DOI: 10.25768/1646 - 4974n42a09

Strategic Communication as a Governance Function in Countering Hybrid Threats

Ciprian Cucu
West University of Timişoara
ciprian.cucu@e-uvt.ro

Abstract

Hybrid threats challenge democratic states by exploiting societal vulnerabilities, while remaining difficult to detect and attribute. Contemporary research has emphasized whole-of-society responses, aimed at building societal resilience. However, the role of strategic communication within this response architecture remains insufficiently conceptualized and is often reduced to discrete functions such as counter-disinformation, crisis messaging, or counter-narrative production. This article argues that strategic communication should instead be understood as a governance function. Drawing on literature on hybrid threats, societal resilience, governmental communication, and strategic communication, the article identifies five interrelated governance functions: sensemaking, coordination, legitimacy, intervention, and learning. It then proposes a six-phase framework that embeds these functions across the full response cycle: vulnerability mapping, detection, assessment, response design, communication and coordination, and evaluation and learning. The article further examines the role and limits of technological tools in supporting this cycle, arguing that such tools can enhance situational awareness and decision support but cannot substitute human judgment and institutional coordination. Finally, it identifies democratic safeguards and framing risks that should constrain strategic communication responses, including misaligned, excessive, misattributed, and ambiguous framing. The article contributes a conceptual model for understanding how strategic communication can support resilient, proportionate, and democratically legitimate responses to hybrid threats.

Keywords: strategic communication, governmental communication, hybrid threats

Comunicação Estratégica como Função de Governação no Combate a Ameaças Híbridas

Resumo

As ameaças híbridas exploram vulnerabilidades sociais e desafiam Estados democráticos, permanecendo difíceis de detetar e atribuir. Embora a investigação recente destaque respostas de toda a sociedade e o reforço da resiliência, o papel da comunicação estratégica continua subdesenvolvido e frequentemente limitado a funções isoladas, como contradesinformação ou comunicação de crise. O artigo propõe compreender a comunicação estratégica como uma função de governação, identificando cinco funções interligadas — sensemaking, coordenação, legitimidade, intervenção e aprendizagem — e integrando-as num modelo de seis fases do ciclo de resposta: mapeamento de vulnerabilidades, deteção, avaliação, desenho da resposta, comunicação e coordenação, e avaliação e aprendizagem. Analisa ainda o contributo e os limites das ferramentas tecnológicas, argumentando que estas podem reforçar a consciência situacional e o apoio à decisão, mas não substituem o juízo humano nem a coordenação institucional. Por fim, identifica salvaguardas democráticas e riscos de enquadramento que devem orientar e limitar a ação comunicacional. O artigo oferece, assim, um modelo conceptual para compreender como a comunicação estratégica pode apoiar respostas resilientes, proporcionais e democraticamente legítimas às ameaças híbridas.

Palavras-chave: comunicação estratégica; comunicação governamental; ameaças híbridas

Data de submissão: 2026-01-23. Data de aprovação: 2026-05-14.

Revista Estudos em Comunicação é financiada por Fundos FEDER através do Programa Operacional Factores de Competitividade – COMPETE e por Fundos Nacionais através da FCT – Fundação para a Ciência e a Tecnologia no âmbito do projeto *LabCom – Comunicação e Artes, UIDB/00661/2020.*

1. Introduction

Hybrid threats have become a central concern for democratic societies, because they exploit existing vulnerabilities across political, informational, social, economic, cyber, and institutional domains, often remaining below the threshold that would trigger a traditional military or legal response.

In the European and NATO policy environment, hybrid threats are increasingly understood as coordinated and illegitimate activities that seek either to undermine and eventually replace the governing regime of the target state, or to paralyze its decision-making capacity by fostering internal polarization, institutional distrust, and cognitive fatigue within society (Simons, 2023; Lanoszka, 2016).

Disinformation, cyber operations, economic pressure, electoral interference, lawfare, sabotage, and cognitive manipulation are not necessarily hybrid threats in isolation. They become part of the hybrid-threat landscape when they are combined, synchronized, and directed toward strategic political objectives. This is why countering hybrid threats requires more than targeted responses to individual domains such as cybersecurity, disinformation, electoral security etc.

This shift has also changed the logic of defence, with recent policy and academic debates increasingly converging around a whole-of-society approach. Such approaches focus on increasing societal resilience, understood not only as the ability to absorb and recover from disruption, but also as the capacity to anticipate, adapt, and prepare for different future scenarios (Jungwirth et al., 2023; European Commission, 2025). In this perspective, resilience depends on the coordinated participation of state institutions, civil society, private actors, media, academia, and citizens, as well as on the preservation of public trust and democratic legitimacy.

Strategic communication occupies a crucial but still insufficiently explored position in this defence architecture. Especially in hybrid-threat domains (migration, civil rights, media, elections), communication is not merely a tool for disseminating official messages. It is also a mechanism of coordination, sensemaking, legitimacy-building, deterrence, and institutional learning. Because hybrid threats operate partly by manipulating perceptions, exploiting ambiguity, and weakening the relationship between citizens and institutions, strategic communication becomes essential to how democratic states interpret threats, align institutional action, engage publics, and preserve trust while avoiding overreaction or politicization.

This article argues that strategic communication should be conceptualized not only as a messaging or counter-disinformation activity, but as a governance function that connects vulnerability assessment, threat detection, institutional coordination, public engagement, proportional intervention, and democratic accountability.

Objectives and research questions

Despite the growing emphasis on countering hybrid threats by building societal resilience through whole-of-society approaches, the role of strategic communication remains underdeveloped. Existing approaches often acknowledge the importance of communication, but they tend to focus on issue-specific functions: public messaging, counter-disinformation, debunking, counter-narratives, crisis communication etc. While these functions are important, they do not fully capture the broader strategic role that communication plays in democratic responses to hybrid threats.

As a result, strategic communication is often positioned as a supporting activity within hybrid--threat response rather than as a core governance function that connects detection, assessment, coordination, intervention, evaluation, and democratic accountability.

In hybrid-threat contexts, official communication may fail not only by being absent or delayed, but also by being excessive, ambiguous, misaligned, politicized, or disproportionate. A state response that

over-securitizes public debate, misattributes hostile activity, amplifies adversarial narratives, or undermines democratic values can weaken rather than strengthen resilience. Therefore, countering hybrid threats requires not only more communication, but strategically coherent, evidence-based, proportionate, and democratically legitimate communication.

The objective of this article is to propose a conceptual framework for understanding strategic communication as an integrative governance function in democratic responses to hybrid threats. Rather than treating strategic communication only as counter-messaging or public information, the article conceptualizes it as a mechanism that supports the full cycle of hybrid-threat response: identifying societal vulnerabilities, detecting emerging signals, assessing actors and narratives, designing proportional interventions, coordinating stakeholders, communicating with relevant publics, and evaluating outcomes for institutional learning.

The article aims to contribute to the literature on hybrid threats, resilience, and strategic communication by clarifying how strategic communication can support whole-of-society defence while remaining anchored in democratic principles such as transparency, proportionality, public interest, accountability, and protection of civil liberties.

Research questions

This article is guided by the following main research question: *How can strategic communication be conceptualized as an integrative governance function within whole-of-society responses to hybrid threats?* To answer this question, the article breaks it down in the following sub-questions:

RQ1. How do hybrid threats target democratic societies and institutions, and how do whole-of-society approaches structure the response?

RQ2. What governance functions should strategic communication perform in countering hybrid threats?

RQ3. How can these functions be organized into a strategic communication framework that supports societal resilience while remaining proportional, credible, and democratically legitimate?

2. Hybrid threats and the whole-of-society response

2.1. From hybrid warfare to hybrid threats

The concepts of "hybrid warfare", "grey zone conflict", and "hybrid threats" have been for a while used interchangeably in academic and public discourse. However, recent policy and research suggest the distinction is important. While all three concepts point to the blurring of boundaries between war and peace, they differ in their analytical focus and policy implications.

The concept of hybrid warfare emerged from military and strategic studies. Hoffman (2007) used the term to describe how state and non-state actors were conducting increasingly complex and interconnected, "synergistic" activities that posed a significant danger to other states. In this sense, hybrid warfare was initially concerned with the changing character of war and with the operational challenges posed by actors capable of combining different instruments of conflict.

The related concept of grey zone conflict also refers to the blurred space between peace and open war, but its emphasis is on strategic competition below the threshold of conventional armed conflict. In this sense, grey zone conflict is less a description of how actors fight and more a description of how they

compete without triggering a traditional military response. Ambiguity, deniability, incremental pressure, and calibrated escalation are central to this logic (Mazarr, 2015; U.S. Special Operations Command, 2015).

The term "hybrid threats" developed in a more policy-oriented direction, focusing not on the tools used, but on the way those tools are synchronized to exploit weaknesses in democratic political systems. Recent research (Giannopoulos et al., 2021; Bertolini et al., 2023) places the targeting of civil societies by exploiting societal vulnerabilities (e.g., polarization, ethnic tensions, conflicting rights) at the centre of the concept.

While in "hybrid war" the aggressor is confident regarding its capacity to dominate their targets militarily if needed, Heier (2023) argues that the hybrid threats are predicated on the opposite, on a "battle avoidance" approach. Using Russia's hybrid attacks on European democracies as a case study, he argues that, contrary to a common perspective of Russia as a significant military threat, it is rather a declining power that would be "unable to seize and control NATO territories", thus focuses on non-military means and uses their military for intimidation, "a mafiosi tool designed to install fear, anxiety, and respect among Western policy makers and citizens" (Heier, 2023, p. 130).

The shift from "hybrid warfare" to "hybrid threats" represents moving away from a primarily military understanding of conflict toward a broader governance problem. Hybrid threats target the connective tissue of democratic societies: trust in institutions, confidence in public information, social cohesion, political accountability, and the capacity of governments to make and implement decisions.

This article uses the concept of hybrid threats rather than hybrid warfare because its concern is not primarily with the conduct of war, but with the governance challenge posed by hostile, coordinated, and often ambiguous activities that exploit democratic vulnerabilities below the threshold of open conflict.

This conceptual choice is also important for understanding the role of strategic communication. If hybrid threats work by manipulating meaning, amplifying uncertainty, and weakening trust between citizens and institutions, then the response cannot be limited to military deterrence, cybersecurity, or technical countermeasures. It must also involve the capacity of democratic institutions to interpret threats, coordinate action, communicate credibly, and preserve legitimacy under conditions of uncertainty.

2.2. The logic of whole-of-society defence

The strategic relevance of hybrid threats lies in the way they interact with the inherent weaknesses of democratic societies. Hybrid actions are not limited to targeting state capacity in an administrative or military sense but aim to undermine the social conditions that allow democratic systems to function public trust, political accountability, social cohesion, reliable information flows, institutional legitimacy, and the perceived capacity of authorities to act in the public interest.

Hybrid actors exploit the openness of democratic societies: freedom of expression, political pluralism, decentralized media systems, protest rights, electoral competition, and public contestation. These are foundations of democratic systems and are not weaknesses in themselves; however, they become exploitable when states deal with low institutional trust, high polarization, corruption, social inequalities, weak public services, or unresolved identity conflicts. In such contexts, hostile actors do not need to create social conflict but amplify existing grievances, weaponize uncertainty, distort public debate, and increase the perceived distance between citizens and their governments (Heier, 2023).

This is why hybrid threats cannot be reduced to isolated incidents or domain-specific disruptions. A cyberattack may have technical effects, but its wider strategic impact may depend on whether it reinforces narratives of state incompetence. A disinformation campaign can have relevant political effect if it resonates with pre-existing distrust. Economic pressure can also be used to frame democratic go-

vernments as incapable of protecting citizens. Sabotage or disruption of critical infrastructure function beyond the physical damage, as symbolic communication signalling vulnerability, uncertainty, and loss of control.

The logic of hybrid threats thus demands responses that are not limited to individual sectors. Cybersecurity, military deterrence, factchecking, platform regulation, counter-disinformation, intelligence monitoring, and crisis communication are all necessary, but they are insufficient when treated as separate instruments.

The current state-of-the-art response, distilled from contemporary policy and academic debates converges toward whole-of-society approaches, that see state institutions, civil society, private actors, media organizations, academia, local communities, and citizens as contributors. The goal is not to militarize society or to place public life under a security logic, but to recognize that resilience cannot be produced by the state alone.

In this sense, whole-of-society defence shifts attention from reacting to hostile acts toward identifying and mitigating vulnerabilities before they are exploited. This approach is visible in models such as the EU's CORE framework (Jungwirth et al., 2023), which conceptualizes democratic societies as complex resilience ecosystems composed of interdependent domains, including information, politics, law, public administration etc. The importance of such models lies in their systemic perspective: hybrid threats do not act on isolated institutions, but on the relations among institutions, citizens, infrastructures, narratives, and expectations.

As mentioned, the goal of whole-of-society defence is societal resilience in a pro-active understanding, that includes the capacity to anticipate threats, adapt to changing conditions, maintain democratic legitimacy, and preserve public trust during periods of uncertainty.

Trust is one of the core conditions of this approach, since citizens are more likely to withstand manipulation, accept difficult decisions, and support institutional responses when they believe that authorities are competent, honest, and oriented toward the public interest. Conversely, when public services are weak, corruption is widespread, communication is poor, or citizens feel ignored, hostile narratives encounter a more receptive environment. In such cases, disinformation and other influence operations are not effective merely because they are technologically sophisticated, but because they attach themselves to existing grievances and credibility gaps.

This point is especially important for democratic governance. Resilience cannot be built only through technical capacity, surveillance, or coercive instruments. Measures that protect infrastructure, cybersecurity, borders, or electoral systems must be complemented by measures that reinforce social cohesion, media literacy, civic participation, transparency, independent journalism, and institutional accountability. Otherwise, the response may protect systems while leaving the underlying vulnerabilities intact. A society may have strong technical defences but remain vulnerable if citizens distrust institutions, reject official information, or interpret state action through adversarial frames.

Whole-of-society defence requires coordination, but also restraint, as democratic states must respond to hybrid threats without undermining the democratic principles they seek to protect. This creates significant challenges, since authorities must identify and counter illegitimate interference while preserving legitimate dissent, pluralism, freedom of expression, and political contestation. They must communicate risks clearly, but without alarmism, and must coordinate institutional responses without converting public communication into propaganda or partisan messaging.

Strategic communication comes into focus as part of the response mechanism itself, rather than as a secondary activity that follows policy decisions. In whole-of-society defence, the communicative challenge is not simply to "send the right message," but to sustain the relationships, meanings, and forms of coordination that allow democratic societies to resist manipulation and coercion.

2.3. Communication, meaning, and trust in hybrid-threat contexts

As the article has shown, hybrid threats are not defined only by the material effects of hostile actions, but also by the meanings those actions acquire in the public sphere. Their strategic impact often depends on how events are interpreted, and how narratives are amplified and connected to broader perceptions of institutional competence or failure.

This communicative dimension is especially important because ambiguity is one of the defining characteristics of hybrid threats. Their effectiveness often depends on making it difficult to determine what has happened, who is responsible, whether different incidents are connected, and what level of response is warranted. Bertolini et al. (2023) emphasize that hybrid threats frequently remain difficult to distinguish from isolated actions, normal statecraft, or diplomacy precisely because strategic ambiguity is built into their design. Ambiguity slows institutional response, complicates public explanation, and opens space for competing narratives before authorities can establish a credible account of events.

The information environment thus becomes the space in which other actions acquire political and societal significance. Information influence activities are designed to interfere with the processes through which citizens form opinions and make sense of public affairs, using deceptive, manipulative, and disruptive techniques to benefit hostile actors (Pamment et al., 2018). However, as Lucas and Pomeranzev (2016) argue, the goal is not to persuade citizens of one stable alternative reality, but to produce disorientation, uncertainty, and exhaustion, thus weakening the shared reference points that democratic decision-making requires.

This helps explain why hybrid-threat responses cannot focus exclusively on correcting false content. Disinformation matters, but it is only one mechanism within a wider struggle over meaning. Pamment et al. (2018) show that influence operations commonly rely not on isolated techniques, but on coordinated "stratagems" such as laundering, flooding, polarization, and point-and-shriek tactics, all of which manipulate visibility, credibility, and emotional salience rather than merely factual accuracy.

Recent work on cognitive warfare and cognitive hacking reinforces this point. These concepts shift attention from the manipulation of individual pieces of information to the manipulation of the cognitive and social conditions under which information is processed. Bârgăoanu and Durach (2023) describe cognitive warfare as an effort to disrupt public conversations, cultivate doubt, and produce polarization that is both emotional and cognitive. Rather than targeting only what people think, such approaches target how they evaluate information, how they perceive institutions, and how they respond to uncertainty. From this perspective, democratic vulnerability is not limited to exposure to false claims; it also includes exposure to communicative environments that normalize distrust, suspicion, and interpretive instability.

Trust is central in this dynamic because it mediates the relationship between events, official responses, and public interpretation. Citizens do not evaluate every claim independently, but rely on institutions, media, experts, and social networks as credibility structures. Hybrid threats seek to weaken these structures by portraying public authorities as incompetent or malevolent, independent media as corrupt, experts as politically captured, and democratic procedures as fraudulent or meaningless. When such narratives take hold, the state's capacity to respond is diminished: public warnings get ignored, factual corrections are dismissed as propaganda, and necessary security measure become reframed as authoritarian overreach.

The communicative problem is twofold: democratic institutions must be able to provide explanations under conditions of uncertainty without overstating what is known, while at the same time acknowledge that "everything communicates" (NATO StratCom COE, 2019), meaning that silence, delay, vagueness, and contradiction all communicate as well.

At the same time, communication in hybrid-threat contexts cannot be reduced to reactive clarification but includes a preventive and connective role. Citizens are more resistant to manipulation when institutions communicate transparently, when uncertainty is acknowledged rather than concealed, when public decisions are explained in relation to shared values and concrete consequences, and when communication is embedded in broader relationships of institutional competence and accountability. Conversely, no amount of messaging can compensate for sustained governance failure. If public institutions are perceived as corrupt, arbitrary, or incapable of delivering essential services, hostile narratives find fertile ground.

This makes communication central to both the problem and the response. Hybrid threats act on meaning, perception, and trust; whole-of-society defence depends on shared situational awareness, credible institutions, and coordination across multiple actors. The relevant question is not whether communication matters, but how it should be organized as part of democratic governance. If the effects of hybrid threats emerge partly through contested interpretation, then countering them requires more than ad hoc messaging. It requires strategic communication capable of supporting sensemaking, coordination, legitimacy, intervention, and learning across the full response architecture.

3. Governance functions of Strategic Communication in countering hybrid threats

3.1. From governmental communication to strategic communication

Governments have always used communication to inform citizens, explain decisions, mobilize public support, signal priorities, and maintain institutional legitimacy. Yet the fact that government communication may produce strategic effects does not necessarily mean that it is strategic by design.

Strategic communication emerged as a distinct field by emphasizing the deliberate, purposeful, and coordinated use of communication in support of organizational objectives. Hallahan et al. (2007) define it as "the purposeful use of communication by an organization to fulfil its mission" (p. 3), while Holtzhausen and Zerfass (2013) further stress that it takes place in the public sphere, where communicative actors pursue goals in environments shaped by competing meanings and contested interpretations. This perspective is especially relevant for public institutions, whose communication is subject not only to managerial considerations, but also to democratic scrutiny, political contestation, and obligations of transparency and accountability.

Governmental communication has similarly been conceptualized as more than the transmission of administrative information. Canel and Sanders (2015) describe it as communication conducted by executive politicians and officials in pursuit of civic and political purposes, aimed at establishing and maintaining relationships with relevant publics. Canel and Luoma-aho (2019) focus on the public-sector dimension, defining it as goal-oriented communication that enables public functions and contributes to building and maintaining the public good and trust between citizens and authorities. In this sense, governmental communication is closely linked to legitimacy: it affects whether citizens perceive institutions as competent, responsive, fair, and oriented toward their interests.

This connection between communication and legitimacy is central in democratic governance. Public communication is one of the means through which authorities explain policy choices, justify action, make uncertainty intelligible, and enable citizens to evaluate institutional performance. It contributes to trust not simply by persuading citizens, but by making governance more understandable and accountable. At the same time, trust is not produced through communication alone. As Saar (2020) notes, the relationship between public communication and trust is bidirectional: effective communication enhances legitimacy and cooperation (promoting trust); on the other hand, low trust in public institutions

can reduce citizens' willingness to engage or comply with policies, which puts additional pressure on government communication. Strategic communication cannot compensate for failures of governance, yet it can either reinforce or undermine the credibility of governmental action.

The distinction between governmental communication and strategic communication is not one between communication and non-communication, but between *communication as an activity* and *communication as an intentionally integrated function of governance*. Governmental communication becomes strategic when it is aligned with public objectives, coordinated across relevant institutions, attentive to the dynamics of the public sphere, and capable of anticipating how messages, decisions, and silences may be interpreted.

Hybrid threats intensify these demands, as fragmented or purely reactive communication can become a vulnerability in itself. Contradictory messages from different agencies, delayed acknowledgement of uncertainty, politicized explanations, or technically accurate but publicly unintelligible statements may create interpretive gaps that hostile actors can exploit. Conversely, strategically coherent communication can help preserve orientation, connect institutional actions to public values, and reduce the space in which adversarial narratives gain traction.

This does not imply that democratic governments should seek to control the information environment or treat citizens as objects of influence. The legitimacy of strategic communication depends on its contribution to public understanding, democratic accountability, and the protection of the public interest. For this reason, the use of strategic communication in countering hybrid threats must be grounded in factuality, proportionality, transparency, and respect for democratic pluralism.

For the purposes of this article, strategic communication is thus understood as the deliberate and coordinated use of communication by public institutions to support democratic governance in contested and uncertain public environments. In hybrid-threat contexts, this requires moving beyond the dissemination of official messages or the correction of falsehoods toward a broader role in connecting institutional interpretation, action, legitimacy, and societal resilience. The following subsection develops this argument by conceptualizing strategic communication as a governance function within hybrid-threat response.

3.2. Strategic communication as a governance function

In hybrid-threat contexts, strategic communication should be understood not as a specialized messaging activity appended to the security policy, but as a governance function that helps democratic institutions interpret threats, coordinate action, preserve legitimacy, intervene proportionately, and learn from evolving challenges.

This broader role is recognized in parts of the strategic communication literature on hybrid threats. Hansen and Gill (2021) describe strategic communication as a "mindset or philosophy" supported by processes and capabilities, and as a function of statecraft located at the intersection of strategy and action. Balomenos (2023) similarly argues that strategic communication helps manage crises (including ones resulted from hybrid threats) assess and shape human perception of unfolding situations.

Conceptualized as a governance function, strategic communication performs several interrelated roles: sensemaking, coordination, preserving/building legitimacy, intervention, and learning.

Sensemaking function

Hybrid threats are difficult to address because they are meant to be ambiguous: their origin is usually unclear, their effects may be distributed across domains, and their significance becomes visible through patterns rather than isolated incidents.

Strategic communication contributes to governance by helping institutions and publics clarify such ambiguity. Internally, it supports the interpretation of emerging signals, identifies information voids, and connects technical assessments to broader questions of public meaning and likely social impact. Externally, it helps explain what is known, what remains uncertain, why certain developments matter, and how authorities understand the situation without claiming more certainty than the evidence allows.

The sensemaking role is particularly important because hybrid actors often seek to exploit the delay between events and communication about the events, or contradictions in messages. When authorities hesitate or contradict one another, hostile actors gain opportunities to define the interpretation first. In such moments, the public sphere does not remain neutral or empty, but becomes filled by speculation, conspiratorial interpretations, and politically motivated reframing.

Strategic communication cannot eliminate uncertainty, but it can reduce interpretive vulnerability by providing timely orientation and by making uncertainty itself intelligible. This is consistent with OECD (2023) principles for public communication responses to mis- and disinformation, which emphasize timeliness, transparency, prevention, and evidence-based communication.

Coordination function

Whole-of-society responses to hybrid threats depend on multiple actors whose actions and messages risk becoming fragmented or contradictory: national government bodies, local authorities, intelligence and security institutions, public-service providers, regulators, civil society organizations, journalists, experts, and international partners. Strategic communication helps connect these actors by aligning their understanding of the problem, clarifying institutional responsibilities, and ensuring that public communication is coherent and doesn't contradict operational action.

The coordination role also extends beyond the state, as whole-of-society approaches include actors that are not part of any command chain. NGOs, independent media, researchers, professional associations etc are not mere channels for official messages but have their own agency and publics. Strategic communication should facilitate cooperation without dissolving institutional boundaries or compromising independence; the challenge is to build coordination through trust and shared purpose, not through centralization of discourse.

Legitimacy function

Part of the means by which hybrid threats work to erode confidence in democratic institutions is portraying authorities as corrupt, incompetent, captured, or indifferent to citizens' concerns. In this context, the credibility of the response matters as much as its timeliness or accuracy. Strategic communication supports legitimacy when it helps institutions justify decisions, explain trade-offs, acknowledge uncertainty, and show how actions serve the public interest. It also contributes to legitimacy by maintaining distinctions between democratic protection and political opportunism. Countering hybrid threats cannot become a pretext for branding criticism as disloyalty or dissent as manipulation.

This function builds on broader scholarship on governmental communication, which links public communication to trust, accountability, and the public good (Canel & Sanders, 2015; Canel & Luoma-aho, 2019). It is also consistent with Pamment et al. (2018), who argue that communicators responding to information influence activities should focus not on "outwitting" adversaries, but on protecting citizens' ability to form opinions free from illegitimate interference. The legitimate purpose of strategic communication is not domination of the public sphere, but preservation of democratic conditions for judgment and participation.

Legitimacy also requires proportionality. Because hybrid threats are often ambiguous and difficult to attribute, responses may easily become excessive or premature. Bertolini et al. (2023) note that

effective deterrence depends on the ability to detect and attribute hybrid attacks, but this also means that public communication must be calibrated to the strength of available evidence. If authorities communicate suspicion as certainty or exaggerate a threat for mobilizational purposes, they risk weakening trust and reinforcing adversarial claims that institutions are manipulative or authoritarian. Strategic communication thus contributes to legitimacy not merely by persuading publics, but by disciplining the response itself.

Intervention function

This is the role most often acknowledged in policy discussions: countering hostile narratives, raising awareness, prebunking likely manipulations, debunking false claims, developing counter-frames, communicating crisis information, and signalling deterrence. García et al. (2021) argue that strategic communication is crucial for deconstructing hostile argumentation and promoting counter-narratives, while Hansen and Gill (2021) describe it as a "retaining wall" against persistent information manipulation. Bertolini et al. (2023) also emphasize its value for deterrence, particularly when states signal resilience, capability, and willingness to impose costs for unacceptable interference.

However, strategic communication should connect intervention to wider resilience objectives, not be limited to counter-messaging, as that would be only addressing symptoms while leaving structural vulnerabilities unexamined.

Intervention also includes deterrence, either "by punishment" - signalling that hostile actors may face meaningful costs, or "by denial" - showing that attacks are unlikely to achieve their purpose (Bertolini et al., 2023). However, such attempts are predicated on existing credibility. Empty threats, exaggerated claims of preparedness, or narratives of resilience contradicted by institutional weakness are unlikely to deter adversaries and may damage domestic trust.

Learning function

Hybrid threats evolve through adaptation: hostile actors test reactions, reuse vulnerabilities, shift platforms, and recalibrate narratives in response to resistance. Democratic institutions must be able to learn from their own communication and from the information environment. Pamment et al. (2018) propose a preparation–action–learning cycle for communicators responding to influence operations, stressing the importance of documenting cases, assessing effects, and integrating lessons into future practice. This principle should be generalized to strategic communication governance more broadly.

Learning requires evaluation not only of whether a message reached its intended audience, but of whether it produced orientation, trust, compliance, resilience, or unintended backlash. It should also examine whether official communication was reframed by hostile actors, whether institutional coordination worked, whether uncertainty was handled effectively, and whether public interventions inadvertently amplified the narratives they sought to contain. In hybrid-threat contexts, success cannot be measured simply by visibility or message volume. A highly visible intervention that increases polarization or distrust may represent failure rather than success.

The learning function also links strategic communication to institutional adaptation. Recurrent failures of communication may reveal deeper problems: unclear decision-making procedures, fragmented authority, insufficient situational awareness, weak engagement with local communities, or inadequate mechanisms for assessing public concerns. When treated as a governance function, strategic communication should not only refine future messages, but also inform how institutions prepare, coordinate, and act. In this sense, communication becomes part of a feedback system between threat perception, institutional response, and democratic resilience.

4. A Strategic Communication governance framework for countering hybrid threats

The functions presented in section 3 can be organized within a response architecture that reflects the temporal and institutional logic of hybrid-threat defence. The proposed framework conceptualizes strategic communication as embedded throughout the response process, rather than activated only at the stage of public messaging. It organizes the role of strategic communication across six connected phases: vulnerability mapping, detection, assessment, response design, communication and coordination, and evaluation and learning.

The framework builds on several insights developed in existing scholarship and policy models, while integrating them into the main argument: strategic communication is a governance function that connects the identification of vulnerabilities with the design, execution, and evaluation of democratic responses.

Whole-of-society approaches emphasize that hybrid threats exploit vulnerabilities across interconnected social, political, informational, and institutional domains, requiring anticipatory and coordinated responses rather than isolated countermeasures (Jungwirth et al., 2023). Research on information influence activities stresses that communicators must move through a cycle of preparation, action, and learning, while preserving democratic principles and avoiding disproportionate responses (Pamment et al., 2018). Strategic communication toolkits for hybrid threats similarly underline the need for alignment between strategy, actions, narratives, and institutional capabilities (Hansen & Gill, 2021).

The proposed framework aims to bring these insights together into a governance cycle that places strategic communication across the full response architecture. It is not a crisis communication model activated only after a visible incident, nor a counter-disinformation model centred on hostile narratives, but reflects the idea that, in hybrid-threat contexts, communication is not simply part of the response; it shapes how the response is understood, calibrated, coordinated, and learned from.

4.1. Framework overview

Hybrid-threat response should not be conceived as a linear sequence triggered after a hostile event becomes visible, since hybrid actions develop gradually, remain ambiguous, and exploit vulnerabilities that predate the concrete action itself.

For this reason, the cycle begins with *vulnerability mapping*: democratic institutions must maintain an informed understanding of the social, institutional, and informational conditions that make certain threats likely to succeed. These may include low trust in public institutions, polarized public debates, weak media ecosystems, recurring conspiracy narratives, grievances linked to public-service failures, or policy domains that are especially prone to manipulation.

The second phase focuses on *detection* - the identification of emerging signals that may indicate hostile activity or the exploitation of known vulnerabilities. These signals may include sudden amplification of polarizing narratives, coordinated inauthentic behaviour, the spread of misleading interpretations around a crisis, or other anomalies in the information environment that suggest the presence of manipulative interference. Detection should cast a relatively wide net, but it should not automatically trigger a response.

Deciding if a response is warranted is the role of the third phase, *assessment*. In this phase, detected signals are evaluated in context: what actors appear to be involved, what narratives or frames are circulating, what evidence exists of coordination or manipulation, what audiences are affected, what vulnerabilities are being targeted, and what degree of confidence is warranted regarding attribution.

The fourth phase, *response design*, translates assessment into possible courses of action. Not all threats require the same response, and some may require no direct public intervention at all. Strategic

communication contributes by helping institutions determine whether the appropriate response is to monitor, inform, warn, prebunk, debunk, coordinate with third parties, initiate a broader resilience campaign, or support non-communicative policy action. This phase also requires anticipating risks: whether an official intervention may amplify a narrative, whether attribution is sufficiently robust, whether the tone of communication could provoke unnecessary fear, and whether the proposed action aligns with democratic principles.

The fifth phase is *communication and coordination*, i.e., the execution of the chosen response, which includes public-facing communication, but is not limited to message dissemination. This phase involves aligning relevant government institutions, engaging external stakeholders, preparing media and expert briefings, supporting civil-society actors with credible information, and ensuring that communicative action is consistent with policy action. The central concern is not only what is said, but whether the wider response appears coherent, legitimate, and intelligible to affected publics.

The cycle ends with *evaluation and learning*, assessed not simply in terms of visibility or message reach, but in terms of their contribution to public understanding, trust, resilience, and institutional coordination. Did the response reduce uncertainty or increase it? Did it prevent harmful narratives from escalating, or inadvertently amplify them? Were different institutions aligned? Did hostile actors successfully reframe the intervention? The answers to such questions should feed back into both vulnerability mapping and future response protocols.

The six phases form a cycle rather than a closed sequence. Evaluation may reveal vulnerabilities that were previously underestimated. Assessment may show that an apparently new narrative is connected to a long-standing grievance already present in vulnerability maps. Communication and coordination may expose institutional gaps that require changes in preparedness. The cyclical structure reflects the adaptive nature of hybrid threats and the need for democratic institutions to learn continuously.

The framework also clarifies the place of strategic communication within hybrid-threat governance. It is not confined to intervention itself, where institutions publicly communicate, but operates throughout the cycle:

- in vulnerability mapping, by identifying societal weaknesses;
- in detection, by monitoring emerging narratives and communicative anomalies;
- in assessment, by interpreting frames, targeted audiences, and likely effects;
- in response design, by evaluating timing, proportionality, credibility, and risks;
- in communication and coordination, by aligning actors, actions, and public explanation;
- in evaluation and learning, by assessing communicative effects and institutional adaptation.

Table 1. Strategic communication governance framework for countering hybrid threats

Phase	Core question	Strategic communication contribution
1. Vulnerability mapping	What pre-existing conditions could hostile actors exploit?	Identifies trust gaps, contested issues, and societal vulnerabilities (e.g., ethnic tensions, economic inequalities, perceived corruption, low media and digital literacy etc).
2. Detection	What emerging signals require attention?	Monitors narratives, amplification patterns, and shifts in public meaning.
3. Assessment	What is happening, how serious is it, and how confident are we?	Interprets likely actors and attribution confidence, frames, intended audiences, and communicative risk
4. Response design	What should be done, and what should be avoided?	Considers whether a response is warranted. Develops proportionate options, message frames, coordination plans, and amplification-risk assessments.
5. Communication and coordination	How should the response be enacted?	Aligns institutions and stakeholders; delivers public-facing communication and supporting materials
6. Evaluation and learning	What effects did the response produce?	Assesses effects on public understanding, changes in vulnerability indicators, reframing, backfire, and provides recommendations for future preparedness

4.2. Technical and technological tools: support, not substitute

The Strategic Communication governance cycle outlined above can be supported by technological tools that can improve situational awareness, structure complex information, reduce response delays, and assist human analysts in identifying relevant patterns.

Such tools may contribute across all six phases of the framework, but their role should be understood as support, not as a substitute for human judgment and institutional coordination. This distinction is important because hybrid threats are difficult to reduce to stable technical indicators.

In the vulnerability mapping phase, indicator-based dashboards, composite indices, and foresight instruments can support a more systematic understanding of societal weaknesses and resilience capacity. The European Commission's Resilience Dashboards, for example, assess vulnerabilities and capacities across social and economic, green, digital, and geopolitical dimensions, helping identify areas that may require further policy attention (European Commission Joint Research Centre, n.d.). Such tools are relevant to hybrid-threat governance because they can inform prior assessments of the conditions that hostile actors may seek to exploit, although they remain dependent on the quality, granularity, and timeliness of the indicators they use.

The detection phase would benefit most from strong, automated tools, yet these are difficult to develop and implement. Rietjens (2020) argues that early warning for hybrid threats is intrinsically challenging because such threats are "ambiguous and fuzzy," involve a wide range of military and non-military instruments, and lack fixed standards for detection and warning. Cullen (2018) similarly describes hybrid-threat early warning as a "wicked problem," in which signals may be weak, dispersed, and difficult to interpret outside their political and social context.

Open-source intelligence systems, social listening platforms, network analysis, anomaly detection, and narrative-monitoring tools can help identify emerging signals: sudden amplification of polarizing claims, coordinated dissemination patterns, clusters of suspicious accounts, or the rapid activation of narratives that attach themselves to an ongoing crisis.

In the specific domain of foreign information manipulation and interference (FIMI), the European External Action Service has developed structured analytical instruments, including a standardized FIMI methodology, a response framework, and the FIMI Exposure Matrix, which maps connections between digital channels and the infrastructure of threat actors (EEAS, 2025). The DISARM Framework also provides a shared taxonomy for describing influence-operation tactics, techniques, and procedures, helping analysts and strategic communication practitioners classify incidents and coordinate responses using a common language (DISARM Foundation, n.d).

The third phase, assessment, can also benefit from tools that classify actors, map networks, detect frames and narratives, compare content across platforms, and assist with multilingual or multimodal analysis. Such systems may help communicators understand how an event is being interpreted, which audiences are being targeted, and which grievances or vulnerabilities are being activated. Yet these tools remain uneven in their capabilities. Pilati and Venturini (2025) argue that AI-based counter-disinformation initiatives require stronger benchmarking, coordination, and safeguards. Similarly, the European Data Protection Supervisor (2025) stresses that human oversight in automated decision-making is meaningful only when human actors have the capacity to evaluate, challenge, and override system outputs. In hybrid-threat assessment, technological outputs should therefore be treated as prompts for expert scrutiny, not as authoritative judgments.

Technical tools may also assist response design and communication and coordination as well. Scenario repositories, structured playbooks, and databases of adversarial tactics can help institutions compare possible courses of action, including whether to monitor silently, issue a clarification, prepare a prebunking message, or coordinate with civil-society actors. The EEAS FIMI Toolbox and Deterrence Playbook illustrate how analytical findings may be linked to coordinated response options (EEAS, 2025). Shared dashboards, secure information-sharing systems, and collaborative repositories can also help align institutions and partners around a common understanding of the situation.

may be supported by social listening, sentiment analysis, frame tracking, media analysis, and other post-response monitoring tools. These can help assess whether an intervention reduced uncertainty, whether official frames were reframed or resisted, and whether public trust or vulnerability indicators shifted. The main challenge is less the absence of tools than their integration into a coherent process guided by human expertise.

Taken together, the current technological landscape suggests neither techno-optimism nor technological dismissal. Tools are becoming more sophisticated and increasingly relevant to hybrid-threat governance, especially in environments characterized by information overload, cross-platform coordination, and rapidly evolving narratives. At the same time, many remain under development, depend on uneven data access, or lack sufficient standardization and benchmarking. Their effectiveness is highest when embedded in human-led, institutionally accountable systems that combine technical capacity with contextual knowledge, democratic judgment, and strategic communication expertise.

5. Democratic safeguards and communication risks

5.1. Democratic safeguards as boundary conditions of the framework

As we have previously stated, the main premise of building any kind of response framework to hybrid threats is starting with protection of democratic principles that hybrid threats seek to undermine. In the case of the proposed framework, such safeguards are not considered as external normative additions to the framework, but boundary conditions of its effectiveness. A response that protects institutions at the cost of pluralism, public trust, or legitimate political contestation risks reproducing the effects of the threat itself.

Democratic societies are defined by disagreement, contestation, protest, and criticism of power. If the hybrid-threat framework is applied too expansively, it may blur the distinction between illegitimate interference and legitimate democratic conflict. This creates a risk of securitizing ordinary public debate and of treating dissent as a vulnerability to be managed rather than as a constitutive feature of democratic life.

The problem is particularly acute in the informational domain. Efforts to counter disinformation, foreign information manipulation, or hostile influence operations are necessary, but they operate in a field where concepts can be politically contested and strategically misused. Bateman and Jackson (2024) note that counter-disinformation efforts can generate overreach and blowback when authorities apply elastic categories too broadly or communicate judgments with insufficient evidentiary caution. The risk is not limited to authoritarian or illiberal systems. Even in democratic contexts, premature or overstated claims about manipulation can be used by hostile actors to portray institutions as censorial, partisan, or unreliable, thereby reinforcing the distrust that countermeasures were meant to reduce.

Strategic communication in hybrid-threat response must preserve a clear distinction between protecting democratic decision-making and controlling democratic debate. As Pamment et al. (2018) argue, communicators responding to information influence activities should focus on protecting citizens' capacity to "make up their own mind free from illegitimate influences," rather than attempting to dominate the information space or "outwit" adversaries. This principle is central to the proposed framework: strategic communication should increase the conditions for informed democratic judgment, not substitute official judgment for public deliberation.

A second safeguard concerns the risk of politicization, as the boundaries between public information and political persuasion are often blurred. Rotaru (2024) identifies this as a structural vulnerability: public officials may "confuse" their institutional roles with their political personas, which undermines the public-interest orientation of governmental communication.

Authorities may be tempted to frame criticism of their policies as evidence of hostile manipulation, to present opponents as vectors of foreign influence without sufficient evidence, or to use national-security rhetoric to reduce the legitimacy of political competition. Such practices would not only violate democratic norms; they would also damage the credibility of future threat communication.

Hybrid threats may target governments, public institutions, electoral processes, or particular policy domains, but the response cannot be owned by the political leadership as a partisan resource. Government communication in this field must remain institutionally grounded and clearly separated from party-political communication.

A third safeguard is proportionality. Hybrid-threat responses may range from passive monitoring to public attribution, regulatory action, deterrent signalling, or coordinated resilience campaigns. Bertolini et al. (2023) argue that responses to hybrid threats should remain proportionate in order to avoid unnecessary escalation and to preserve the legitimacy of countermeasures. This logic applies directly

to strategic communication. Publicly amplifying a marginal narrative, attributing hostile intent before sufficient assessment, or using alarmist frames in a low-confidence situation may cause more harm than the original signal itself.

Proportionality also requires accepting that non-response may sometimes be the most appropriate option. The response-design phase of the framework should not be understood as a mechanism that inevitably produces public messaging. In some cases, silent monitoring, targeted stakeholder briefings, or non-communicative policy action may better protect the public interest than a visible intervention. Strategic communication as governance includes the ability to decide when not to communicate publicly, especially when public attention would raise the salience of a weak or fringe narrative.

Finally, democratic safeguards require that strategic communication remain tied to substantive governance. Communication cannot compensate for failures of institutional/policy performance or public-service delivery. If governments address hybrid threats only through messaging while leaving underlying grievances unaddressed, the response is likely to appear superficial or manipulative. Whole-of-society resilience depends on functioning democratic institutions, not merely persuasive narratives. Strategic communication can explain, coordinate, and support resilience-building measures, but it cannot replace them.

5.2. Framing risks in strategic communication responses

Looking more profoundly at the communication phase of the framework, we should note the central role of framing. In Entman's (1993) formulation, frames select and emphasize aspects of perceived reality in ways that diagnose problems, identify causes, make moral evaluations, and suggest remedies.

When authorities decide a response is warranted and the messaging is being built, framing choices are unavoidable. Authorities must decide whether an incident should be described as a technical disruption, a coordinated hostile act, a disinformation campaign, a threat to democratic integrity, or something else entirely.

Framing also brings specific risks, since government communication unfolds in contested public environments, where official interpretations compete with journalistic accounts, partisan narratives, civil-society perspectives, and adversarial reframing. Frames can backfire if they are poorly aligned with the evidence, with public concerns, or with the wider institutional response.

Research on governmental communication shows that strategic framing does not automatically produce the desired effects. Porumbescu et al. (2022), for example, found that blame-avoidance frames used by political leaders during the COVID-19 pandemic could increase rather than reduce blame attribution, especially when scapegoating was combined with positive performance claims. Similarly, Abdullatif (2024) shows that U.S. counter-terrorism messaging against ISIS did not necessarily resonate with target audiences simply because it was strategically designed. These findings suggest that the framing of strategic responses matters not only for clarity, but also for credibility and legitimacy. In the context of countering hybrid threats, four framing risks deserve particular attention.

- **Misaligned framing**

Occurs when the official interpretation of a threat does not adequately match either the nature of the situation or the public's concerns. Authorities may try framing an incident as foreign interference when citizens perceive it as evidence of domestic institutional failure; they may emphasize manipulation while neglecting the legitimate grievance that made a hostile narrative resonate in the first place. Misaligned framing weakens the sensemaking function of strategic communication because it fails to connect institutional interpretation with the social context.

- **Excessive or overreaction framing**

Institutions may be tempted to dramatize uncertain signals in order to demonstrate vigilance, justify rapid action, or mobilize attention. Yet framing an emerging situation as a major hostile operation before evidence is sufficiently robust can generate fear, amplify marginal narratives, and validate adversarial efforts to portray societies as unstable or governments as panicked. It may also produce "threat inflation," where citizens are repeatedly warned of serious interference but receive little clarity about what has actually occurred, or "fatigue", where citizens disconnect from institutional communication. Overreaction framing can be damaging even when the underlying concern is real, if the intensity of the response exceeds the assessed seriousness of the threat, as the intervention would undermine proportionality and create distrust.

- **Misattribution framing**

Public communication that assigns responsibility too quickly, or blurs the distinction between suspicion and confirmation, can damage institutional credibility if later evidence proves inconclusive or contradictory. Misattribution is especially harmful because attribution itself carries strategic and political consequences: it can shape public perceptions of external actors, justify deterrent measures, influence international coordination, and escalate conflict. This is not to say that authorities should avoid attribution altogether, since responses frequently require public attribution to deter future interference and clarify the nature of the threat. However, the risk lies in communicative overreach. Strategic communication should be precise about evidentiary thresholds and transparent about uncertainty. It should distinguish between observed activity, assessed coordination, likely sponsorship, and formally established responsibility. This is consistent with the broader democratic safeguard that communication should inform judgment rather than substitute assertion for evidence.

- **Ambiguous or weak framing**

If overreaction can damage trust, so can excessive caution. Authorities may communicate in ways that are so vague, delayed, or procedural that they fail to provide orientation during moments of uncertainty. They may avoid naming the nature of a threat, issue fragmented statements across institutions, or rely on technical language that does not help publics understand the significance of events. In such cases, official communication foments speculation instead of preventing it. Furthermore, when public authorities appear reluctant to acknowledge obvious risks, contradict one another, or revise their interpretation without clear explanation, they may be perceived as fearful or incompetent. Strategic communication must balance caution with clarity: uncertainty should be acknowledged but not used as a reason to avoid meaningful public orientation.

These framing risks show that strategic communication responses can fail in opposite directions: by saying too much, too confidently, or too dramatically; but also by saying too little, too vaguely, or too late. The challenge is not to find a "universally correct" frame, but to develop institutional capacity for framing that is evidence-based, context-sensitive, proportionate, and open to revision as situations evolve.

This perspective also reinforces the value of the governance framework proposed above. Vulnerability mapping can help anticipate where official frames may collide with existing grievances. Detection and assessment can distinguish emerging signals from mature threats and reduce pressure toward premature framing. Response design can test possible communicative approaches against amplification,

attribution, and legitimacy risks. Communication and coordination can ensure that institutional action and public explanation reinforce rather than contradict one another. Evaluation and learning can identify when official frames were misunderstood, resisted, or reframed by adversarial actors.

6. Conclusion

Hybrid threats challenge democratic societies through their capacity to exploit existing vulnerabilities. Because they operate across domains and are ambiguous by design, they cannot be countered through isolated measures. The growing emphasis on whole-of-society defence reflects this reality: resilience against hybrid threats depends on the coordinated capacity of democratic institutions, civil society, private actors, media, experts, and citizens to anticipate, withstand, and adapt to disruptive pressures.

The current article argues that, in this type of response architecture, strategic communication should be understood as a governance function. Its role is broader than public messaging, crisis communication, counter-disinformation, or the promotion of counter-narratives. Strategic communication helps democratic institutions make sense of ambiguous threats, coordinate actions across institutional and societal actors, preserve public legitimacy, design proportionate interventions, and learn from the effects of their responses.

To operationalize this argument, the article proposed a Strategic Communication governance framework for countering hybrid threats, organized around six connected phases: vulnerability mapping, detection, assessment, response design, communication and coordination, and evaluation and learning. The framework emphasizes that strategic communication is not activated only after a threat becomes visible and a public message is needed. Rather, it contributes across the full response cycle: by identifying interpretive and trust-related vulnerabilities, monitoring emerging signals, assessing communicative risks, calibrating responses, aligning stakeholders, and evaluating whether interventions supported public understanding, institutional credibility, and societal resilience.

The article also highlighted the role of existing and emerging technological tools as enablers of this process. Monitoring systems, resilience dashboards, taxonomies for information manipulation, analytical platforms, provenance technologies, and AI-supported tools can strengthen situational awareness and decision support. However, they are not sufficient and cannot run autonomously; their value depends on integration into human-led, institutionally accountable systems that combine technical capacity with strategic judgment and communicative competence.

At the same time, conceptualizing strategic communication as a governance function requires clear democratic safeguards. Responses to hybrid threats should not limit ordinary political disagreement, transform government communication into partisan messaging, or treat public persuasion as a substitute for public accountability.

The article also identifies several framing risks that may undermine strategic communication responses: misaligned framing, excessive or overreaction framing, misattribution framing, and ambiguous or weak framing. These risks illustrate that communication can itself become a vulnerability when it fails to balance clarity with caution, vigilance with proportionality, and threat awareness with democratic restraint.

The article makes several contributions. First, it connects the literature on hybrid threats and whole-of-society resilience with strategic communication scholarship, showing that communication is integral to hybrid-threat response. Second, it conceptualizes strategic communication as a governance function grounded in sensemaking, coordination, legitimacy, intervention, and learning. Third, it proposes a framework that organizes these functions into a cyclical response architecture while identifying the democratic constraints and framing risks.

The framework is conceptual and requires further empirical development. Future research could examine how strategic communication capacities are institutionalized in different national contexts, how they interact with existing whole-of-society defence models, and how they perform during concrete hybrid-threat episodes. Comparative work across countries with different levels of institutional trust, resilience infrastructure, and strategic communication capacity could clarify which elements of the framework are most transferable and which remain context dependent. Further research should also investigate the framing risks identified here, particularly how official communication in hybrid-threat contexts may be reframed, resisted, or weaponized within adversarial information environments.

References

Abdullatif, O. A. (2024). *A Framing Analysis of the United States Government Counter-Terrorism Messaging Strategies During the Rise and Fall of ISIS*. University of Leicester. Thesis. https://doi.org/10.25392/leicester.data.25991725.v1

Balomenos, K. (2023). Strategic Communication as a Mean for Countering Hybrid Threats. In *Balomenos, K. et al. (eds.), Handbook for Management of Threats, Springer Optimization and Its Applications 205,* https://doi.org/10.1007/978-3-031-39542-0_1.

Bateman, J., & Jackson, D. (2024, January 31). *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Carnegie Endowment for International Peace. Retrieved October 14, 2025, from https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide

Bârgăoanu, A., & Durach, F. (2023). Cognitive Warfare. Understanding the Threat. In R. Arcos, I. Chiru, & C. Ivan (Eds.), *Routledge Handbook of Disinformation and National Security* (pp. 221–236). https://doi.org/10.4324/9781003190363

Bertolini, M., Minicozzi, R. and Sweijs, T. (2023). Ten Guidelines for Dealing with Hybrid Threats. A Policy Response Framework. The Hague Centre for Strategic Studies.

Canel, M., & Luoma-aho, V. (2019). Public sector communication. Closing gaps between public sector organizations and citizens. Boston, MA: Wiley.

Canel, M., & Sanders, K. (2015). Government communication. In *G. Mazzoleni, K. Barnhurst, K. Ikeda, R. Maia, & H. Wessler (Eds.), The international encyclopedia of political communication*. Boston, MA. Wiley.

Cullen, P. (2018). *Hybrid threats as a new 'wicked problem' for early warning* (Strategic Analysis 8). Hybrid CoE. Retrieved October 26, 2025, from https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-2018-8-Cullen.pdf

DISARM Foundation. (n.d.). DISARM framework. Retrieved October 14, 2025 from https://www.disarm.foundation/framework

Entman, R. M. (1993). Framing: Towards clarification of a fractured paradigm. Journal of Communication, 43(4), 51–58.

European Commission. (n.d.). *Resilience Dashboards*. Retrieved October 28, 2025, from https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report/resilience-dashboards_en

European Commission. (2025). *Foresight Report 2025. Resilience 2.0: Empowering The EU to Thrive Amid Turbulence and Uncertainty*. Retrieved October 29, 2025, from https://commission.europa.eu/document/download/bdba60f0-abb3-42f8-b5be-fd35d693b289_en?filename=SFR2025-Report_web.pdf DOI: 10.2792/6378524

European Data Protection Supervisor. (2025). *TechDispatch #2/2025: Human oversight of automated decision-making.* Retrieved 14 May 2026 from https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-09-23-techdispatch-22025-human-oversight-automated-making_en

European External Action Service. (EEAS) (2025). 3rd EEAS report on foreign information manipulation and interference threats. Retrieved 14 May 2025 from: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

European External Action Service. (EEAS) (2026). 4th EEAS report on foreign information manipulation and interference threats. Retrieved 14 May 2025 from: https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

Fredheim, R. (2023). *Virtual Manipulation Brief: Generative AI and its Implications for Social Media Analysis*. NATO STRATCOM COE. Retrieved October 29, 2025, from https://stratcomcoe.org/pdfjs/?file=/publications/download/Virtual-Manipulation-Brief-2023-1-digital.pdf

García, J.P.V., Quirós, C.T., Soria J. B., Pascual C.G. & Cordero, C. G. (2021). *Strategic communications as a key factor in countering hybrid threats*. Panel for the Future of Science and Technology (STOA), Scientific Foresight Unit of the Directorate-General for Parliamentary Research Services (EPRS).

Giannopoulos, G., Smith, H. & Theocharidou, M. (2021). *The Landscape of Hybrid Threats: A conceptual model*, EUR 30585EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305

Hansen, P., & Gill, M. (2021). *Strategic Communications Hybrid Threats Toolkit. Applying the principles of NATO Strategic Communications to understand and counter grey zone threats.* (B. Heap, Ed.). NATO StratCom COE. Retrieved October 20, 2025, from https://stratcomcoe.org/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf

Hallahan, K., Holtzhausen, D., van Ruler, B., Verčič, D. & Sriramesh, K. (2007) Defining Strategic Communication, *INTERNATIONAL JOURNAL OF STRATEGIC COMMUNICATION, 1:1, 3-35*, DOI: 10.1080/15531180701285244

Heier, T. (2023). Civic Communities Or Armed Forces As First Line Of Defence? In O. J. Borch & T. Heier (Eds.), *Preparing for Hybrid Threats to Security (1st ed., pp. 13–35).* Routledge. DOI: 10.4324/9781032617916-11

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [Retrieved September 20, 2025]

Holtzhausen, D. R., & Zerfass, A. (2013). Strategic communication—Pillars and perspectives on an alternate paradigm. *In K. Sriramesh, A. Zerfass, & J.-N. Kim (Eds.), Current Trends and Emerging Topics in Public Relations and Communication Management (pp. 283–302)*. New York, NY: Routledge.

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A. & Giannopoulos G. (2023). *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg, doi:10.2760/37899, JRC129019.

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs, 92*(1), 175–195. https://doi.org/10.1111/1468-2346.12509

Lucas, E. & Pomeranzev, P. (2016). *Winning the Information War: Techniques and counter-strategies to Russian propaganda in Central and Eastern Europe*, Center for European Policy Analysis, 2016.

Marocico, O., Mirodan, S., & Ings, R. (2025, September 21). *How Russian-funded fake news network aims to disrupt European election - BBC investigation*. BBC. Retrieved October 11, 2025, from https://www.bbc.com/news/articles/c4g5kl0n5d2o

Mazarr, M.J. (2015) *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. US Army War College Press. https://press.armywarcollege.edu/monographs/428

NATO StratCom COE [NATO Strategic Communications Centre of Excellence] (2019). Hybrid Threats. A Strategic Communications Perspective. https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79

OECD (2023). Good practice principles for public communication responses to mis- and disinformation, *OECD Public Governance Policy Papers*, No. 30, OECD Publishing, Paris, https://doi.org/10.1787/6d141b44-en.

Pamment, J., Nothhaft, H., & Fjällhed, A. (2018) *Countering Information Influence Activities: The State of the Art.* MSB. https://www.msb.se/RibData/Filer/pdf/28697.pdf

Pilati, F., & Venturini, T. (2025). The use of artificial intelligence in counter-disinformation: A world wide (web) mapping. *Front. Polit. Sci. 7:1517726.* doi: 10.3389/fpos.2025.1517726

Porumbescu, G., Moynihan, D., Anastasopoulos, J., & Olsen, A. L. (2022). When blame avoidance backfires: Responses to performance framing and outgroup scapegoating during the COVID-19 pandemic. *Governance, 36(3)*, 779–803. https://doi.org/10.1111/gove.12701

Rotaru, I. (2024). Comunicarea guvernamentală – despre vulnerabilități și posibile soluții [Governmental Communication – vulnerabilities and possible solutions] in *Dobrescu, P., Zeru, F. (editors) (2024) Comunicarea guvernamentală în România. O abordare strategică [Romanian Governmental Communication – a strategic approach]*, Tritonic, Bucharest.

Rietjens, S. (2020). A warning system for hybrid threats – is it possible? In *Hybrid CoE* (Strategic Analysis 22). Hybrid CoE. Retrieved October 26, 2025, from https://www.hybridcoe.fi/wp-content/uploads/2020/06/Strategic-Analysis_22_WarningSystem-1.pdf

Saar A. (2020). Can Government Public Communications Elicit Undue Trust? Exploring the Interaction between Symbols and Substantive Information in Communications, Journal of Public Administration Research and Theory, Volume 30, Issue 1, Pages 77–95, https://doi.org/10.1093/jopart/muz013

Simons, G. (2023). Western Hybrid Warfare: Crisis and Subversion in Regime Change. In Chifu, I. Simons, G. - *Rethinking Warfare in the 21st Century* (pp. 219–245). Cambridge University Press. https://doi.org/10.1017/9781009355247.008

U.S. Special Operations Command. (9 September 2015) The Gray Zone (White Paper). https://info.publicintelligence.net/USSOCOM-GrayZones.pdf