The necessity for a new NATO communication strategy in social media and the public sphere

By Vassilis Nanis

Over the past decade, profound shifts in the international security environment have coincided with an equally disruptive transformation of the information space. Russia's war of aggression against Ukraine, renewed great-power competition and the rise of hybrid warfare have unfolded in parallel with the expansion of high-speed internet, smartphones and social media platforms that connect billions of users in real time.

In this networked environment, the traditional information hierarchy – with journalists and major media organisations acting as agenda setters and gatekeepers – has been significantly weakened. Today, any individual with a mobile phone can produce and disseminate "news" to a potentially global audience, often without editorial control, professional ethics or clear accountability. This shift has empowered citizens, but it has also created unprecedented opportunities for state and non-state actors to manipulate information, spread disinformation and polarise societies.

For NATO, an alliance whose legitimacy ultimately depends on public trust and democratic consent, these developments pose a strategic challenge. The Alliance's existing communication frameworks, designed for a more linear and predictable media environment, are increasingly strained by an information ecosystem that is fast-moving, fragmented and vulnerable to manipulation.

This paper argues that NATO urgently requires a new communication strategy tailored to the dynamics of contemporary social media and the broader public sphere. The analysis proceeds in four parts: a theoretical framework for understanding communication in a hybrid security environment; an overview of NATO's existing communication architecture; an examination of the challenges the Alliance faces in today's digital ecosystem; and a concluding section outlining principles for a renewed communication strategy.

Theoretical Framework

1. Strategic Communication

NATO defines Strategic Communications as:

"the coordinated and appropriate use of NATO communications activities and capabilities—Public Diplomacy, Public Affairs, military Public Affairs, Information Operations, and Psychological Operations—as appropriate, in support of Alliance

policies, operations and activities"
(NATO Military Committee Policy MC 0628/1, 2017)

This definition highlights two fundamental principles: **coherence** (all communication efforts must align with NATO's actions and policies) and **integration** (communication is not an afterthought but a strategic tool embedded across political and military structures).

However, this doctrine was formulated before the rise of TikTok, algorithmic recommendation systems, generative AI and large-scale platform manipulation. The assumption that NATO can shape perceptions by controlling its outputs is increasingly untenable in a horizontal, participatory information environment.

2. Public Diplomacy and Credibility

NATO's Public Diplomacy Division (PDD) emphasises that communication must build trust and mutual understanding. As stated on NATO's official website:

"Our aim is to explain the Alliance's role and policies to publics worldwide, to foster dialogue and to strengthen support for the values the Alliance upholds."
(NATO Public Diplomacy Division, 2022)

Public diplomacy research shows that **credibility**, not message volume, is the decisive factor influencing persuasion—especially among young audiences. Moysaki's 2022 study on Greek Generation Z found that NATO's credibility determines the effectiveness of its messaging more strongly than argument quality, supporting the **Elaboration Likelihood Model (ELM)**: audiences under cognitive load rely on **peripheral cues**, such as messenger trustworthiness, platform familiarity and emotional resonance.

Thus, NATO must move beyond institutional monologues and incorporate **trusted intermediaries** (experts, influencers, local voices) into its communication ecosystem.

3. Hybrid Warfare and the Information Battlespace

Hybrid warfare blends military and non-military tools, prominently including information manipulation. The NATO StratCom COE stresses that:

"Hostile actors exploit the vulnerabilities of the open information environment, spreading disinformation, amplifying polarisation and eroding public trust."
(NATO StratCom COE, "Social Media Manipulation 2022–2023")

Unlike traditional propaganda, hybrid information threats are **multiplatform, asynchronous, deniable and adaptive**. They exploit speed, anonymity and emotional triggers—areas where institutional actors like NATO are structurally disadvantaged.

4. The Networked Public Sphere

As scholars such as Castells and Boyd argue, the public sphere has evolved into a **networked** environment characterised by decentralised participation, fluid boundaries and algorithmic filtering. While this expands opportunities for engagement, it also fragments audiences and privileges emotionally charged content.

Habermas' framework serves as a normative benchmark: contemporary debate systematically deviates from deliberative ideals due to platform logics that privilege speed, virality and outrage.

5. Mediatization

Mediatization theory posits that institutions increasingly adapt to the logic of media. For NATO, this means:

- responding at social-media speed
- crafting platform-specific narratives
- engaging emotionally, not only informationally

Yet the Alliance continues to operate partially within a traditional **broadcast logic**, which limits its competitiveness in a crowded and adversarial environment.

NATO's Current Communication Architecture

NATO's communication system has evolved significantly over the past two decades, becoming more structured, integrated and strategically oriented. However, despite these developments, the current architecture still reflects assumptions rooted in an earlier media ecosystem. Understanding this institutional framework is essential for analysing where the Alliance succeeds, where vulnerabilities emerge, and why a new communication strategy may be required for the digital public sphere.

1. Organisational Structure and Responsibilities

NATO's communication responsibilities are distributed across several bodies that operate in coordination but retain distinct mandates.

a. The Public Diplomacy Division (PDD)
The PDD, based at NATO Headquarters in Brussels, is the Alliance's primary civilian communication arm. It is responsible for:

- Public outreach and information campaigns
- Media relations (briefings, press conferences, fact sheets)
- Speechwriting and editorial oversight
- Communication with civil society, NGOs, academia and youth audiences
- Digital engagement on NATO's main platforms (website, social channels)

Its mission is to explain NATO's policies, actions and values to internal and external audiences, and to foster understanding and support among publics in member states and partner countries. While PDD has expanded its digital capabilities, its structure still resembles a **centralised corporate communications model**, suited to linear media flows rather than distributed, social-media-driven dynamics.

b. Press and Media Division within the NATO International Staff
This division manages the daily relationship with journalists, including accreditation, press materials and crisis communication. Its output remains essential for shaping mainstream media narratives, yet its impact on social media discourse is increasingly indirect.

c. Allied Command Operations (ACO) and Military Public Affairs
At SHAPE and across NATO's operational commands, **Military Public Affairs Officers (PAOs)** manage communication during missions, exercises and crises. Their work ensures operational transparency and supports situational awareness among domestic publics and international observers. However, military communication cultures tend to emphasise accuracy, caution and verification, often making them slower to respond than adversarial actors who exploit speed and ambiguity on social platforms.

d. Information Operations (Info Ops) and Psychological Operations (PSYOPS)
These functions, integrated within the military chain of command, aim to influence perceptions and behaviours of relevant audiences in support of operations. Although strictly regulated and distinct from public-facing communications, they form part of the broader **Strategic Communications mindset**, which requires synchronization of messages and actions across all domains.

e. NATO Strategic Communications Centre of Excellence (StratCom COE)
Based in Riga, the StratCom COE is not part of NATO's command structure but is accredited by NATO and funded by member states. It operates as a research and capacity-building hub, providing:

- Analysis of disinformation campaigns
- Studies on algorithmic manipulation, deepfakes and synthetic media
- Training for member-state officials
- Assessments of social media platform vulnerabilities

The COE has been instrumental in highlighting how legacy communication models struggle in a high-speed, adversarial information environment.

Together, these entities form a **complex but relatively compartmentalised communication architecture**. While coordination mechanisms exist, NATO communication sometimes remains siloed, with different strands (public diplomacy, military PA, Info Ops) operating at different speeds, with different audiences and different risk tolerances.

2. Doctrinal Foundations

NATO's contemporary communication doctrine is anchored in two key documents:

a. NATO Strategic Communications Policy (2009)

This foundational document established the need for a coherent, cross-domain communication mindset. It reflected an early recognition that messaging must be aligned with actions, and that communication should support political and military objectives. However, it was drafted before today's algorithmic and AI-driven information ecosystem emerged.

b. Military Committee Policy MC 0628 (2017)

This document formalised StratCom within NATO's military structures. It placed Public Affairs, Info Ops and PSYOPS under the conceptual umbrella of Strategic Communications, emphasising coherence, planning and the shaping of the information environment. Yet, its underlying assumptions—hierarchical information flows, relatively stable gatekeeping institutions, predictable media cycles—no longer hold in today's environment.

Additionally, NATO's more recent articulation of **"countering information threats"** acknowledges that communication challenges now include disinformation, manipulation, impersonation, deepfakes, bot networks and platform vulnerabilities. This shift shows evolving awareness but has not yet been matched by a full strategic overhaul.

3. Tools and Instruments: From Traditional Outreach to Digital Diplomacy

NATO uses a variety of tools to communicate with audiences:

- **Digital Platforms**: NATO's website, Twitter/X, Facebook, Instagram, LinkedIn, YouTube, and recently TikTok serve as primary channels for information dissemination and engagement.
- **#WeAreNATO Campaign**: Launched in 2017, this was NATO's flagship public diplomacy campaign, aimed particularly at young people, women and communities with low awareness of NATO's role. It provided templates for member states to adapt locally. While successful in visibility, its top-down structure and limited adaptability to rapidly changing online trends showed the limitations of centralisation.
- **Crisis Communication Mechanisms**: NATO maintains rapid-reaction communication protocols during crises, including joint statements, coordinated social media messaging and briefings. However, these mechanisms often prioritise accuracy over velocity, creating a temporal disadvantage against fast-moving disinformation.

- **Partner Engagement**: NATO increasingly assists partner countries in strengthening their own communication capacities, especially in Eastern Europe and the Western Balkans, where vulnerability to influence operations is high.

4. Strengths and Limitations of the Current Architecture

The Alliance's communication system benefits from:

- Strong institutional legitimacy
- Professionalised public diplomacy and PA structures
- High-quality research through the StratCom COE
- Increasing coordination among members

However, limitations persist:

- **Structural centralisation** slows adaptation to platform-specific trends
- **Fragmentation** between military and civilian communication strands
- **Cultural caution** reduces response speed compared to adversaries
- **Lack of distributed networks** of messengers (influencers, journalists, local actors)
- **Outdated assumptions** about gatekeeping and audience behaviour

These limitations directly impact NATO's ability to operate effectively in an information environment defined by speed, virality, fragmentation and manipulation. As the next section will show, the challenges of today's social media ecosystem further expose why the existing architecture needs transformation.

5. Recent Restructuring of NATO's Public Diplomacy Division (2025)

Since the submission of this paper, NATO's public diplomacy and communication structures have entered a new phase of institutional reorganisation. In early 2025, under the leadership of Secretary General Mark Rutte, the Alliance initiated a significant restructuring of its Public Diplomacy Division (PDD), framed as part of a broader effort to streamline internal processes, optimise resources and enhance institutional efficiency.

Available information indicates that the restructuring involves a reduction in the size of the PDD, the reallocation or discontinuation of certain outreach and engagement activities, and the integration of press and spokesperson functions more directly under the authority of the Secretary General. In parallel, funding for some externally oriented public diplomacy projects and partnerships has reportedly been curtailed, while personnel structures are being adjusted to reduce turnover and administrative overhead.

These reforms are taking place within a broader political context marked by heightened pressure on NATO to demonstrate efficiency, fiscal discipline and focus on core defence priorities. They also reflect an effort to reassure key Allies—most notably the United States—that the Alliance is responsive to concerns regarding bureaucratic expansion and resource allocation, particularly at a time of renewed uncertainty in the transatlantic political environment.

From a strategic communication perspective, however, the restructuring raises important questions. While centralising press functions may enhance message discipline and political control, the downsizing of public diplomacy capacity risks weakening NATO's ability to engage proactively with non-elite audiences, civil society actors and younger publics. These audiences are precisely those most exposed to disinformation, algorithmic amplification and influence operations within social media ecosystems.

Rather than undermining the arguments advanced in this paper, the 2025 restructuring reinforces their urgency. At a moment when the information environment is becoming more fragmented, emotionally driven and technologically complex, reductions in communication capacity increase the importance of adopting more agile, networked and platform-sensitive strategies. The challenge for NATO is therefore not simply institutional efficiency, but ensuring that organisational reform does not translate into diminished narrative resilience or reduced ability to compete in the information space.

Challenges in the Contemporary Information Environment

At the same time, the contemporary information environment poses structural, technological and behavioural challenges that expose vulnerabilities in NATO's communication posture. These challenges are multidimensional and interconnected, forming an ecosystem where malign actors can operate at scale while institutional communicators struggle to maintain visibility, trust and narrative coherence.

1. Speed, Virality, and Asymmetry

Information now travels at unprecedented speed. Early narratives often dominate public perception, even if later proven false. As the NATO StratCom COE notes:

"In the first hours of a crisis, deceptive narratives can become dominant before official actors respond."
(StratCom COE, 2024)

This creates a fundamental **asymmetry**:

- Disinformation can be produced and disseminated instantly.
- Accurate information requires verification, coordination and political clearance.

NATO's institutional communication processes — designed for accuracy, stability and coherence — often cannot match this velocity. The result is a "first-mover disadvantage" in the narrative space.

2. Algorithmic Amplification and the Platform Logic

Social media platforms optimise for engagement, not veracity. Algorithmic curation reinforces existing biases and promotes:

- emotionally charged content
- conspiratorial narratives
- polarising frames
- sensationalism

NATO's communications, however, are often technical, cautious and institutional in tone — precisely the kind of content algorithms deprioritise. This mismatch creates structural invisibility: even high-quality messages fail to gain traction.

Moreover, platform architecture encourages fragmentation into "micro-publics" where different audiences receive radically different narratives. This challenges NATO's ability to convey cohesive messages across its 32 member states.

3. Deepfakes, AI-Generated Content, and Synthetic Media

The emergence of deepfakes and synthetic media introduces epistemic instability. The NATO Emerging Security Challenges Division warns:

"Deepfakes have the potential to erode trust and disrupt democratic processes." *(NATO ESCD, 2023)*

AI allows malign actors to:

- impersonate NATO officials
- fabricate images or videos of NATO troops
- simulate military incidents
- create manipulated statements attributed to Allied leaders

The speed of circulation makes it difficult for NATO to debunk such content before it becomes entrenched in online discourse. Verification mechanisms, traditionally slow and centralised, are insufficient in an era requiring rapid, automated response.

4. Coordinated Inauthentic Behaviour and Bot Networks

Hostile state and non-state actors deploy automated accounts to amplify narratives. According to a StratCom COE experiment:

"Major platforms continue to be permeable to manipulation, despite repeated efforts to detect coordinated inauthentic behaviour."
(StratCom COE, "Social Media Manipulation 2022–2023")

These networks can:

- flood NATO hashtags with counter-narratives
- fabricate the impression of public opposition
- derail conversations with hostile messaging
- distract audiences during crises through narrative saturation

This creates an environment where NATO must compete not only with genuine public opinion but also with artificially manufactured perceptions.

5. Declining Trust and Institutional Fatigue

The erosion of trust in institutions — documented across multiple Eurobarometer surveys — affects how NATO's messages are received. Demographic trends show younger audiences expressing lower levels of institutional trust and relying more on peer networks and influencers for information.

This aligns with the findings of Moysaki (2022):

- NATO's credibility is the strongest predictor of message acceptance among Greek Gen Z.
- The messenger matters more than the message.

Thus, even accurate NATO communication can be dismissed if perceived as institutional propaganda.

6. Information Pollution, Cognitive Overload, and Attention Scarcity

The abundance of information creates **cognitive overload**, reducing the capacity of audiences to evaluate content critically. In such contexts, as the ELM explains, individuals rely on peripheral cues:

- aesthetics
- relatability
- emotional tone
- messenger identity

This dynamic disadvantages fact-based institutional communication and advantages emotionally resonant disinformation.

7. The Fragmentation of the Public Sphere

The networked public sphere is not a single arena but a constellation of micro-environments — TikTok teens, Twitter foreign-policy elites, Facebook boomers, Instagram influencers, Telegram channels. Each community operates with different norms, aesthetics and attention patterns.

NATO must therefore engage in **segmented communication**, but its centralised structure makes platform-specific targeting difficult.

8. Hybrid Threats and Information Laundering

Hybrid actors employ sophisticated techniques to obscure their involvement. The StratCom COE describes "information laundering" as:

"a process in which illegitimate or false narratives are circulated through a chain of intermediaries before entering mainstream discourse."
(StratCom COE, 2021)

This makes attribution difficult and undermines NATO's ability to counter narratives without appearing politically biased.

Elements of a New NATO Communication Strategy

A renewed NATO communication strategy must adapt to the realities outlined above. It must be faster, more decentralised, more data-driven, more platform-specific and more resilient. The following principles offer a comprehensive framework.

1. Adopt a Networked Communication Model

NATO should transition from a hierarchical communication structure to a **networked model**. This involves:

- empowering national communication teams
- collaborating with influencers and content creators
- engaging civil society organisations

- developing youth ambassador programmes
- integrating local voices in partner countries

As public diplomacy research shows, *peer-to-peer communication is far more persuasive than top-down messaging*.

2. Establish Rapid Reaction Narrative Units

NATO needs “communication crisis cells” capable of:

- issuing statements within minutes
- publishing visual situation updates
- countering disinformation as it emerges
- coordinating rapid messaging among Allies

This does not compromise accuracy — it brings accuracy to speed.

3. Build an Alliance-Wide Social Listening Architecture

NATO must invest in AI-driven monitoring tools to detect:

- narrative shifts
- bot activity
- deepfake dissemination
- emerging disinformation clusters
- platform-specific sentiment

Such systems should feed into daily briefings at NATO HQ, SHAPE and national communication bodies.

4. Platform-Specific Communication Strategies

NATO must adopt communication tailored to each platform’s logic:

a. TikTok and Reels

- 15–30 second vertical videos
- emotive storytelling
- on-the-ground footage

b. Instagram

- strong visuals
- infographics
- behind-the-scenes content

c. YouTube

- explainers
- mini-documentaries
- interviews with NATO soldiers

d. Twitter/X

- rapid updates during crises
- expert commentary
- media briefings

Failure to adapt leads to invisibility.

5. Build Credibility Through Transparency and Authenticity

NATO should:

- show authentic content from missions
- use real voices of soldiers, medics, humanitarian experts
- publish behind-the-scenes footage
- address mistakes openly rather than defensively

Transparency fosters trust.

6. Strengthen Cooperation with Tech Platforms

NATO must:

- establish dedicated liaison teams with major platforms
- improve rapid reporting channels for deepfakes
- co-develop tools for detecting coordinated inauthentic behavior
- participate in transparency initiatives

This partnership-based model is essential for resilience.

7. Integrate Ethical AI into Communication Workflows

AI can support NATO communication by:

- automating routine messaging
- translating content instantly
- generating multimedia at scale
- analysing audience behaviour
- detecting manipulated media

All use must comply with NATO's values, transparency principles and human oversight.

8. Build Narrative Resilience in Member Societies

NATO should support member states with:

- media literacy programmes
- critical thinking workshops
- digital citizenship initiatives
- school-level educational content

Resilience is a long-term investment in societal security.

9. Integrate Strategic Communication into Planning and Operations

StratCom must be present from the planning phase of every operation. Military actions and political decisions must align with narrative objectives. As MC 0628/1 states:

"Words and actions must be mutually reinforcing."

This requires deeper integration between political, military and communication structures.

Conclusion

The transformation of the information environment has redefined the strategic landscape in which NATO operates. The collapse of traditional gatekeeping, the rise of algorithmic amplification, the scale of hostile information manipulation and the speed at which narratives circulate require a fundamentally new approach to communication. NATO's current architecture—solid but centralised, professional but slow, coherent but not adequately adapted to platform logic—cannot meet the demands of today's networked public sphere. A renewed communication strategy

must be agile, decentralised, data-driven, ethically grounded and deeply integrated into NATO's broader strategic posture.

Communication is no longer merely an accessory to security; it is one of its core domains. For NATO to maintain legitimacy, effectiveness and deterrence in the coming decade, it must recognise that the battle for public understanding is inseparable from the defence of the Euro-Atlantic area.

Bibliography

NATO Documents

NATO. *Military Committee Policy MC 0628/1: NATO Military Policy on Strategic Communications.* 2017.
NATO. "Public Diplomacy Division – What We Do." NATO Official Website, 2022.
NATO. "Countering Information Threats." Emerging Security Challenges Division, 2023.

NATO StratCom COE Reports

NATO Strategic Communications Centre of Excellence. *Social Media Manipulation 2022–2023.* Riga: NATO StratCom COE, 2023.
NATO Strategic Communications Centre of Excellence. *Social Media Manipulation 2024.* Riga: NATO StratCom COE, 2024.

Academic Works

Castells, Manuel. *Communication Power.* Oxford University Press, 2009.
boyd, danah. *It's Complicated: The Social Lives of Networked Teens.* Yale University Press, 2014.
Habermas, Jürgen. *The Structural Transformation of the Public Sphere.* MIT Press, 1991.
Moysaki, Anastasia. "Public Perceptions about NATO Brand – Greek Generation Z and Its Public Opinion." MA Thesis, 2022.

Additional Sources

European Commission. *Eurobarometer Surveys.* Brussels, various years.
NATO. *#WeAreNATO Campaign Overview.* Brussels: NATO PDD, 2017.