo9781139199254.001
3. Hybrid CoE. (2023.). Hybrid threats as a concept – Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. Retrieved from https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
4. Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Fathaigh, R. Ó., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. H. (2018). Online political microtargeting: Promises and threats for democracy. Utrecht Law Review, 14(1), 82. https://doi.org/10.18352/ulr.420
5. Koch, H. (2024). Strategic communications in the global security environment: StratCom's shift of the balance of power. MacEwan University Student eJournal, 8(1).
6. Barovska, A. (Ed.). (2016). Informatsiini vyklyky hibrydnoi viiny: kontent, kanaly, mekhanizmy protydii [Information challenges of hybrid war: Content, channels, counteraction mechanisms]. Kyiv: NISD. Retrieved from https://niss.gov.ua/sites/default/files/2016-06/inform_vukluku.pdf [in Ukrainian]
7. Bastos, M., & Mercea, D. (2017). The Brexit botnet and user-generated hyperpartisan news. Social Science Computer Review, 37(1). https://doi.org/10.1177/08944393177341
8. Bukanov, H. (2025). Politychna komunikatsiia vlady i suspilstva v umovakh voiennoho stanu v Ukraini [Political communication between the government and society under martial law in Ukraine]. Visnyk NTUU "KPI" Politolohiia. Sotsiolohiia. Pravo, 2(66), 72–78. https://doi.org/10.20535/2308-5053.2025.2(66).337624 [in Ukrainian]
9. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559
10. Tarielkin, Yu., & Tsykyn, V. (2010). Metodolohiia naukovykh doslidzhen [Methodology of scientific research]. Sumy: SumDPU im. A. S. Makarenka. Retrieved from https://library.sspu.edu.ua/wp-content/uploads/2018/04/42-1.pdf [in Ukrainian]
11. Khudolii, A. (2014). Politychnyi dyskurs yak obiekt linhvistychnoho analizu [Political discourse as an object of linguistic analysis]. Naukovi zapysky Natsionalnoho universytetu "Ostrozka akademiia", 42, 174–177. [in Ukrainian]
12. Bataieva, K., et al. (2018). Suchasni metodyky kontent-analizu [Modern methods of content analysis]. Kyiv: Kondor. [in Ukrainian]
13. Elstub, S., & Pomatto, G. (2022). Case study research. In Research methods in deliberative democracy (pp. 406–420). https://doi.org/10.1093/oso/9780192848925.003.0028
14. Zaiets, O. (2024). Analiz sotsialnykh merezh [Social network analysis]. In Metody, instrumenty ta trendovi novatsii kryminalnoho analizu v Ukraini (pp. 359–366). Retrieved from https://www.researchgate.net/publication/381385861_Analiz_socialnih_merez [in Ukrainian]
15. Ostapenko, M. (2012). Politychna komunikatsiia: teoretychni aspekty doslidzhennia [Political communication: Theoretical aspects of research]. Politychnyi menedzhment, 3, 135–144.

Retrieved from https://ipiend.gov.ua/wp-content/uploads/2018/08/ostapenko_politychna.pdf [in Ukrainian]

16. Arcos, R., Brandt, M., Fernández-García, N., & Gil-Ortega, M. (2022). Responses to digital disinformation as part of hybrid threats: A systematic review on the effects of disinformation and the effectiveness of fact-checking/debunking. Open Research Europe, 2, 8. https://doi.org/10.12688/openreseurope.14088.1

17. Hlynskyi, N., & Donets, V. (2025). Vplyv lideriv dumok na hromadsku dumku i povedinku molodi: komunikatsiinyi aspekt [The influence of opinion leaders on public opinion and youth behavior: A communication aspect]. Menedzhment ta pidpryiemnytstvo v Ukraini: etapy stanovlennia ta problemy rozvytku, 1(25), 142–151. Retrieved from https://science.lpnu.ua/sites/default/files/journal-paper/2025/may/38876/250524maket-144-153.pdf [in Ukrainian]