Communication

War in Social Media: Soft Systems Modelling of NATO Fracture Through Grey Zone Operations

Graham Wild *

Posted Date: 21 January 2026

doi: 10.20944/preprints202601.1500.v1

Keywords: communication; disinformation; Greenland; grey zone operations; hybrid wars; information warfare; NATO; propaganda; social media; war

 doi:10.20944/preprints202601.1500.v1

Communication

War in Social Media: Soft Systems Modelling of NATO Fracture Through Grey Zone Operations

Graham Wild

UNSW Canberra at the Australia Defence Force Academy; g.wild@adfa.edu.au; Tel.: +61 2 5114 5221

Abstract

Proposed is a soft systems model of how grey zone military and cyber operations interact with coupled traditional and social media to condition alliance instability. Focusing on the media-mediated translation of physical signaling and digital narratives, the model shows how recursive feedback can stabilize interpretations of ambiguous events without persuasion, coercion, or attribution. Considering Greenland as an illustrative case, the framework highlights how localized epistemic instability within a single member state can propagate across NATO through horizontally coupled policy–media networks. The analysis highlights alliance vulnerability driven by mediated salience and performative discourse rather than force, and identifies key interfaces requiring further interdisciplinary investigation.

Keywords: communication; disinformation; Greenland; grey zone operations; hybrid wars; information warfare; NATO; propaganda; social media; war

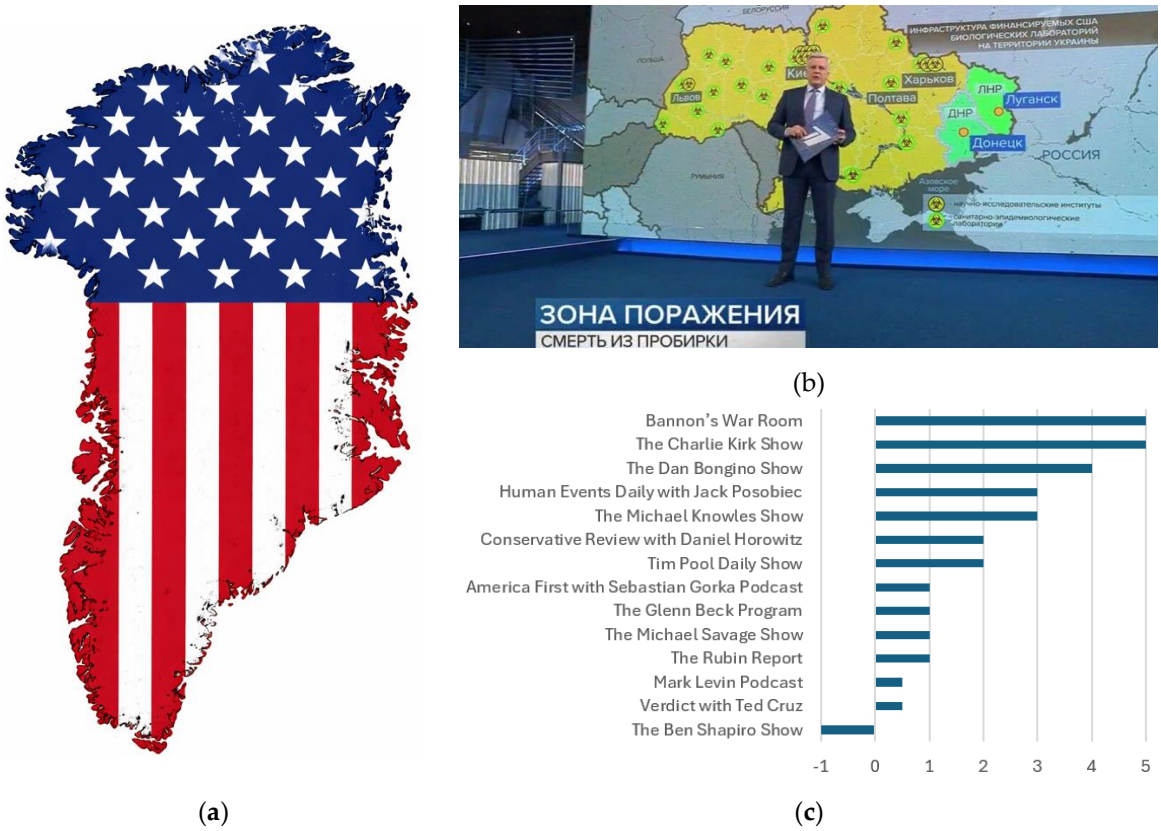
1. Introduction

Recent public discourse has increasingly framed the North Atlantic Treaty Organization (NATO) as fragile, internally divided, or approaching strategic rupture; the contemporary manifestation is the discussed US "acquisition" of Greenland. Such claims are no longer confined to fringe commentary but now appear mainstream, often in conjunction with discussions of grey zone competition, hybrid warfare, and great power rivalry [1,2]. An example of this is shown in recent social media posts (see Figure 1 a). Simultaneously, contemporary military activity and cyber influence operations rarely present themselves as discrete events. Instead, they unfold on the intensely coupled media landscape where physical actions, digital narratives, and public reaction are recursively intertwined.

Substantial progress has been made analyzing grey zone operations, information warfare, and media effects in conflict [2,3]. However, military signaling is analyzed separately from media dynamics, while social media influence is often examined without sustained attention to its interaction with observable military activity or alliance politics. Consider the misinformation campaign about US biolabs in the Ukraine [4,5], illustrated in Figure 1 (b) and (c). As a result, there remains a conceptual gap in understanding how grey zone operations can plausibly translate into alliance-level instability without overt conflict or formal coercion [1,6].

To address this gap, a soft systems model of alliance fracture grounded in the interaction between military operations, cyber influence, and coupled traditional and social media ecosystems is proposed. Rather than attributing intent or reconstructing specific campaigns, the model focuses on systemic vulnerability, showing how mediated feedback can destabilize individual alliance members and propagate uncertainty across a networked military alliance.

 doi:10.20944/preprints202601.1500.v1



(a) (b) (c)

Figure 1. Illustrative media artefacts; (a) symbolic territorial reframing through visual appropriation of Greenland by the United States, (b) Ukraine biolabs narrative broadcast [4], and (c) downstream amplification through Western podcast ecosystems of biolabs narrative [5].

2. Literature Review

Recent work on war, media, and conflict increasingly converges on the role of elite and institutional signaling within coupled media systems, rather than on persuasion or disinformation alone. Studies of executive communication and legacy media demonstrate how rapid agenda-setting and framing can stabilize interpretation under conditions of uncertainty, even when reporting remains largely factual [7]. This dynamic extends beyond national executives to supranational institutions, where coordinated platform-native discourse functions as a form of strategic signaling that foregrounds values, legality, and unity while avoiding operational specificity [8,9]. Media systems, in turn, act as legitimacy infrastructures, translating ambiguous events into institutionally actionable narratives, for example in the interaction between international legal bodies and early war reporting [10–12]. Together, this literature shows that traditional and social media are not sequential channels but mutually reinforcing sites through which elite narratives are normalized and rendered politically salient.

A second strand of research focuses on platform dynamics, amplification gates, and epistemic infrastructure. Here, social media are treated as constrained environments in which affordances are selectively realized under algorithmic governance, moderation regimes, and resource asymmetries [13]. Organizational and individual actors adopt systematically different strategies to achieve visibility, persistence, and mobilization, while optimization behavior often responds more to platform penalties than to evidentiary standards. Within this environment, fact-checking and verification operate as partial counter-forces that reintroduce epistemic friction but rarely arrest narrative circulation or salience escalation [14]. Empirical studies of wartime disinformation further show how narratives evolve temporally, shift focus from battlefield claims to alliance and legitimacy themes, and rely heavily on visual decontextualization across platforms [15]. Collectively, this work

 doi:10.20944/preprints202601.1500.v1

supports the view of media as a circulatory system in which credibility and importance are inferred from repetition and visibility rather than proof.

A third body of literature examines uptake, affect, and perception as conditioning environments rather than decision mechanisms. Audience-focused research highlights widespread mistrust, differentiated credibility gradients between media types, and demographic asymmetries in information uptake, even in the absence of persuasion or belief change [16,17]. At the same time, affective dynamics such as verbal aggression and outrage emerge as endogenous properties of social-media-mediated politics, functioning to contest legitimacy, reinforce identity boundaries, and escalate polarization without direct policy instruction [18]. Comparative studies of international broadcasting further show how emotional repertoires are systematically aligned with geopolitical interests, using fear, neutrality, or hope as tools of legitimacy construction rather than information delivery [19,20]. Taken together, this literature frames public sentiment as a mediated conditioning field that shapes political cost, legitimacy, and expectation, providing a plausible pathway through which local epistemic instability can propagate across alliance networks without overt coercion or attribution.

A fourth strand of the literature addresses computational sensing of affect, discourse, and behavioral proxies in wartime social media, treating platforms as large-scale observational instruments rather than persuasion channels [21]. Work on emotion classification demonstrates how war-related discourse on Twitter can be systematically mapped into structured emotional repertoires, revealing patterned distributions of fear, anger, solidarity, and anxiety that track phases of escalation and international attention rather than discrete events [22]. Complementary analyses of European interest groups show how organized actors inhabit X as networked discursive agents, using sentiment, framing, and coordination to condition visibility and legitimacy within transnational issue spaces, without necessarily targeting mass persuasion [23]. At a different observational scale, mobility analysis using geo-tagged Twitter data illustrates how war-related events generate indirect behavioral effects, such as altered travel patterns driven by sanctions, energy prices, and refugee flows, highlighting how mediated conflict produces secondary societal impacts that are legible through digital traces [24]. Finally, survey-level syntheses of social media analytics in the context of Russia–Ukraine cyber conflict situate these methods within a broader methodological landscape, emphasizing both the power and limits of NLP-based approaches for capturing narratives, coordination, and affect under adversarial and high-noise conditions [25]. Taken together, this literature supports the use of computational social media analysis as a diagnostic layer, capable of detecting shifts in emotion, discourse, and behavior that condition political salience and legitimacy, while reinforcing the need for interpretive restraint when translating such signals into claims about intent, causation, or strategic control.

3. Approach

An explicitly abductive and hypothetical approach was adopted. This exploratory work does not seek to attribute responsibility, reconstruct specific operations, or demonstrate causal pathways in an evidentiary sense [3,26]. Rather, it asks if, given contemporary military practice and media ecology, alliance fracture becomes a strategically plausible outcome without direct conflict. The goal is systemic exposure and not proof of execution.

The model is deliberately constrained. It focuses on adversary-side signaling through physical military operations (Trad-Ops) and cyber influence capacities (Cyber-Ops), and on the interaction of those with traditional [27], and social media [28]. Downstream processes such as elite psychology, internal policy deliberation, electoral behavior, and intelligence coordination are not modelled [29,30]. These elements are treated as black-boxed subsystems whose internal workings require further research beyond the present work.

Soft systems modelling is used because the phenomenon under consideration involves heterogeneous actors, feedback loops, and interpretive processes that resist linear or mechanistic

 doi:10.20944/preprints202601.1500.v1

representation [31,32]. The aim is not to optimize prediction, but to show the interactions through which media-mediated military signaling can influence alliance stability.

Figure 1 presents the proposed soft systems model. The figure should be read as a conceptual map of interactions and feedback loops, not as a linear sequence of actions or a claim of attribution. The following sections will discuss the elements of the model.

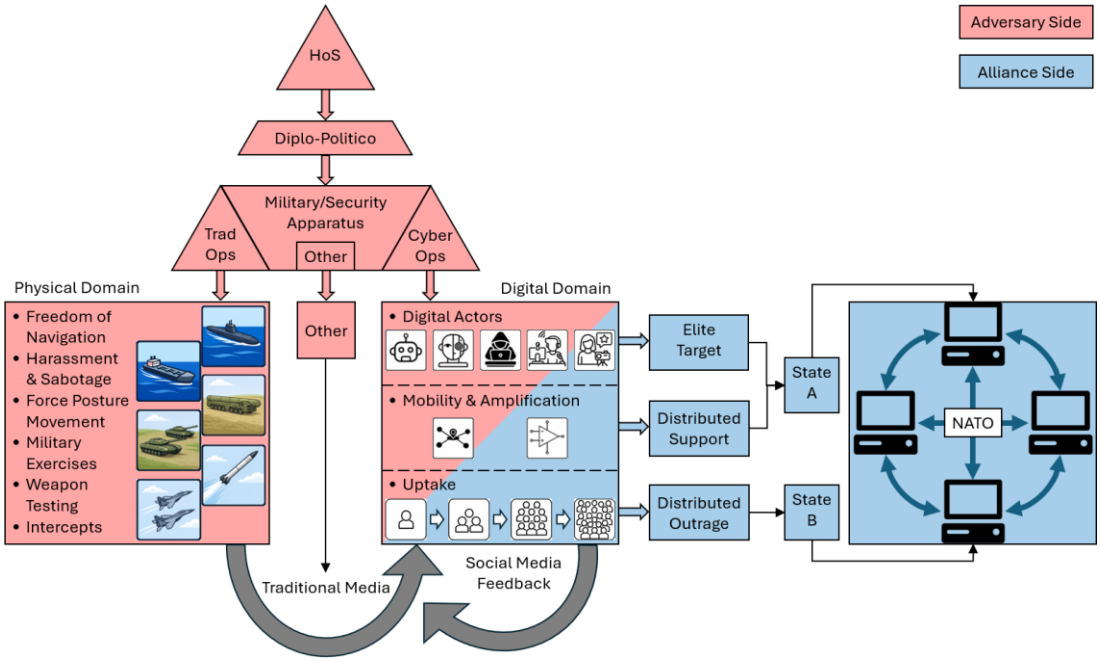


Figure 1. Soft systems model of grey zone operations, media coupling, and alliance instability.

4. Adversary-Initiation

Adversary behavior spans strategic, political, and military domains, each contributing to the production of meaning as much as to material effect [33,34]. At the strategic level, head-of-state (HoS) signaling likely sets broad boundaries rather than issuing instructions [35]. It establishes what kinds of risk appear tolerable and what kinds of action can be framed as reasonable. Political and diplomatic activity then does the interpretive work, converting intent into publicly legible narratives through speeches, formal statements, and multilateral performance [36]. This layer matters because it normalizes later military and cyber activity by embedding it within familiar claims of legality, necessity, or grievance, without ever needing to specify operational detail.

The military and security apparatus occupies a third layer, where strategic intent and political framing are converted into capability domains [37]. Rather than issuing direct instructions, this layer delineates the range of actions that are feasible, deniable, and communicatively effective [38]. Within the model, it is analytically useful to distinguish between Trad-Ops, Cyber-Ops, and "other", not because they are separate in practice, but because they interact with media systems in different ways.

Together, these layers constitute the adversary-side inputs to the broader system depicted in Figure 1. They supply the stimuli that enter coupled media environments as well as condition alliance dynamics.

4.1. Traditional Operations

Trad-Ops constitute the physical signaling domain within the model. Trad-Ops are defined as observable, materially instantiated military activities that are lawful, routine, and institutionally attributable, yet strategically ambiguous. Their relevance in grey zone dynamics lies not in coercion

 doi:10.20944/preprints202601.1500.v1

or escalation, but in their capacity to generate visible events that enter mediated environments as objects of interpretation.

This domain includes several distinct but related activities [39]:

- freedom of navigation movements assert access, transit rights, and jurisdictional contestation through routine passage in disputed or sensitive spaces;
- harassment and sabotage introduce friction, disruption, or damage while remaining below thresholds that would compel formal military response or attribution;
- force posture adjustments modify basing, readiness, or deployment configurations to signal capability, commitment, or flexibility without direct engagement;
- military exercises rehearse operations and interoperability in a manner that is visible, repeatable, and plausibly defensive;
- weapons testing demonstrates technological capability and credibility while remaining temporally and geographically bounded; and
- close encounters such as intercepts probe behavioral norms and thresholds through controlled proximity and interaction.

Trad-Ops are highly visible and routinely generate traditional media coverage [40]. Their significance lies not only in their material characteristics but in their ambiguity [33]. Such actions are observable, yet open to interpretation, allowing competing narratives to circulate regarding intent, escalation, and alliance credibility [41]. This ambiguity makes physical operations particularly effective as media-generating signals rather than as instruments of coercion.

4.2. Other

Between physical military operations and overt digital influence activities lies a set of institutional security functions that shape interpretation without acting directly on publics or adversaries. This domain, labelled "Other" in the model, consists of authoritative meaning production by the security state. These activities do not involve force movement, technical cyber operations, or audience engagement. Instead, they structure the epistemic conditions under which military activity is understood, debated, and normalized.

This domain includes several distinct but related functions:

- doctrinal and conceptual production defines what counts as realistic, responsible, or credible security thinking through strategy documents and official concepts;
- intelligence boundary management calibrates uncertainty through selective emphasis, declassification, or silence, using ambiguity as a resource rather than a failure;
- lawfare and normative preparation establishes legal and historical frames around sovereignty, treaties, and jurisdiction in advance of contestation;
- resource and industrial framing presents infrastructure, energy, and dependency issues as technical or economic facts while encoding security logics of scarcity and inevitability; and
- counterfactual and futures conditioning narrows perceived possibilities through war games, scenarios, and strategic foresight that circulate indirectly via expert communities.

Media engagement with this domain is indirect and asymmetric. Traditional media draws selectively on these materials as authoritative context, expert reference, or background framing, while social media re-circulates fragments detached from their institutional origins. The effect is not persuasion but plausibility conditioning, narratives resonate more strongly when they align with pre-existing doctrinal, legal, or strategic frames. In this way, the "Other" domain quietly stabilizes interpretation across both media environments without acting as a signaling channel in its own right.

4.3. Cyber Operations

Cyber-Ops function differently [42]. They are treated here as a capability domain that shapes the information environment rather than as a set of tactics [43]. Their primary role is to introduce, amplify, or stabilize narratives that resonate with existing political tensions, often operating

 doi:10.20944/preprints202601.1500.v1

alongside or in anticipation of physical signaling [44]. In the context of this model, their importance lies in how they interact with media ecosystems, rather than in any specific operational mechanism.

Cyber-Ops in this context can be defined to include [45–47]:

- disinformation operations deliberately seed false or misleading content in order to shape belief, trust, or perceived reality;
- misinformation amplification increases the visibility and reach of misleading claims regardless of their original source, often through coordinated networks;
- coordinated inauthentic behavior deploys networks of accounts that conceal coordination or identity to simulate organic consensus or grassroots activity;
- automation and computational propaganda use political bots and automated agents to manipulate visibility, ranking, and perceived popularity;
- cyborg operations combine human control with automation, producing accounts that shift between bot-like and human-like behavior over time;
- troll and persona management employs human-operated accounts to provoke, antagonize, distract, and polarize through identity performance and conflict generation; and
- hack-and-leak as cyber-enabled influence releases authentic but selectively obtained material through digital means in order to shape media narratives and political salience.

Section 6 below details the digital environment in which these cyber-ops are occurring. At a high level, cyber-enabled influence operations exploit the substitution of platform visibility cues for evidentiary evaluation under time pressure. Social media supplies apparent distributed endorsement through repetition and engagement metrics, while traditional media confers perceived legitimacy when it reports on online reaction, circulating claims, or leaks. This is why Russian influence activity around Ukraine is analytically legible as cyber-enabled narrative warfare, even when the specific technical mechanisms are left black-boxed.

5. Media

In contemporary conflict, military signaling does not enter public discourse through a single media channel. Trad-Ops are primarily interpreted through traditional media, which provides initial framing, authoritative narration, and perceived legitimacy through official sources, expert commentary, and visual documentation [48]. In contrast, social media functions as a distributed environment for amplification, reframing, and affective engagement, where narratives acquire salience, emotional intensity, and the appearance of widespread endorsement [49].

These two media domains are no longer sequential or hierarchically ordered [50]. Traditional media coverage of military activity is rapidly circulated, excerpted, and selectively reframed across social platforms, where it is embedded within ideological commentary, identity signaling, and partisan interpretation [51]. In turn, social media discourse is increasingly re-imported into traditional media reporting, framed as public reaction, online mobilization, or evidence of emerging political pressure [52]. This process collapses the distinction between reporting and reaction, producing a recursive feedback loop in which each validates and amplifies the other [53].

This coupled system has important consequences. It accelerates the stabilization of particular interpretations of inherently ambiguous Trad-Ops (harassment and sabotage, e.g. of undersea cables [54]). Once an interpretive frame circulates across both traditional and social media, it can appear self-evident or commonsensical, even in the absence of new empirical information [49,55]. The effect is a form of credibility laundering [56,57]. Narratives that would once be dismissed gain standing simply by being repeated often enough and in the right places. At that point, intensity replaces evidence, and visibility itself becomes a signal of importance.

In the context of Cyber-Ops, this coupled system transforms military activity into a continuous narrative environment rather than a series of discrete events. The strategic effect is not persuasion in the narrow sense, but the conditioning of interpretive space within which alliance commitments,

 doi:10.20944/preprints202601.1500.v1

escalation risks, and political costs are assessed. As depicted in Figure 1, this coupled media system is a significant vector through which adversary-side signaling enters broader alliance dynamics.

6. Digital Environment

The digital environment is modelled here as a systemic space in which narratives are produced, mobilized, and transformed [58]. Its analytical value is in what it does to meaning, rather than in the specific technologies through which it operates [58,59]. For this reason, the model abstracts the digital domain into three interacting layers: digital actor, mobility and amplification, and uptake [60].

The first layer is a heterogeneous digital actor ecology [61,62]. This ecology spans fully automated agents (bots), semi-automated or "cyborg" accounts, coordinated human operators, ideological volunteers, and apparently authentic domestic commentators [62,63]. From a systems perspective, plausible deniability and narrative resilience arise precisely from there blending, as similar claims appear to circulate organically across actor types without clear provenance [61,63]. The effect is not to convince through argument, but to normalize through repetition across diverse voices [58,60].

The second layer concerns how narratives move [60]. They do not simply diffuse outward, they climb. Claims that begin in low-credibility or overtly partisan spaces can work their way upward through repetition by more visible or socially trusted actors [60]. This can be through influencers or commentators, as well as media-adjacent figures who repackage the same material in other forms [60]. The mechanisms are familiar, algorithmic ranking, engagement incentives, reposting by high-visibility accounts, paid promotion, and cross-platform circulation [59,64], but their effect is cumulative rather than directional. Salience builds even when nothing new is added, and importance is inferred from repetition rather than coordination or intent [58,60].

The third layer captures uptake pathways [58]. Digital narratives are taken up in at least two analytically distinct ways [58,62]. Individual uptake occurs when high-access or elite-adjacent actors internalize and repeat narratives within policy-relevant networks. Mass uptake occurs when narratives achieve distributed resonance, generating alignment, outrage, or polarization at scale [58,64]. These pathways are treated separately because they condition political outcomes through different mechanisms [58].

Within the broader system shown in Figure 1, the digital domain functions as a key interface through which cyber influence and mediated physical signaling exert pressure on alliance stability.

7. Political Salience

Digital uptake does not flip policy switches. What it does instead is narrower and more consequential, it changes what feels politically live [50,65]. Certain positions begin to look costly, others defensible, and some suddenly risky to ignore [58,66]. This shift in salience matters precisely because it operates without persuasion or coercion, altering the conditions under which decisions are taken rather than the decisions themselves [65,67].

Individual uptake by high-access or elite-adjacent actors alters internal discourse by reducing epistemic friction [50,66]. Narratives repeated within policy-relevant networks acquire standing through proximity rather than evidence, becoming available as "reasonable" frames for discussion [66]. This effect is amplified when such actors are themselves embedded within digital media production, collapsing the distinction between uptake and dissemination [50,52].

Mass uptake works through a different mechanism [58,68]. Widespread resonance does not tell governments what to do, but it does change what they feel they can get away with [52,65]. When certain narratives dominate the media environment, they create expectations about support, backlash, or controversy that decision-makers cannot ignore [65,67]. Traditional and social media matter here less because they transmit opinion, and more because they signal, loudly and repeatedly, what is being treated as normal, outrageous, or politically dangerous [50,52].

 doi:10.20944/preprints202601.1500.v1

The model assumes political salience is an intermediate conditioning environment. It is the space in which beliefs and reactions are transformed into constraints on rhetoric and action. While the internal mechanisms of this transformation vary across political systems and require specialist investigation, its systemic role is to couple mediated uptake to policy-relevant signaling. As depicted in Figure 1, this conditioning layer enables narratives generated through grey zone operations to exert pressure on alliance dynamics without direct intervention

8. NATO Network

Within this model, NATO is treated as a network of national policy–media nodes linked through formal commitments and continuous signaling. Each member state combines military obligations, political leadership, media ecosystems, and public accountability in distinct ways, producing asymmetries in how pressure is absorbed and transmitted [69,70]. Alliance cohesion therefore depends not only on shared doctrine or capability, but on the stability of these national nodes under mediated stress [70,71].

Horizontal signaling between member states does most of the real work in alliance politics [72]. Statements, policy cues, and media narratives that originate in one national context are quickly read elsewhere as signals of resolve, hesitation, or internal division [71,72]. This does not depend on formal disagreement or treaty violation. In practice, quite small shifts in rhetoric, conditional phrasing, or strategic ambiguity inside a single node are enough to introduce uncertainty that others feel obliged to react to [69].

Alliance fracture, when it occurs, is rarely dramatic [70]; it tends not to arrive as sudden collapse or coordinated withdrawal, but as a gradual erosion of confidence driven by these accumulating signals. It emerges more quietly, when one or more nodes become epistemically unstable and mediated narratives begin to crowd out established expectations [70,71]. Once that happens, the character of alliance signaling changes, even though material capabilities and formal commitments remain exactly the same [72].

In this horizontally coupled network the relevant failure mode is local and contingent, but its effects are distributed. Mediated instability within a single member state can therefore condition alliance-wide dynamics without requiring overt conflict or explicit policy reversal.

9. Implications

The model presented has several implications for the study of contemporary conflict and alliance stability. First, it proposes that military and media dynamics are analytically inseparable. Trad-Ops, Cyber-Ops, and media circulation jointly constitute a signaling environment in which strategic effects emerge through interpretation rather than force [48,50]. Analyses that isolate one element risk overlooking the mechanisms through which pressure is exerted.

Second, the model shows the need to move beyond narrow conceptions of influence that focus on persuasion or deception [65]. The effects qualitatively modelled here arise from salience conditioning, legitimacy formation, and feedback-driven normalization, processes that operate even when audiences are skeptical or ideologically opposed. This has relevance for alliance politics, where ambiguity and expectation management play a central role.

The most serious implication is if elite targets exist and can be targeted. Such a “susceptible mediator”, adjacent to an authentic domestic commentator, supported by perceived distributed support from likes and shares, and with direct political influence, would make such grey zone attack vectors strategically irresistible. In fact, if the literal signaling was to invade a NATO ally, destroying the alliance, it would be strategically irresponsible not to try the grey zone attack.

Future work is needed on the interface between physical military activity and media framing, on cross-platform circulation and credibility laundering [56,57,73], and on elite-native digital media production as a first-order political phenomenon [74–76]. Other military/security activities around espionage and overt disinformation also need to be investigated and expanded on (the “other” vector

 doi:10.20944/preprints202601.1500.v1

in Figure 1). Equally important are studies of how mediated narratives are converted into internal policy signals within different national contexts. By identifying these interfaces without attempting to exhaust them, the present contribution aims to provide a structured starting point for interdisciplinary investigation into media-mediated alliance vulnerability.

10. Conclusions

The contemporary case of Greenland illustrates how alliance vulnerability can emerge without escalation, coercion, or overt conflict with an adversary. As an object of strategic interest, Greenland sits at the intersection of military posture, sovereignty, and alliance obligation, making it especially susceptible to mediated reframing. Physical signaling in the Arctic, coupled with cyber influence and recursive media feedback, can transform a geographically specific issue into a narrative test of alliance resolve. In this sense, Greenland is not exceptional but exemplary, showing how grey zone operations could easily exploit media coupling to condition alliance stability. Understanding this dynamic is essential if NATO is to recognize and mitigate fracture driven not by force, but by farce.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Jordan, J. International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict. *Journal of Strategic Security* **2020**, *14*, 1-24, doi:10.5038/1944-0472.14.1.1836.
2. Dobias, P.; Christensen, K. The 'Grey Zone' and Hybrid Activities. *Connections: The Quarterly Journal* **2022**, *21*, 41-54, doi:10.11610/Connections.21.2.03.
3. Cormac, R.; Aldrich, R.J. Grey is the new black: covert action and implausible deniability. *International Affairs* **2018**, *94*, 477-494, doi:10.1093/ia/iiy067.
4. Shelest, H.; Parachini, J.V. Why Does Russia Disinform About Biological Weapons? *Ukraine Analytica* **2023**, *1*, 3-17, https://ukraine-analytica.org/wp-content/uploads/Shelest3.pdf.
5. Brandt, J.; Wirtschafter, V.; Danaditya, A. Popular Podcasters Spread Russian Disinformation about Ukraine Biolabs. *Brookings TechStream* **2022**, *23*, https://www.brookings.edu/articles/popular-podcasters-spread-russian-disinformation-about-ukraine-biolabs/.
6. Mälksoo, M. A ritual approach to deterrence: I am, therefore I deter. *European Journal of International Relations* **2020**, *27*, 53-78, doi:10.1177/1354066120966039.
7. Hyzen, A.; Van den Bulck, H. "Putin's War of Choice": U.S. Propaganda and the Russia–Ukraine Invasion. *Journalism and Media* **2024**, *5*, 233-254, doi:10.3390/journalmedia5010016.
8. Ruiz-Incertis, R.; Tuñón-Navarro, J. European Institutional Discourse Concerning the Russian Invasion of Ukraine on the Social Network X. *Journalism and Media* **2024**, *5*, 1646-1683, doi:10.3390/journalmedia5040102.
9. Ruiz-Incertis, R.; Tuñón-Navarro, J. EU Digital Communication in Times of Hybrid Warfare: The Case of Russia and Ukraine on X. *Information* **2025**, *16*, 825, doi:10.3390/info16100825.
10. Selvarajah, S.; Fiorito, L. Media, Public Opinion, and the ICC in the Russia–Ukraine War. *Journalism and Media* **2023**, *4*, 760-789, doi:10.3390/journalmedia4030048.
11. Pallarés-Renau, M.; Miquel-Segarra, S.; López-Font, L. Red Cross Presence and Prominence in Spanish Headlines during the First 100 Days of War in Ukraine. *Social Sciences* **2023**, *12*, 368, doi:10.3390/socsci12070368.

12. Rožukalne, A.; Kažoka, A.; Siliņa, L. "Are Journalists Traitors of the State, Really?"—Self-Censorship Development during the Russian–Ukrainian War: The Case of Latvian PSM. *Social Sciences* **2024**, *13*, 350, doi:10.3390/socsci13070350.
13. Ronzhyn, A.; Batlle Rubio, A.; Cardenal, A.S. Affordances of Wartime Collective Action on Facebook. *Journalism and Media* **2025**, *6*, 194, doi:10.3390/journalmedia6040194.
14. Morais, R.; Piñeiro-Naval, V.; Blanco-Herrero, D. Beyond Information Warfare: Exploring Fact-Checking Research About the Russia–Ukraine War. *Journalism and Media* **2025**, *6*, 48, doi:10.3390/journalmedia6020048.
15. Sánchez-del-Vas, R.; Tuñón-Navarro, J. Beyond the Battlefield: A Cross-European Study of Wartime Disinformation. *Journalism and Media* **2025**, *6*, 115, doi:10.3390/journalmedia6030115.
16. Skarpa, P.E.; Simoglou, K.B.; Garoufallou, E. Russo-Ukrainian War and Trust or Mistrust in Information: A Snapshot of Individuals' Perceptions in Greece. *Journalism and Media* **2023**, *4*, 835-852, doi:10.3390/journalmedia4030052.
17. Melotti, G.; Villano, P.; Pivetti, M. Social Representations of the War in Italy during the Russia/Ukraine Conflict. *Social Sciences* **2024**, *13*, 545, doi:10.3390/socsci13100545.
18. Domalewska, D. Online Verbal Aggression on Social Media During Times of Political Turmoil: Discursive Patterns from Poland's 2020 Protests and Election. *Journalism and Media* **2025**, *6*, 146, doi:10.3390/journalmedia6030146.
19. Qiu, X.; Yu, W.; Huang, Y.; Yang, J. Emotional Geopolitics of War: Disparities in Russia–Ukraine War Coverage Between CGTN and VOA. *Journalism and Media* **2025**, *6*, 208, doi:10.3390/journalmedia6040208.
20. Hajek, A.; Kretzler, B.; König, H.-H. Social Media Addiction and Fear of War in Germany. *Psychiatry International* **2022**, *3*, 313-319, doi:10.3390/psychiatryint3040025.
21. Sufi, F. Novel Application of Open-Source Cyber Intelligence. *Electronics* **2023**, *12*, 3610, doi:10.3390/electronics12173610.
22. Vyas, P.; Vyas, G.; Dhiman, G. RUemo—The Classification Framework for Russia-Ukraine War-Related Societal Emotions on Twitter through Machine Learning. *Algorithms* **2023**, *16*, 69, doi:10.3390/a16020069.
23. Gorostiza-Cerviño, A.; Serna-Ortega, Á.; Moreno-Cabanillas, A.; Almansa-Martínez, A.; Castillo-Esparcia, A. Examining the Roles, Sentiments, and Discourse of European Interest Groups in the Ukrainian War through X (Twitter). *Information* **2024**, *15*, 422, doi:10.3390/info15070422.
24. Shu, Y.; Chen, X.; Di, X. Mobility Pattern Analysis during Russia–Ukraine War Using Twitter Location Data. *Information* **2024**, *15*, 76, doi:10.3390/info15020076.
25. Sufi, F. Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges. *Information* **2023**, *14*, 485, doi:10.3390/info14090485.
26. Skopik, F.; Pahi, T. Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity* **2020**, *3*, 8, doi:10.1186/s42400-020-00048-4.
27. Rushing, B. Analysis of Media Influence on Military Decision-Making. In Proceedings of the International Conference on Cyber Warfare and Security, Johannesburg, South Africa, 2024; pp. 308-316. Available online: https://www.academia.edu/download/122060634/1918.pdf.
28. Makhortykh, M.; Sydorova, M. Social media and visual framing of the conflict in Eastern Ukraine. *Media, War & Conflict* **2017**, *10*, 359-381, doi:10.1177/1750635217702539.
29. Joseph, M.F.; Poznansky, M. Media technology, covert action, and the politics of exposure. *Journal of Peace Research* **2017**, *55*, 320-335, doi:10.1177/0022343317731508.
30. Mustafa, H.; Luczak-Roesch, M.; Johnstone, D. Conceptualizing the evolving nature of computational propaganda: a systematic literature review. *Annals of the International Communication Association* **2025**, *49*, 45-60, doi:10.1093/anncom/wlaf001.
31. Wilson, B. Soft systems methodology: Conceptual model building and its contribution; Wiley: Chichester, UK, 2001.
32. Nadolski, M.; Fairbanks, J. Complex systems analysis of hybrid warfare. *Procedia Computer Science* **2019**, *153*, 210-217, doi:10.1016/j.procs.2019.05.072.
33. Glaser, C.L. Political Consequences of Military Strategy: Expanding and Refining the Spiral and Deterrence Models. *World Politics* **1992**, *44*, 497-538, doi:10.2307/2010486.

 doi:10.20944/preprints202601.1500.v1

34. George, A. The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries. *Comparative Strategy* **2003**, *22*, 463-487, doi:10.1080/01495930390256527.
35. Altman, D. Advancing without Attacking: The Strategic Game around the Use of Force. *Security Studies* **2018**, *27*, 58-88, doi:10.1080/09636412.2017.1360074.
36. Faizullaev, A.; Cornut, J. Narrative practice in international politics and diplomacy: the case of the Crimean crisis. *Journal of International Relations and Development* **2017**, *20*, 578-604, doi:10.1057/jird.2016.6.
37. Haelig, C.G. Political-Military Integration: The Relationship Between National Security Strategy and Changes in Military Doctrine in the United States Army and Marine Corps. Ph.D., Princeton University, United States -- New Jersey, 2023. Available online: https://www.proquest.com/dissertations-theses/political-military-integration-relationship/docview/2869881038/se-2.
38. Alberts, D.S.; Hayes, R.E. *Power to the Edge: Command, Control in the Information Age*; CCRP Publication Series: 2003.
39. Pedrozo, R. Close Encounters at Sea. *Naval War College Review* **2009**, *62*, 101-112, http://www.jstor.org/stable/26397037.
40. Lindsay, J.R.; Gartzke, E. Politics by many other means: The comparative strategic advantages of operational domains. *Journal of Strategic Studies* **2022**, *45*, 743-776, doi:10.1080/01402390.2020.1768372.
41. Lucas, E. *The Coming Storm: Baltic Sea Security Report, Washington, DC*; Center for European Policy Analysis: Washington, DC, 2015. Available online: https://ekspertai.eu/static/uploads/2014/01/Baltic%20Sea%20Security%20Report-%20(2)_compressed.pdf.
42. Valeriano, B.; Jensen, B.M.; Maness, R.C. *Cyber Strategy: The Evolving Character of Power and Coercion*; Oxford University Press: 2018.
43. Fitton, O. Cyber Operations and Gray Zones: Challenges for NATO. *Connections* **2016**, *15*, 109-119, http://www.jstor.org/stable/26326443.
44. Schulze, M. Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. In Proceedings of the 2020 12th International Conference on Cyber Conflict (CyCon), 26-29 May 2020, 2020; pp. 183-197. Available online.
45. Howard, P.N.; Woolley, S.; Calo, R. Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics* **2018**, *15*, 81-93, doi:10.1080/19331681.2018.1448735.
46. Ng, L.H.X.; Robertson, D.C.; Carley, K.M. Cyborgs for strategic communication on social media. *Big Data & Society* **2024**, *11*, 20539517241231275, doi:10.1177/20539517241231275.
47. Di Salvo, P. "Hacking and information disorder: the weaponization of leaking". *Critical Studies in Media Communication* **2025**, *42*, 83-88, doi:10.1080/15295036.2025.2465693.
48. Hoskins, A.; O'Loughlin, B. *War and Media*; Polity Press: 2010.
49. Durani, K.; Eckhardt, A.; Durani, W.; Kollmer, T.; Augustin, N. Visual audience gatekeeping on social media platforms: A critical investigation on visual information diffusion before and during the Russo–Ukrainian War. *Information Systems Journal* **2024**, *34*, 415-468, doi:10.1111/isj.12483.
50. Chadwick, A. *The Hybrid Media System: Politics and Power*; Oxford University Press: 2017.
51. Bruns, A. *Gatewatching and news curation*; Peter Lang Publishing: New York, NY, 2018; Volume 113.
52. McGregor, S.C. Social media as public opinion: How journalists use social media to represent public opinion. *Journalism* **2019**, *20*, 1070-1086, doi:10.1177/1464884919845458.
53. Sacco, V.; Bossio, D. Using social media in the news reportage of War & Conflict: Opportunities and Challenges. *The journal of media innovations* **2015**, *2*, 59-76, doi:10.5617/jmi.v2i1.898.
54. Loik, R. Undersea Hybrid Threats in Strategic Competition: The Emerging Domain of NATO–EU Defense Cooperation. *Journal on Baltic Security* **2024**, *10*, 1-25, doi:10.57767/jobs_2024_008.
55. Składanowski, M.; Smuniewski, C.; Lukasik-Turecka, A. The Media's Role in Preparing Russian Society for War with the West: Constructing an Image of Enemies and Allies in the Cases of Latvia, Poland, and Serbia (2014–2022). *Journalism and Media* **2025**, *6*, 79, doi:10.3390/journalmedia6020079.
56. Meleshevich, K.; Schafer, B. Online information laundering: The role of social media. *Alliance for Securing Democracy* **2018**, *9*, 8, https://www.gmfus.org/sites/default/files/InfoLaundering_final%20edited.pdf.

57. Cordeiro, A. Digital Deceptions: Unveiling the Impact of Pseudo-Local News on Democracy and Crafting Countermeasures (Metric Media Case Study). Masters, Concordia University, 2025. Available online: https://spectrum.library.concordia.ca/id/eprint/995423/.
58. Papacharissi, Z. Affective publics: Sentiment, technology, and politics; Oxford University Press: 2015.
59. Gillespie, T. Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media; Yale University Press: 2018.
60. Tsfati, Y.; Boomgaarden, H.G.; Strömbäck, J.; Vliegenthart, R.; Damstra, A.; Lindgren, E. Causes and Consequences of Mainstream Media Dissemination of Fake News: Literature Review and Synthesis. *Annals of the International Communication Association* **2020**, *44*, 157-173, doi:10.1080/23808985.2020.1759443.
61. Bradshaw, S.; Howard, P.N. *The global disinformation order: 2019 global inventory of organised social media manipulation*; Project on Computational Propaganda: Oxford, UK, 2019. Available online: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1209&context=scholcom.
62. Woolley, S.C. Bots and Computational Propaganda: Automation for Communication and Control. In *Social Media and Democracy*, Persily, N., Tucker, J.A., Eds.; SSRC Anxieties of Democracy; Cambridge University Press: Cambridge, 2020; pp. 89-110, https://www.cambridge.org/core/product/A15EE25C278B442EF00199AA660BFADD.
63. Woolley, S.; Monaco, N. Amplify the Party, Suppress the Opposition: Social Media, Bots, and Electoral Fraud. *Geo. L. Tech. Rev.* **2019**, *4*, 447-461.
64. Tufekci, Z. Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Tech. LJ* **2015**, *13*, 203.
65. Bennett, W.L.; Livingston, S. The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication* **2018**, *33*, 122-139, doi:10.1177/0267323118760317.
66. Benkler, Y.; Faris, R.; Roberts, H. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. **2018**, doi:10.1093/oso/9780190923624.001.0001.
67. Lazer, D.M.J.; Baum, M.A.; Benkler, Y.; Berinsky, A.J.; Greenhill, K.M.; Menczer, F.; Metzger, M.J.; Nyhan, B.; Pennycook, G.; Rothschild, D.; et al. The science of fake news. *Science* **2018**, *359*, 1094-1096, doi:10.1126/science.aao2998.
68. Vosoughi, S.; Roy, D.; Aral, S. The spread of true and false news online. *Science* **2018**, *359*, 1146-1151, doi:10.1126/science.aap9559.
69. Pesu, M.; Sinkkonen, V. Trans-atlantic (mis)trust in perspective: asymmetry, abandonment and alliance cohesion. *Cambridge Review of International Affairs* **2024**, *37*, 206-225, doi:10.1080/09557571.2023.2225650.
70. Kunertova, D.; Schmitt, O. Assessing NATO's cohesion: methods and implications. *International Politics* **2025**, *62*, 1097-1110, doi:10.1057/s41311-024-00641-1.
71. Homolar, A.; Turner, O. Narrative alliances: the discursive foundations of international order. *International Affairs* **2024**, *100*, 203-220, doi:10.1093/ia/iiad291.
72. Snyder, G.H. *Alliance politics*; Cornell University Press: 2007.
73. DeMets, S.A.; Spiro, E.S. Podcasts in the periphery: Tracing guest trajectories in political podcasts. *Social Networks* **2025**, *82*, 65-79, doi:10.1016/j.socnet.2025.03.003.
74. Wilson, T.; Starbird, K. Cross-platform disinformation campaigns: lessons learned and next steps. *Harvard Kennedy School Misinformation Review* **2020**, *1*, doi:10.37016/mr-2020-002.
75. Dowling, D.O.; Johnson, P.R.; Ekdale, B. Hijacking Journalism: Legitimacy and Metajournalistic Discourse in Right-Wing Podcasts. *Media and Communication; Vol 10, No 3 (2022): Journalism, Activism, and Social Media: Exploring the Shifts in Journalistic Roles, Performance, and Interconnectedness* **2022**, doi:10.17645/mac.v10i3.5260.
76. Rasheed, H.; Cuddy, L.; Molokach, B.; Nam, J.; Feuerstein, S.; Holbert, L.; Young, D. From Punchlines to Politics: The Joe Rogan Experience as a Case Study of the Politicization of Apolitical Spaces in the US. *APSA Preprints* **2025**, doi:10.33774/apsa-2025-v05hb.

 doi:10.20944/preprints202601.1500.v1

disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.