INTERNATIONAL RELATIONS

Elena MÂRZAC
Moldova State University, Republic of Moldova

STRATEGIC COMMUNICATION AS A TOOL FOR COUNTERING HYBRID THREATS. A FOCUS ON NATIONAL RESILIENCE AND PUBLIC TRUST

Abstract:	*This paper examines strategic communication's important role in countering hybrid threats through early detection, real-time response, and collaboration among government, civil society, and technology sectors. Hybrid threats, such as foreign information interference, disinformation, cyberattacks, and political influence campaigns, present challenges to national security, particularly in the digital age. By fostering societal resilience and enhancing public trust in institutions, strategic communication frameworks are essential to safeguarding national interests. This paper explores how strategic communication frameworks can detect, respond to, and mitigate the impacts of hybrid threats, rapid and coordinated responses.* *Strategic communication can prevent the spread of disinformation, help build national resilience. By creating collaborative networks and using digital technologies, strategic communication protects national security and underscores their role in safeguarding national resilience. It aligns messaging across agencies, reinforcing government credibility during crises and fostering societal resilience through transparent, accurate information. By engaging with diverse audiences, StratCom adapts messages to influence positive public behaviors and build social cohesion. Additionally, it supports national interests by unifying government and societal efforts under clear objectives, while protecting information channels to secure communication. This proactive, coordinated approach strengthens democratic values and national security against hybrid threats.*
Keywords:	**Strategic communication; disinformation; hybrid threats; national interests; national resilience; societal resilience; social cohesion.**
Contact details of the authors:	E-mail: elena.marzac@gmail.com
Institutional affiliation of the authors:	**Moldova State University, Republic of Moldova**
Institutions address:	Alexei Mateeveci 60 street, Chișinau, MD-2009, tel: +37322244810, www.usm.md, rector@usm.md

Context of hybrid threats

Hybrid threats are complex, combining conventional and non-conventional tactics to destabilize social and political environments, often undermining public trust in government institutions and social cohesion[1]. Hybrid threats are not new, but their impact has become massive and dangerous in a globalized world with rapid communication development. The fundamental characteristic of hybrid aggression is that it is intended to exploit weaknesses and vulnerabilities within the political, economic and social systems, as well as in the critical infrastructures and information environments of the target state. Therefore, it is important for each state to be aware of its own vulnerabilities and to have the capacity to identify any changes in the public and

[1] Nicolas Jankowski, *Researching Fake News: A Selective Examination of Empirical Studies*, https://doi.org/10.1080/13183222.2018.1418964 (21.10.2024)

information security environment that could constitute elements of a foreign information interference campaign[1].

Hybrid threats are an umbrella term describing adversarial activities that blend military and non-military tactics, particularly in the digital and information domains. These activities exploit vulnerabilities within a state's cyber, political, and social infrastructures, often aiming to create confusion and erode public confidence in the government[2].

Hybrid tactics may include disinformation, cyber espionage, and political influence, complicating conventional defense mechanisms. In this regard, according to the Countering Hybrid Warfare in the Black Sea Region an effective institutional framework to counter hybrid threats needs to address four interconnected areas of action: (1) countering disinformation; (2) cybersecurity; (3) the resilience of critical infrastructure and supply chains; and (4) crisis and emergency management and defence[3].

The first two areas – countering disinformation and cybersecurity – have an impact on all aspects of social life. Securing the digital and information space requires inter-agency coordination and strengthening strategic communications capabilities. Additionally, sensitizing the public to the tools and effects of Russian disinformation is crucial for detecting and addressing the threat of hybrid warfare.

Achieving national resilience, including informational resilience to address hybrid threats, requires identifying key vulnerabilities and conducting a common risk assessment. This process demands a shared understanding of security threats and the synchronization of efforts among various state institutions. The war in Ukraine has clearly shown the importance of societal resilience, the existence of mechanisms for collaboration between the state and society, strategic communication, and efforts to prevent and combat propaganda and disinformation[4]. Effective defensive measures open immense opportunities for societies. Such threats are generally associated with foreign actors seeking to disrupt national stability through digital manipulation, cyberattacks, and disinformation campaigns[5]. Russia's influence in Eastern Europe, particularly in Moldova and Georgia, and disinformation efforts exemplify these tactics, where information manipulation has a profound impact on political stability[6].

These hybrid tactics are closely linked to information warfare, a phenomenon that Chifu and Simons argue that information warfare is made up of two parts that interact and influence one another—offensive and defensive components. For example, the offensive component is related to the goal of exploiting corrupting, denying, and destroying an adversary's information space. The goal is to advance the objectives and interests of the user. The defensive component concerns guarding, reinforcing, dominating, and enabling one's own information space, where the goal is to defend the objectives and interests of the user. Together, hybrid threats and information warfare represent a coordinated approach to achieving political influence, destabilizing adversaries in a volatile international and regional security environment.

In the current context of an increasingly interconnected world and vulnerable to information threats, Foreign Information Manipulation and Interference (FIMI) amplifies these risks, posing a growing threat to international security and stability. The concept of FIMI was developed by the European Union's (EU) European External Action Service (EEAS) in response to emerging threats, particularly those posed by Russian

[1] Viorica Ionela Trincu, *Contracararea amenințărilor hibride la nivelul Uniunii Europene,* "Gândirea Militară Românească", No. 2, 2019, p. 47

[2] *Understanding Hybrid Threats,* Helsinki, 2020, https://www.hybridcoe.fi/ (30.10.2024)

[3] *The Countering Hybrid Warfare in the Black Sea Region*, https://csd.eu/fileadmin/user_upload/publications_library/files/2024_2/Countering_Hybrid_Warfare_Black_Sea_Region_ENG_fin.pdf p.12 (29.10.2024)

[4] *Reziliența în fața amenințărilor de tip hibrid. Un "sport de echipă" în care nimeni nu trebuie lăsat în urmă,* https://e-arc.ro/2022/06/07/rezilienta-in-fata-amenintarilor-de-tip-hibrid-un-sport-de-echipa-in-care-nimeni-nu-trebuie-lasat-in-urma/ (29.10.2024)

[5] Iulian Chifu, Greg Simons, *Rethinking Warfare in the 21st Century. The Influence and Effects of the Politics, Information and Communication Mix*, https://www.cambridge.org/core/books/rethinking-warfare-in-the-21st-century/05181F92A0DFD584C1C609430F01B324 (29.10.2024)

[6] Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou, *The landscape of Hybrid Threats: A conceptual model*, https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/ (29.10.2024)

disinformation campaigns[1]. FIMI refers to the intentional and coordinated efforts by state or non-state actors to manipulate information environments to achieve political, security, or other strategic objectives[2]. This concept covers not only disinformation, but also various forms of information manipulation and interference, which can undermine public trust in democratic institutions and affect political and social processes. The actors in such activity may be state or non-state actors, including their agents, either inside or outside their own territory[3].

For example, the EU's "Joint Framework on Countering Hybrid Threats" includes a very broad area of activities to counter hybrid threats, demonstrating the broadness of the field. The framework outlines several key areas: strategic communication to counter the systematic spread of disinformation; protection of critical infrastructures, such as energy supply chains and transportation, from unconventional attacks. This includes broad policy goals like diversifying the EU's energy sources, suppliers, and routes, ensuring transport and supply chain security, protecting space infrastructure from hybrid threats, and generally enhancing defense capabilities. Additionally, it emphasizes protecting public health and food security, including safeguards against chemical, biological, radiological, and nuclear (CBRN) threats. The framework also focuses on enhancing cybersecurity, with particular attention to industry, energy, financial, and transport systems. Furthermore, it addresses targeting the financing of hybrid threats and building resilience against radicalization and violent extremism[4].

In this article, we will refer to the role of strategic communication in countering hybrid threats and will demonstrate its important role. StratCom not only informs and raises awareness among the public, but also contributes to building social resilience by encouraging the adoption of positive and sustainable behaviors. The integration of strategic communication into information operations and intelligent data analysis are ways to develop coordinated and effective responses to information manipulations. In the specialized literature, we find several definitions of the concept. Christopher Paul defines strategic communication as a sum of "coordinated actions, messages, images, and other forms of signaling or engagement to inform, influence, or persuade selected audiences in support of national objectives"[5]. According to the author of the book "Corporate Communication," P.A. Argenti, who describes the concept of organizational communication (in our perspective, equivalent to strategic communication at the organizational level), defines the notion as "the solution through which employees can become more productive, and the created interaction provides management with greater credibility among employees"[6].

Strategic Communication is an indispensable informational element for national authorities. It emphasizes the state's efforts to understand and engage the target audience to create, strengthen, or maintain favorable conditions for advancing national interests, policies, and objectives. This involves coordinated communication—through programs, plans, themes, messages, and products—synchronized with the actions of all instruments of national power, both official and unofficial[7].

Various international organizations have also developed their own definitions of strategic communication. At the NATO level, strategic communication is understood as the coordinated and timely use of communication activities and capabilities-public diplomacy, public relations, information operations, and

[1] *Tackling Online Disinformation: An European approach*, https://ec.europa.eu/information_society/newsroom/image/document/2018-28/presentationcomm_paolo_cesarini_202D869F-9A13-6D79-FC46C00EAAE3E9AC_53429.pdf (28.10.2024)

[2] *Foreign Information Manipulation and Interference (FIMI),* https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html (18.11.2024)

[3] Bernard Siman, *Countering FIMI: A Critical Imperative for Mission Safety*, https://www.egmontinstitute.be/countering-fimi-a-critical-imperative-for-mission-safety/ (22.10.2024)

[4] European Union, *Joint Framework on countering hybrid threats, a European Union response', Joint Communication to the European Parliament and the Council,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (22.10.2024)

[5] Christopher Paul, *Getting Better at Strategic Communication*, Rand Corporation, Pittsburgh, 2011

[6] Paul Argenti, *Corporate Communication*, Irwin McGraw-Hill, Boston, 1998, p. 17

[7] Kenneth E. Kim, *Framing as a Strategic Persuasive Message Tactic*, "The Routledge Handbook of Strategic Communication", p. 285, https://www.routledge.com/The-Routledge-Handbook-of-Strategic-Communication/Holtzhausen-Zerfass/p/book/9780367367732?srsltid=AfmBOoqL8zgYUO5NOK1a7-8-uH_JtsTvFBGTjeO-v2F-G1M3eaqSE4AP (22.10.2024)

psychological operations, as necessary, to support NATO policies, operations, and activities and to achieve Alliance objectives[1].

Defined broadly, strategic communication is a framework used to align governmental and societal messaging in a manner that counters adversarial narratives and enhances resilience. It involves targeted messaging, stakeholder engagement, and the use of digital platforms to bolster national security against hybrid threats. Through strategic communication, governments can build a narrative that counters misinformation effectively[2]. Strategic communication has emerged as an essential tool for counteracting hybrid threats, involving the use of coordinated messaging to protect national interests and maintain social cohesion. StratCom supports both proactive and reactive approaches, equipping governments and institutions with the capacity to inform, educate, and engage the public effectively[3].

Strategic communication: diverse approaches

The process is designed to counter the disruptive effects of disinformation and malicious information, targeting not only the external public, to promote national interests, but also the internal public, to increase its resilience to information attacks. Process integrated into a large-scale initiative, encompasses multidisciplinary and social marketing, non-formal education, public participation, aimed at innovative and sustainable change of practices, behaviors and lifestyles, guides communication processes and media interventions among social groups and is a prerequisite and a tool for change at the same time.

StratCom is a process that interconnects democratic values, public institutions, supra-state institutions, the media, and various national and international categories of public. This requires an understanding of relevant actors, their strategic objectives, the measures they employ and which of our own vulnerabilities might be exploited. All of these are wrapped up in the narratives adopted by any hostile actor, designed to target different audiences[4]. StratCom can be an option for changing people's way of thinking, which in addition to voluntary involvement and unconditional assumption of responsibility, first, also includes continuous adaptability and flexibility to keep up with the expansion and diversification of the hybrid phenomenon. Ideally, it should be established at the highest leadership level within a state, organization, or institution and should be communicated and implemented effectively down to the lowest tactical level. Its role is to educate and inform the public, but, more than that, the most effective kind of strategic communication changes behaviors[5]. To effectively counter hybrid threats, strategic communication plays a critical role by serving multiple functions that work together to enhance national resilience. These functions include:

1. Early Detection and Monitoring

One of the most effective uses of strategic communication is early detection. By employing monitoring tools across social media and other digital platforms, governments can detect hybrid threats before they escalate. Real-time monitoring, coupled with data analytics, provides a foundation for rapid response strategies[6], integrating these approaches allows governmental and non-governmental agencies to counteract disinformation campaigns and manage crises proactively. The European Union has implemented several measures for the early detection and monitoring of disinformation. For example, the EU Code of Practice on Disinformation (established in 2018 and strengthened in 2022), involves commitments from online platforms, trade associations, and the advertising sector to curb disinformation. It includes measures to improve transparency, empower users, and enhance cooperation with fact-checkers.[7]. Other successful could be

[1] NATO, *ACO Strategic communications* AD 95-2/21 May 2012, https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf (22.10.2024)

[2] Andrew, Chadwick*, The Hybrid Media System. Politics and Power*, Oxford University Press, Oxford 2017, p. 43

[4] *Strategic communications hybrid threats toolkit. Comunications to understand and counter grey zone threats*, https://stratcomcoe.org/cuploads/pfiles/Strategic-Communications-Hybrid-Threats-Toolkit_Rev_12l.pdf (22.10.2024)

[5] Elena Mârzac, Sanda Sandu, *Comunicarea strategică – instrument de fortificare a rezilienței informaționale*, "Reziliența în atenția securității. Concepte, procese, necesități", USM, Chișinău, 2022, p. 66

[6] Dakota Cary, Daniel Cebul, *Destructive Cyber Operations and Machine Learning*, https://cset.georgetown.edu/publication/destructive-cyber-operations-and-machine-learning/ (22.10.2024)

[7] *A strengthened EU Code of Practice on Disinformation*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_en (22.10.2024)

considered the Action Plan Against Disinformation, launched in 2018, this plan focuses on improving detection, analysis, and exposure of disinformation. It also emphasizes stronger cooperation between Member States and EU institutions, as well as mobilizing the private sector to tackle disinformation[1].

2. Coordination and Rapid Response

Strategic communication, as a process, can contribute to a more effective orchestration of government activities, integrating various activities within the instruments of power, in order to strategically influence and form national resilience. Integration of efforts between all instruments of power: diplomatic, informational, military and economic, based on the national security strategy and risk and threat assessment.

Strategic communication aims to influence, and strategic influence depends entirely on effective coordination between the government and, beyond it, to achieve national strategic objectives. Given the central influence on the national strategy, a strategic communication framework must be present in strategic planning and in the preparation and implementation of policies[2].

Strategic communication enables a coordinated response to hybrid threats by creating a unified message across multiple agencies and sectors. It requires a high level of coordination across different strategic, operational, and tactical levels. This ensures that all communication efforts are aligned and reinforce each other[3]. For instance, the EU's "East StratCom Task Force" was established to monitor and counteract Russian disinformation campaigns, ensuring that coordinated, accurate messaging reaches European citizens.

3. Building Public Trust and Social Cohesion

Strategic communication serves to build resilience by fostering public trust through transparency and accountability. When governments deliver credible and timely information, they are better positioned to gain public support. Studies demonstrate that consistent, truthful communication helps mitigate the influence of adversarial misinformation[4]. Moreover, societal resilience is strengthened when citizens are informed and can differentiate between authentic information, disinformation, and manipulation. Effective, citizen-centred public communication can help build trust in democratic institutions by ensuring and demonstrating that the government is reliable, responsive, open and fair. It is an essential asset to prevent and counteract mis- and disinformation, along with other governance responses[5]. Strategic communication is a two-way process, which conveys the reactions and points of view of the different audiences involved in the communication process. Public feedback should be used for regular policy and strategy adjustments. More ambitiously, strategic communication is not limited only to media messages; it must contribute to the development of a communication campaign oriented towards behavioral or social changes of the public. That is why effective strategic communication presumes identification, understanding and engagement with target audiences. This process involves deep knowledge of their needs, values, fears, beliefs, and behaviors that would allow bettering to reach the audience, to adjust the messages and to identify better channels of communication.

It is necessary to identify and coordinate all governmental instruments (political leaders, decision-makers, strategic actors, communicators, implementing actors, official diplomacy, public affairs, media operations, public-private partnership, military diplomacy, internal communication, interdepartmental public relations), as well as societal instruments (media, NGOs, private communication entities, academia, cultural institutions, business, public figures, influential authors, scientists, the diaspora, etc.).

Strategic communication is an indispensable tool in the process of good governance and development of the Republic of Moldova, both for streamlining the governing act and for ensuring common communication and understanding between all stakeholders. Good governance assumes that states institutions must be transparent in decision-making and accountable for their actions, correctly and impartially implement laws to

[1] *Action plan against disinformation. Report on progress*, https://ec.europa.eu/commission/presscorner/api/files/attachment/857709/factsheet_disinfo%20elex_140619%20final.pdf (22.10.2024)

[2] Elena Mârzac, Sanda Sandu, *Op. cit.*, p. 66

[3] European Parliament, *Strategic communications as a key factor in countering hybrid threats*, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656323 (30.09.2024)

[4] Lance Bennett, Steven Livingston, *The disinformation order: Disruptive communication and the decline of democratic institutions*, "European Journal of Communication", Vol. 33, No. 2, 2018, p. 129

[5] *Good practice principles for public communication responses to mis- and disinformation*, https://www.oecd-ilibrary.org/governance/good-practice-principles-for-public-communication-responses-to-mis-and-disinformation_6d141b44-en (20.11.2024)

maintain order and protect citizens' rights, reform the judiciary to ensure the independence of the judiciary and fight corruption, etc. An indicator of good governance is the active involvement of citizens in political and social processes, both through public consultations, citizens' initiatives and by supporting a strong civil society.

Without communication structures and processes that allow the exchange of information between the state and citizens, it is difficult to imagine that states can be responsive to the needs, expectations, and needs of the public. Trust has played an important role in effectively managing the COVID-19 pandemic, as countries with higher levels of social and government trust have typically seen slower virus spread and a lower mortality rate[1]. As trust rises, so does confidence in government information generally, enabling a unified response and increased citizen cooperation.

Since the start of the pandemic, Singapore has focused on clear and consistent information sharing. The government had an effective communication plan: The members of the COVID task force held daily press conferences, during which they explained the evolving COVID-19 situation and resulting government decisions[2]. Data trusts and data-sharing infrastructure, such as Estonia's X-tee platform, build public trust by facilitating the secure and authenticated exchange of data. Estonian public sector organizations are required to use the heavily regulated X-tee tool to access or share data. This platform improves cohesion across government agencies and bolsters citizen confidence[3]

4. Promoting national interests and supporting the implementation of national policies and objectives.

Given the current risks and threats, as well as national interests, strategic communication is an essential piece of information for national authorities and is one of the tools that the state uses to achieve its objectives. The promotion of national interests depends on the continued efforts of state and non-state actors to coordinate messages and actions and how all stakeholders will perceive them in the national security and defence sector.

In the absence of effective strategic communication, national interests are compromised, political changes lead to deviations, and the population becomes vulnerable to disinformation and manipulation. Additionally, the lack of a clear international vision generates domestic skepticism, facilitating propaganda and confusion among foreign partners. The lack of StratCom can generate incoherence and chaos in actions and messages, with serious consequences, as strategic communication supports the implementation of national strategies and counteracts conflicts, including hybrid wars, being vital for achieving the political, economic, social, security and defense objectives of the state. Effective communication reflects and supports good governance. Effective coordination and the delivery of the right messages, in line with the strategic objectives of the state and its institutions, will help align the efforts of the various national entities and strengthen cohesion in different sectors, with a view to countering disinformation.

The integration of a common mentality of strategic communication at all levels of state institutions and implementation of the national strategy will determine a high strategic culture, which will facilitate the necessary changes in the current practice. Thus, strategic communication can become a powerful tool of power, used to shape attitudes and behaviors, to listen to and understand the public, and to coordinate messages between the government and its partners, ensuring an effective integration of information with other instruments of national power[4]. In this regard, StratCom can accelerate, influence and improve citizens' perceptions of certain vital areas for the country's development, understanding the actions of decision-makers, raising awareness and supporting certain reforms.

For the Republic of Moldova, strategic communication and combating information manipulation through FIMI are critical due to its position between the European Union and the Russian Federation. Moldova is particularly vulnerable to disinformation campaigns aimed at destabilizing society and undermining trust in

[1] Thomas Bollyky, *Fighting a pandemic requires trust: Governments have to earn it*, "Foreign Affairs", October 23, 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-23/coronavirus-fighting-requires-trust, (20.11.2024)

[2] Jeremy Lim, *How Singapore is taking on COVID-19,* "Asian Scientist Magazine", April 3, 2020, https://www.asianscientist.com/2020/04/features/singapore-covid-19-response/ (20.11.2024)

[3] Bruce Chew, Michael Flynn, Georgina Black, Rajiv Gupta, *Sustaining public trust in government*, https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2021/public-trust-in-government.html, (20.11.2024)

[4]Elena Marzac, Viorica Zaharia, *Comunicarea strategică și combaterea dezinformării. Ghid de combatere a dezinformării prin comunicare strategică*, Bons Office, Chișinău, 2024, p. 12

democratic institutions[1]. FIMI seeks to provoke political and ethnic tensions, leading to polarization and hindering the implementation of democratic, economic, and security reforms. Additionally, in the context of national security, disinformation fosters confusion and uncertainty, eroding public confidence in the state's capacity to address pressing challenges.

According to the National Security Strategy, the Republic of Moldova faces several threats to national security, including the hybrid operations carried out by the Russian Federation against the Republic of Moldova in the political, economic, energy, social, informational, cyber fields, etc., with the aim of undermining the constitutional order, derailing the country's European course and/or disintegrating the state[2]. In addition, Moldova, in the desire to integrate with the European Union and to maintain stable relations with its neighbors, is subject to information manipulation, which can influence public opinion and hinder pro-European policies. Thus, strengthening strategic communication is an important action in protecting democratic values, maintaining social cohesion and increasing resilience to external threats.

5. Strategic communication is vital in countering disinformation campaigns as it is a process designed, among other things, to counter the disruptive effects of disinformation. It targets not only external audiences with the aim of promoting national interests but also internal audiences to enhance resilience against national attacks.

The process of strategic communication can be the opportunity needed to stop the evolution of certain currents, to increase the public's resilience to disinformation campaigns and to promote certain basic narratives/messages regarding the national interests of the state among the population. For example, the European Commission is strengthening its strategic communication to combat disinformation, manipulation of information from outside and foreign interference targeting EU policies. This requires a whole-of-society approach, as many sectors play an important role in preventing and combating disinformation. It is also important to ensure that citizens have access to quality and trustworthy news and information[3]. In this regard, the Commission, among others, is directing its efforts in the fight against disinformation by developing policies aimed at strengthening European democracies, making it harder for disinformation actors to misuse online platforms, protecting journalists and media pluralism, countering foreign interference and cyberattacks through awareness-raising projects, advanced technological solutions, and better coordination, and strengthening society's resilience against disinformation through media literacy and awareness-raising initiatives[4].

For instance, the EU’s StratCom East Task Force has been effective in countering Russian disinformation campaigns targeting Eastern European countries, including Moldova. This initiative involved monitoring and exposing disinformation narratives, as well as providing alternative, fact-based information to local populations[5].

Another example is the NATO Strategic Communications Centre of Excellence, which has supported member states in developing their own StratCom capabilities. Their efforts in Ukraine during the 2014 crisis and Russian war in Ukraine started in February 2022 are a prime example of how coordinated communication can counteract propaganda and support democratic resilience in the face of external threats. Similarly, in the Republic of Moldova, efforts have been made to institutionalize strategic communication and respond to the challenges associated with fake news, propaganda, and disinformation campaigns. To this end, in the Republic

[1] *Blurring the Truth: Disinformation in Southeast Europe*, https://www.kas.de/documents/281902/281951/E-book+Blurring+the+Truth.pdf/fd6abbb3-f49e-115b-090e-7c9f3a20dfc6?version=1.2&t=1680504776349%20Blurring%20the%20Truth:%20Disinformation%20in%20Southeast%20Europe (30.09.2024)

[2] Parlamentul Republicii Moldova, *Strategia Națională de Securitate a Republicii Moldova*, https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023.pdf (30.09.2024)

[3] *Comunicare strategică și combaterea dezinformării*, https://commission.europa.eu/topics/strategic-communication-and-tackling-disinformation_ro (26.10.2024)

[4] Parlamentul Republicii Moldova, *Strategic communications as a key factor in countering hybrid threats*, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656323 (30.09.2024)

[5] Kristina Berzina, Kovalcikova Nada, David Salvo, Soula Etienne, *European policy blueprint for countering authoritarian interference in democracies,* https://www.jstor.org/stable/pdf/resrep21251.8.pdf?refreqid=excelsior%3A2a2bf2246650062af2b9851a5db9023 (30.09.2024)

of Moldova, the Center for Strategic Communication and Combating Disinformation was created in July 2023. The Center's mission is to increase efforts in combating specific actions that pose a threat to national interests.

According to the Concept of Strategic Communication and Countering Disinformation for 2024-2028[1], the need for an institutionalized and integrated approach to strategic communication and countering disinformation in the context of external and internal threats faced by the Republic of Moldova, especially from the Russian Federation, was argued. The vision consists of "supporting, consolidating and contributing to the achievement of national interests, which are the foundations of the idea of the Republic of Moldova as a state of the century. The concept has the following general objectives: to develop the institutional capacities of the state and society to communicate effectively and combat disinformation. The main thematic areas addressed are: European integration, social cohesion, economic resilience, strengthening the defense sector and strengthening national security in the regional context.

This integrated and action-oriented approach aims to strengthen the democracy, security and socio-economic development of the Republic of Moldova in the coming years. An important argument for supporting the importance of strategic communication as a tool to counter hybrid threats that negatively impact national security, is the fact that the national security strategy of the Republic of Moldova[2].

Beyond informing, strategic communications aim to influence and promote specific behaviors. This can be crucial in situations where public cooperation is needed to counter hybrid threats[3]. The strategic mindset in communication also implies an integrated vision, which combines persuasive strategies with participatory practices. It is not limited to one-way communication, but promotes dialogue and engagement, recognizing the importance of building new realities through the active involvement of the public. In a world where many external factors compete for influence in a complex information environment, strategic communication must be flexible and adaptable, able to respond to challenges proactively and creatively.

Strategic communication communicates "narratives". Narratives, according to Lawrence Freedman, are conceived or cultivated with the intention of structuring audiences' responses to certain events, therefore, narratives refer to influence. Narratives are stories that make sense to the audience because they relate to shared values and experiences, however, in the long run they can be used to shape an audience's perceptions and interests. Realized at the strategic level, narratives are a means for political actors to build a common sense of the past, present and future of international politics to shape domestic behavior and international actors. Strategic narratives can be used to communicate the "soft power" that a country wants to design. Indeed, according to Roselle, strategic narrative is soft power in the 21st century.

Key approaches to strategic communication in hybrid threat scenarios

To deter hybrid threats, it is necessary to take several proactive and reactive measures that are interdependent. To achieve them, specific capabilities are needed to cover all the essential functions necessary to counter hybridity in a timely manner, as early as possible, such as: monitoring, detecting, identifying, disclosing and rejecting any hybrid actions and activities. These capabilities give weight to the approach and increase the determination to react and fight back when the relaunched competition and the influence sought by hybridity exceed any limit of bear ability in the target state. Without these capabilities to ensure early detection and timely intervention to counter hybrid threats, regardless of the volume of communication involved, there would most likely not be enough credibility framework.

On the other hand, beyond the presentation and promotion of these specific capabilities and their overall effectiveness, there is another facet of credibility, namely political determination, the willingness to

[1] Parlamentul Republicii Moldova, *Hotărâre privind aprobarea Concepţiei de comunicare strategică și contracarare a dezinformării, a acţiunilor de manipulare a informaţiei și a ingerinţelor străine pentru anii 2024–2028*, https://www.parlament.md/LegislationDocument.aspx?Id=25cfe6b6-795d-47eb-82a3-065d51d26fdf (30.09.2024)

[2] Parlamentul Republicii Moldova, *Lege privind Centrul pentru Comunicare Strategică și Combatere a Dezinformării și modificarea unor acte normative,*
https://presedinte.md/app/webroot/uploaded/Proiect%20Lege%20Centrul%20CSC%20Dezinformare%2005.07.23.pdf (26.10.2024)

[3] *Hybrid Threats: A Strategic Communications Perspective - StratCom COE*, https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79 (26.10.2024)

.

point the finger at the hybrid aggressor and publicly disclose hybrid actions. StratCom is involved in this process by delivering appropriate messages that serve its own purposes. The process must be organized in a synchronized, coherent manner, so that the target audience can anticipate, be prepared, involved and proactively against hybrid actions. Proactive measures, including awareness campaigns and digital literacy programs, play an essential role in preparing the public to identify and resist disinformation. These efforts are akin to "inoculating" the population against false narratives by preemptively educating citizens on recognizing misinformation tactics. Public awareness campaigns on social media can demystify misinformation and guide citizens toward credible sources, strengthening resilience against hybrid threats[1].

In scenarios where hybrid threats are already present, governments must employ targeted reactive measures. Strategic communication can include rebuttal campaigns, rapid fact checking, and coordinated messaging to counteract narratives already circulating within the information ecosystem. By establishing a rapid response system, governments can swiftly correct misinformation, reducing its impact on the public[2].

Digital platforms play a crucial role in the dissemination of strategic communication. Through data-driven insights and targeted outreach, governments can respond to threats more effectively. Artificial intelligence (AI) enhances the detection of threats and assists the strategic communication specialists to adjust the strategies, tailor the messages and to understand the emotions and in result to shape the perceptions. AI and machine learning algorithms can process vast amounts of data to identify patterns and predict future trends. This enhances the strategic planning and execution of communication campaigns[3]. IAI-driven tools can automate the detection and countering of disinformation, making information operations more efficient and scalable[4].

Artificial intelligence plays a double role here, as it can be used by both the promoters of hybrid threats to develop attacks that are more sophisticated and by defenders to counter them. AI can be used to create and spread false content (text, images, audios, videos) without human intervention, which could accelerate and reduce the costs of disinformation campaigns. It is also a key technology used in detecting and preventing disinformation and other components of hybrid *threats*. The European Union's experience with strategic communication highlights the necessity of a coordinated response to hybrid threats. The EU's East StratCom Task Force, established in 2015, has been instrumental in monitoring and countering FIMI specifically targeting Russian influence operations in Eastern Europe[5]. This initiative underscores the effectiveness of regional collaboration in combatting hybrid threats through strategic communication.

While StratCom is crucial for ensuring clarity in activities, engaging diverse target audiences and stakeholders, managing crises, and enhancing overall efficiency, it also presents challenges and limitations. One major challenge is information overload, where an audience inundated with excessive information may experience fatigue and disengagement. A relevant example is the overwhelming flow of information about the war in Ukraine in Central and Eastern Europe[6]. Therefore, it's crucial to balance the volume of communication and ensure that messages are concise and impactful for the specific target audiences. Prioritizing information is also essential to ensure that the most critical messages are delivered effectively.

Another significant challenge is coordinating communication efforts across multiple stakeholders, including departments, teams, and external partners. This complexity demands clear protocols and effective management to ensure alignment. Maintaining consistency in strategies and messages across large organizations further complicates the process. For instance, in organizations like NATO or EU, different members may convey messages that deviate from agreed-upon frameworks. Similarly, challenges arise in states where StratCom is not adequately institutionalized, leading to fragmented or conflicting communication.

[1] Andrew Chadwick, *Op. cit.*, p. 45

[2] Richey Mayson, *Disinformation and Strategic Communication in Hybrid Warfare*, "Journal of Strategic Studies", Vol. 12, No. 1, 2021, p. 78

[3] *AI in Support of StratCom Capabilities*, https://stratcomcoe.org/pdfjs/?file=/publications/download/Revised-AI-in-Support-of-StratCom-Capabilities-DIGITAL---Copy.pdf?zoom=page-fit (22.11.2014)

[4] US Department of Defence, *Strategy for operations in the information environment*, *2023*, https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF (22.11.2024)

[5] European Parliament, *Strategic communications as a key factor in countering hybrid threats*, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656323 (30.09.2024)

[6] Claudia Ciobanu, Jules Eisenchteter, Nicholas Watson, Edit Inotai, *War fatigue in central Europe is spreading*, https://balkaninsight.com/2024/07/01/war-fatigue-in-central-europe-is-spreading/ (22.11.2024)

Coordinating a coherent strategic message is further complicated by new media outlets such as blogs, chat rooms and text messaging, which are becoming preferred sources for information-regardless of validity-in some demographic groups and make "managing" information release impossible[1]. StratCom also requires significant resources. Developing and implementing a strategic communication plan can be time-consuming and costly, requiring investment in skilled personnel and technology. Continuous training is necessary to keep the communication team updated on best practices and emerging trends.

In our opinion one of the most important barriers is the Resistance to change. Employees and other stakeholders might resist new communication strategies, preferring familiar practices. This is particularly challenging in multinational organizations (e.g. NATO, EU, OSCE), where cultural differences can hinder the implementation of a unified communication strategy. Finally, measuring effectiveness poses its own challenges. Identifying the right metrics to assess the effectiveness of strategic communication can be complex. States and organizations need to establish clear goals and balance qualitative and quantitative data to make informed decisions.

Conclusions

Strategic communication is one of the indispensable instruments in countering hybrid threats. By enabling the timely and accurate transmission of information, StratCom frameworks build public trust, enhance resilience, and safeguard national security. The coordinated use of stakeholder engagement, coordination communication activities help governments to counteract FIMI, disinformation, mitigate cyber threats, and strengthen societal cohesion, thus, to obtain the support for governmental decisions and reforms.

Strategic communication is key for effectively countering hybrid threats and promoting a safer and more informed society, helping to protect national security and state integrity. StratCom in the fight against FIMI contributes to protecting democratic values and increasing social resilience. By integrating data analytics and information operations, StratCom develops coordinated and effective responses to disinformation campaigns, facilitating collaboration between governments, NGOs and local communities. These efforts make it possible not only to combat information threats, but also to change behaviors and promote social cohesion, which are essential for long-term democratic stability.

Strategic communication not only provides the necessary framework for the rapid and accurate transmission of messages, but also strengthens society's resilience by educating and informing the public.

In addition, by disseminating the right messages and using digital technologies, strategic communication can counter propaganda and disinformation and support efforts to ensure security. Moreover, while StratCom provides substantial benefits, overcoming challenges such as information fatigue, uncoordinated messaging, and limitations in human and technical resources requires meticulous planning, efficient management, and a commitment to continuous improvement.

Bibliography

Books

1. Argenti, Paul, *Corporate Communication*, Irwin McGraw-Hill, Boston, 1998
2. Chadwick, Andrew, *The Hybrid Media System. Politics and Power*, Oxford University Press, Oxford 2017
3. Chifu, Iulian; Simons, Greg, *Rethinking Warfare in the 21st Century*, Cambridge University Press, Cambridge, 2013
4. Marzac, Elena; Zaharia, Viorica, *Comunicarea strategică și combaterea dezinformării. Ghid de combatere a dezinformării prin comunicare strategică*, Bons Office, Chișinău, 2024
5. Paul, Christopher, *Getting Better at Strategic Communication*, Rand Corporation, Pittsburgh, 2011

[1] Michael, A. Brown, *Challenges of Strategic Communication*, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1171&context=ils (23.11.2024)

Studies and Articles

1. Bachmann, Sascha-Dominik; Gunneriusson, Hakan. *Hybrid Warfare: The Law and Policy of Leveraging Non-Military Elements,* "Journal of Strategic Security", Vol. 14, No. 2, 2017
2. Bachmann, Sascha-Dominik; Putter, Dries; Duczynsk, Guy, *Hybrid warfare and disinformation: A Ukraine war perspective*, https://doi.org/10.1111/1758-5899.13257
3. Bennett, Lance; Livingston, Steven, *The disinformation order: Disruptive communication and the decline of democratic institutions*, "European Journal of Communication", Vol. 33, No. 2, 2018
4. Bollyky, Thomas, *Fighting a pandemic requires trust: Governments have to earn it* , "Foreign Affairs", October 23, 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-23/coronavirus-fighting-requires-trust
5. Kim, Kenneth E., *Framing as a Strategic Persuasive Message Tactic*, "The Routledge Handbook of Strategic Communication", 2015, https://www.routledge.com/The-Routledge-Handbook-of-Strategic-Communication/Holtzhausen-Zerfass/p/book/9780367367732?srsltid=AfmBOoqL8zgYUO5NOK1a7-8-uH_JtsTvFBGTjeO-v2F-G1M3eaqSE4AP
6. Lim, Jeremy, *How Singapore is taking on COVID-19*, "Asian Scientist Magazine", April 3, 2020, https://www.asianscientist.com/2020/04/features/singapore-covid-19-response/
7. Mârzac, Elena; Sandu, Sanda, *Comunicarea strategică – instrument de fortificare a rezilienței informaționale,* "Reziliența în atenția securității. Concepte, procese, necesități", USM, Chișinău, 2022
8. *Reziliența în fața amenințărilor de tip hibrid. Un "sport de echipă" în care nimeni nu trebuie lăsat în urmă*, https://e-arc.ro/2022/06/07/rezilienta-in-fata-amenintarilor-de-tip-hibrid-un-sport-de-echipa-in-care-nimeni-nu-trebuie-lasat-in-urma/
9. Trincu, Viorica, Ionela, *Contracararea amenințărilor hibride la nivelul Uniunii Europene*, "Gândirea Militară Românească", No. 2, 2019

Documents

1. *Action plan against disinformation. Report on progress*, https://ec.europa.eu/commission/presscorner/api/files/attachment/857709/factsheet_disinfo%20elex_140619%20final.pdf
2. Bachmann, Sascha-Dominik, *Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats– mapping the new frontier of global risk and security management*, https://www.researchgate.net/publication/228214544_Hybrid_Threats_Cyber_Warfare_and_NATO%27s_Comprehensive_Approach_for_Countering_21st_Century_Threats_-_Mapping_the_New_Frontier_of_Global_Risk_and_Security_Management
3. *Blurring the Truth: Disinformation in Southeast Europe*, https://www.kas.de/documents/281902/281951/E-book+Blurring+the+Truth.pdf/fd6abbb3-f49e-115b-090e-7c9f3a20dfc6?version=1.2&t=1680504776349%20Blurring%20the%20Truth:%20Disinformation%20in%20Southeast%20Europe
4. Cary, Dakota; Cebul, Daniel, *Destructive Cyber Operations and Machine Learning***,** https://cset.georgetown.edu/publication/destructive-cyber-operations-and-machine-learning/
5. Chew, Bruce; Flynn, Michael; Black, Georgina; Gupta, Rajiv, *Sustaining public trust in government*, https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2021/public-trust-in-government.html
6. Ciobanu, Claudia; Eisenchteter, Jules; Watson, Nicholas; Inotai, Edit, *War fatigue in central Europe is spreading*, https://balkaninsight.com/2024/07/01/war-fatigue-in-central-europe-is-spreading/
7. *Comunicare strategică și combaterea dezinformării*, https://commission.europa.eu/topics/strategic-communication-and-tackling-disinformation_ro
8. Doncheva, Tihomira; Svetoka, Sanda, *Russia's Footprint in the Western Balkan Information Environment: Susceptibility to Russian Influence*, https://stratcomcoe.org/publications/russias-footprint-in-the-western-balkan-information-environment-susceptibility-to-russian-influence/216
9. *East StratCom Task Force in the Strategic Communication, Task Forces and Information Analysis.* https://www.eeas.europa.eu/eeas/contract-agent-fg-iii-post-strategic-communications-assistant-east-stratcom-task-force-strategic_und_en

10. European Parliament, *Strategic communications as a key factor in countering hybrid threats*, 2021, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656323
11. European Union, *Joint Framework on countering hybrid threats, a European Union response', Joint Communication to the European Parliament and the Council*, https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:52016JC0018R(01)
12. *Foreign Information Manipulation and Interference (FIMI)*, https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html
13. Giannopoulos, Georgios; Smith, Hanna, Theocharidou Marianthi, *The landscape of Hybrid Threats: A conceptual model,* https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/
14. *Good practice principles for public communication responses to mis- and disinformation*, https://www.oecd-ilibrary.org/governance/good-practice-principles-for-public-communication-responses-to-mis-and-disinformation_6d141b44-en
15. *Hybrid Threats: A Strategic Communications Perspective - StratCom COE.* https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79,
16. Jankowski, Nicolas W., *Researching Fake News: A Selective Examination of Empirical Studies*, https://doi.org/10.1080/13183222.2018.1418964
17. Lucas, Edward; Pomerantsev, Peter, *Winning the Information War*, https://cepa.org/comprehensive-reports/winning-the-information-war/
18. NATO, *ACO Strategic communications AD 95-2/21 May 2012*, https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf
19. Parlamentul Republicii Moldova, *Lege privind Centrul pentru Comunicare Strategică și Combatere a Dezinformării și modificarea unor acte normative*, https://presedinte.md/app/webroot/uploaded/Proiect%20Lege%20Centrul%20CSC%20Dezinformare%2005.07.23.pdf
20. Parlamentul Republicii Moldova, *Strategia Națională de Securitate a Republicii Moldova*, https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023.pdf
21. Siman, Bernard, *Countering FIMI: A Critical Imperative for Mission Safety*, https://www.egmontinstitute.be/countering-fimi-a-critical-imperative-for-mission-safety/
22. *Strategic communications hybrid threats toolkit. Comunications to understand and counter grey zone threats*, https://stratcomcoe.org/cuploads/pfiles/Strategic-Communications-Hybrid-Threats-Toolkit_Rev_12l.pdf
23. *Tackling Online Disinformation: An European Approach*, https://ec.europa.eu/information_society/newsroom/image/document/2018-28/presentationcomm_paolo_cesarini_202D869F-9A13-6D79-FC46C00EAAE3E9AC_53429.pdf,
24. *The Countering Hybrid Warfare in the Black Sea Region*, https://csd.eu/fileadmin/user_upload/publications_library/files/2024_2/Countering_Hybrid_Warfare_Black_Sea_Region_ENG_fin.pdf
25. *The Influence and Effects of the Politics, Information and Communication Mix*, https://www.cambridge.org/core/books/rethinking-warfare-in-the-21st-century/05181F92A0DFD584C1C609430F01B324
26. *Understanding Hybrid Threats,* Helsinki, 2020. https://www.hybridcoe.fi/
27. US Department of Defence, *Strategy for operations in the information environment, 2023*, https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF
28. Weissmann, Mikael, *Conceptualizing and countering hybrid threats and hybrid warfare*, https://www.academia.edu/83737397/Conceptualizing_and_countering_hybrid_threats_and_hybrid_warfare?nav_from=39e5c9a6-48a6-443e-8135-8ce4d77af977

Websites

1. https://cepa.org/
2. https://commission.europa.eu/
3. https://csd.eu/

4. https://cset.georgetown.edu/
5. https://e-arc.ro/
6. https://ec.europa.eu/
7. https://ec.europa.eu/
8. https://eur-lex.europa.eu/
9. https://media.defense.gov
10. https://presedinte.md/
11. https://stratcomcoe.org/
12. https://stratcomcoe.org/
13. https://www.academia.edu/
14. https://www.act.nato.int/
15. https://www.asianscientist.com/
16. https://www.eeas.europa.eu/
17. https://www.europarl.europa.eu/
18. https://www.foreignaffairs.com/
19. https://www.hybridcoe.fi/
20. https://www.kas.de/
21. https://www.oecd-ilibrary.org/
22. https://www.routledge.com
23. https://www2.deloitte.com/us/