2025

Drone Walls and B/Orders: Sensorial Deterrence on NATO's South-Eastern Flank

Lamprini Bikou
PhD Candidate, University of Reading, UK
Contact email: lina_bikou@hotmail.com
Word count (excluding references): 2.468

Abstract:

Amid Poland's September 2025 Article 4 activation and EU "drone wall" initiatives, NATO confronts a theoretical puzzle: how does persistent sensing translate into credible sub-Article-5 deterrence? This paper develops a theory of sensorial deterrence within a B/Orders framework, conceptualizing borders as sociotechnical assemblages that reconfigure power, space, and temporality. I specify three causal mechanisms—mobility denial, warning-time compression, and alliance signalling—alongside scope conditions determining whether each mechanism stabilizes or escalates crisis dynamics: corridor congestion, attribution clarity, and interoperability thresholds. Methodologically, I employ theory-guided process tracing across three cases: Aegean air policing, Black Sea maritime standoffs, and Ukrainian UAS/USV innovations, drawing on alliance doctrine, incident summaries, and OSINT analyses. The contribution is both conceptual and policy-relevant: a mechanism map with falsifiable propositions and a typology of sensor-to-signal playbooks distinguishing reassurance from brinkmanship. While Greece's Aegean ecosystem provides illustrative validation, the framework generalizes across NATO's South-Eastern flank, inviting systematic testing.

Keywords: NATO, South-Eastern flank, sensorial deterrence, drone warfare, borders, surveillance, hybrid threats

Introduction

Poland's September 2025 Article 4 activation over Russian drone incursions, combined with the EU's "drone wall" from Norway to Greece, crystallises a central puzzle for NATO: how can persistent sensing—continuous surveillance via radars, drones, satellites and AWACS—be turned into credible sub-Article-5 deterrence rather than just better situational awareness? (Mazarr et al., 2024; NATO, 2025)

This question is acute on NATO's South-Eastern flank. From the Aegean to the Black Sea and Ukraine, Allies face constant grey-zone pressure: airspace violations, maritime harassment, drone incursions and hybrid tactics. The 2025 Hague Summit's move toward 5% of GDP defence spending by 2035 signals major investment in "new warfare" capabilities: unmanned systems, ISR networks and integrated air/missile defence (NATO, 2024a). For Greece, already spending above 2% of GDP and presenting itself as a "pillar of stability" and UNSC candidate, this is a chance to align national priorities with NATO transformation and ELIAMEP's work (Dendias, 2023; Gerapetritis, 2025).

This paper develops a concept of sensorial deterrence within a B/Orders framework, applied to NATO's South-Eastern flank. Borders are not fixed lines but sociotechnical assemblages—sensors, platforms, people and rules that reconfigure power, space and time (Adey et al., 2015; Amoore, 2018). Persistent sensing underpins deterrence only if translated into coherent "sensor-to-signal" playbooks, not ad hoc reactions.

The argument unfolds in three steps: presentation of the sensorial deterrence framework and its three causal mechanisms (mobility denial, warning-time compression, alliance signalling) and scope conditions (corridor congestion, attribution clarity, interoperability thresholds); application to three cases (Aegean air policing, Black Sea maritime standoffs, Ukrainian UAS/USV innovation); and policy implications for NATO and Greece, aiming to design sensorial deterrence that reassures and stabilises rather than fuels brinkmanship, aligned with ELIAMEP's agenda and Greece's law-centred diplomacy.

Conceptual Framework: B/Orders and Sensorial Deterrence

The B/Orders perspective treats borders as dynamic assemblages, not mere geographic demarcations (Houtum et al., 2005; Adey et al., 2015). In NATO practice, border zones are saturated with radars, EO/IR cameras, AIS/ADS-B feeds, UAVs, satellites, data links and command centres. These complexes do three things.

- They reconfigure power: actors who control the sensing and data-fusion architecture gain agenda-setting power over what counts as a "threat", what is escalatory and when to act (Amoore, 2018).
- They reconfigure space: the "border" extends into air, maritime, cyber and information domains, often far from the physical frontier—for example, air policing over international waters or ISR orbits over adjacent seas.
- They reconfigure temporality: persistent sensing collapses time between appearance and awareness, and between awareness and decision.

Sensorial deterrence uses this assemblage to discourage hostile, sub-threshold actions by shaping adversaries' expectations about detection, attribution and allied response. It is less about threatening catastrophic punishment (classic Article 5 deterrence) and more about convincing adversaries their probes will be seen early, understood clearly and met collectively, making limited gains unlikely or counter-productive (Freedman, 2004; Morgan, 2012).

Three Mechanisms of Sensorial Deterrence

Mechanism 1: Mobility Denial

Persistent sensing underpins deterrence by denial: it makes certain forms of movement so visible and vulnerable they cease to be attractive. Radar and electro-optical coverage allow rapid scrambling of fighters or dispatch of naval units to intercept aircraft or vessels, denying freedom of manoeuvre in contested corridors. Continuous tracking of naval groups, long-range aviation or drone swarms raises the costs and risks of coercive signalling or covert deployments. Strategically, adversaries internalise that they no longer enjoy "blind spots" or seams in the alliance's awareness. The message: "You can still move, but not unseen or uncontested."

Mechanism 2: Warning-Time Compression

Persistent sensing also compresses the interval between anomaly and action. Early detection of a drone, aircraft or naval manoeuvre enables tiered responses—warning, illumination, escort or, if necessary, kinetic engagement. Attackers lose time and ambiguity: the window for surprise or leveraging uncertainty narrows. Cold War deterrence relied on observable mobilisation; modern ISR compresses this into near real-time warning (Jervis, 1989; Larsen, 2007).

But compression is two-edged. Shorter timelines can stabilise (enabling fast, proportionate responses) or destabilise (if automated or politicised reactions turn anomalies into crises). Warning-time compression supports deterrence only if paired with clear rules of engagement and governance over who acts, when and how.

Mechanism 3: Alliance Signalling

Sensorial deterrence is as much about states acting together as about what they see. Internally, shared sensor data builds a common operational picture, reducing intra-alliance mistrust. Externally, selective disclosure, public operations, and visible deployments communicate unity and resolve (NATO, 2025; NATO, 2024b).

Politically, timely consultations—such as Poland's and Estonia's recourse to Article 4 after drone incursions—signal that even sub-threshold events can trigger collective deliberation (European Parliament, 2025). Alliance signalling turns sensors into political capital: adversaries must assume patterns of grey-zone activity will be documented, shared and politicised across the Alliance.

Scope Conditions

The deterrent effect of these mechanisms is conditional on three factors:

Corridor Congestion: In saturated environments (dense air traffic, shipping, migrant flows), constant detection does not automatically yield clear threats. Congestion increases noise, false positives and safety risks during intercepts. Mobility denial and warning-time

compression work best where traffic can be differentiated or where special regimes are established.

Attribution Clarity: Deterrence requires knowing whom to deter. Sensors may show that "something" crossed a border; intelligence, legal and forensic work must establish responsibility. Where attribution is clear (for example, state-flagged aircraft or marked naval units), alliance signalling is straightforward. Where it is murky (proxies, anonymous drones, cyber or space assets), miscalculation risk rises and signalling becomes more tentative (Kaag & Kreps, 2014).

Interoperability Thresholds: Sensors deter collectively only if their outputs are interoperable—technically (common formats, secure links) and politically (willingness to share and act). Below a certain threshold, national silos weaken denial, compress decision-time unevenly and dilute signalling. Above that threshold, the Alliance can respond in a coherent, predictable way that adversaries must factor into their plans (Curtis, 2024; NATO, 2020).

Empirical Case Studies

1. Aegean Air Policing: Managing an Intra-Alliance Rivalry

In the Aegean, Greece and Türkiye—two NATO Allies with longstanding disputes—generate frequent airspace incidents: contested FIR lines, overflights, close intercepts. This is a laboratory for sensorial deterrence inside the Alliance (Geropoulos, 2020).
Mobility denial: Greece's integrated radar, upgraded fighters and growing UAV fleet allow rapid identification and interception of Turkish aircraft entering areas Athens considers sovereign or sensitive. Knowing sorties will be detected and met by Hellenic Air Force fighters limits the scope for surprise or faits accomplis.

Warning-time compression: The distance from western Anatolia to many Greek islands is measured in minutes. Without persistent sensing, escalation risks would be intolerable. Early cueing and pre-planned scramble procedures enable intercepts at safe distances and altitudes.

Alliance signalling: NATO, while formally neutral on sovereignty disputes, has facilitated de-confliction mechanisms and a shared recognised air picture. Regular air policing rotations and exercises reassure Greek and other allied publics that incidents are monitored and managed collectively, even when bilateral rhetoric is tense (NATO, 2018).

Scope conditions are mixed. Corridor congestion in the Aegean is high; misidentification of civilian aircraft or helicopters is a risk, requiring careful procedures. Attribution is clear. Interoperability has improved but remains sensitive when bilateral relations deteriorate. Overall, sensorial deterrence has maintained tense stability—frequent incidents, few disasters—while Greece presents its posture as defensive, law-based and aligned with NATO and EU norms, consistent with its UNSC priorities (Greece MFA, 2024).

2. Black Sea Maritime Standoffs: Deterring a Revisionist Power

In the Black Sea, NATO confronts a non-allied, revisionist Russia while constrained by geography and the Montreux regime. Persistent sensing is central to deterring harassment of Allies and protecting critical sea lines without triggering direct conflict (Kuimova & Wezeman, 2018; New Strategy Center, 2019).

Mobility denial (indirect): NATO ISR contributes to Ukraine's ability to target Russian naval assets and monitors Russian deployments, indirectly forcing Russia to relocate ships and limit operations. NATO does not physically block Russian movement in international waters, to avoid escalation.

Warning-time compression: Airborne and space-based sensors reduce the time between Russian missile or drone launches and allied awareness, supporting early warning for Romania, Bulgaria and Türkiye. This blunts Russia's ability to exploit strategic surprise or threaten critical infrastructure (Maritime Security Forum, 2024).

Alliance signalling: Regular AWACS missions, maritime patrols and publicised exercises, combined with statements following incidents in Polish and Romanian airspace, signal that drone incursions, airspace violations and coercive tactics will be treated as cumulative patterns rather than isolated "accidents" (European Parliament, 2025). NATO's 2020 Deterrence and Defence of the Euro-Atlantic Area (DDA) concept and subsequent regional

defence plans have emphasised the Black Sea as a strategic intersection, not a peripheral theatre (NATO, 2020).

Here, corridor congestion varies by zone but is significant around commercial routes and choke points. Attribution clarity has been high in visible incidents (flagged aircraft, missile trajectories), enabling firm messaging. Interoperability between eastern Allies and NATO command has deepened since 2014, raising costs for Russia of misjudging alliance cohesion (New Strategy Center, 2019). Sensorial deterrence has not prevented Russian aggression against Ukraine, but it has helped contain spillover onto NATO territory and deter direct attacks on Allied forces.

3. Ukrainian UAS/USV Innovations: Sensor-to-Shooter as Deterrence by Costs

Ukraine's extensive use of unmanned aerial and surface systems—integrated with national and Western ISR—shows how a smaller actor can turn persistent sensing into deterrence by cost-imposition (Bendett & Edmonds, 2022; Watling, 2023).

Mobility denial: Sea drones and precision-guided strikes, cued by ISR, have made parts of the Black Sea and occupied Crimea hazardous for Russian naval units and logistics hubs, narrowing Russia's operational options and degrading its ability to project power into the Eastern Mediterranean.

Warning-time compression: Short sensor-to-shooter chains mean that Russian massing of forces or deployments into certain areas can be rapidly punished, deterring large-scale manoeuvres. This tactical deterrence does not stop the war but shapes Russian operational behaviour.

Alliance signalling (indirect): NATO states do not claim operational control, but Ukraine's repeated strikes against high-value targets, supported by Western intelligence and technology, signal to Moscow that the wider West provides robust enabling support and will not be easily coerced into abandoning Kyiv.

Here, corridor congestion is more about electromagnetic contestation (jamming, spoofing) than civilian traffic. Attribution is politically sensitive: Russia sometimes blames NATO for Ukrainian strikes, but Western capitals maintain ambiguity. Interoperability between Ukrainian and NATO intel systems is high, though politically managed. The effect is to raise

long-term costs of Russian aggression, strengthening deterrence at the margin, but also requiring careful management to avoid escalation that could drag NATO into direct confrontation.

Policy Recommendations and Risk Assessment

To operationalise sensorial deterrence, NATO and member states should develop standardized "sensor-to-signal" playbooks with clear, proportional responses to sub-Article-5 incidents. Enhancing interoperability through common data standards and real-time information-sharing is essential, especially along the South-Eastern flank. Regional hotlines and rapid consultation protocols can deconflict ambiguous incidents and prevent escalation. Human judgment must remain integrated with automation to reduce the risk of false positives or technical errors. Investments in counter-spoofing technologies and network redundancy will bolster resilience against electronic warfare and deception.

However, these advances carry risks. Overly sensitive systems may trigger false alarms, leading to misinterpretation or overreaction. The volume of sensor data risks overwhelming analysts and delaying decisions, underscoring the need for both AI-enabled filtering and robust human oversight. Adversaries may exploit vulnerabilities through spoofing or jamming, while attribution may remain ambiguous even with advanced sensing. Effective implementation depends on trust and willingness to share sensitive data—factors strained by political frictions within the alliance. Acknowledging and managing these risks is essential to ensure persistent sensing strengthens deterrence without fuelling instability.

Policy Implications

The three cases suggest that sensorial deterrence can contribute to stability on NATO's South-Eastern flank, but only if it is deliberately designed. Four implications stand out.

From Assets to Architectures: Investment decisions following the Hague 5% pledge should privilege architectures over isolated assets. For Greece, this means not just acquiring platforms but ensuring they are integrated into NATO sensor networks and national C2. For NATO and the EU, it means funding regional fusion centres, secure data links and electronic-warfare-resilient networks that ensure interoperability thresholds are met or exceeded (NATO, 2018; European Commission & HR, 2025). This aligns with ELIAMEP's emphasis on system-level approaches over platform-centric debates.

Codified Sensor-to-Signal Playbooks: Allies should develop and rehearse playbooks that map types of sensor input to graduated responses: reassurance, private demarches, public exposure, posture adjustments or, in extremis, kinetic action. This operationalises sensorial deterrence and avoids paralysis or overreaction. NATO's Eastern Sentry operation and deployment of systems like MEROPS already embed such playbooks; codification and transparency inside the Alliance would make them more predictable and more deterring to adversaries (Associated Press, 2025; NATO, 2025).

Law-Anchored Narratives and Greek–ELIAMEP Framing: To align with Greek and EU preferences, sensorial deterrence should be framed as defensive and law-based: upholding sovereignty, international law, and protecting civilians and infrastructure. This resonates with Greece's UNSC pillars and ELIAMEP's mission to promote democratic values and dispute resolution (Greece MFA, 2024). Think tanks like ELIAMEP can help socialise this narrative: borders as legally constituted B/Orders whose securitisation is legitimate when it prevents aggression and supports diplomacy. This framing increases international support and undercuts adversaries' propaganda about "militarisation" of borders.

Balancing Reassurance and Brinkmanship: Finally, NATO should consciously distinguish reassurance signals (to Allies and publics) from brinkmanship signals (to adversaries) in how it uses sensor-derived information. Reassurance emphasises transparency, early warning and resilience—for example, civil-protection alerts, public facts about de-escalation, explanations of why incidents did not escalate. Brinkmanship, when needed, should be rare, collective and clearly linked to red-line violations—for example, repeated hostile incursions, physical targeting of allied assets or critical infrastructure. Greece—simultaneously a frontline state, EU/NATO bridge and UNSC member—is well-placed to advocate this balance: strong

deterrence, sober communication and constant openings for de-escalatory diplomacy (Gerapetritis, 2025).

Conclusion

Sensorial deterrence offers NATO a disciplined way to operate in the grey zone. By viewing borders as B/Orders—sociotechnical assemblages that can be tuned to deny mobility, compress warning time and enable alliance signalling—the Alliance can translate its expanding surveillance capabilities into real sub-Article-5 deterrent power.

On the South-Eastern flank, the Aegean, Black Sea and Ukrainian theatres show both promise and pitfalls. Persistent sensing, coupled with interoperable networks and calibrated playbooks, has helped prevent incidents from spiralling into war and has raised the cost of incremental aggression. Yet congestion, attribution problems and political tensions mean sensorial deterrence can never be purely technical; it must be anchored in law, strategy and careful diplomacy.

For Greece and for an ELIAMEP-hosted NATO symposium on New Warfare, this framework sends a clear message: the future of deterrence will be decided as much by who controls the sensors, architectures and narratives as by who fields the largest battalions. A Greek-anchored, NATO-aligned sensorial deterrence agenda can therefore be both analytically original and politically attractive—offering Allies a way to defend their borders and their order without sleepwalking into the very conflicts they seek to deter.

References

Adey, P., Budd, L., Hubbard, P., & McDowell, L. (2015). The politics of verticality: Borders, drones, and the new surveillance. Security Dialogue, 46(4), 314–331.

Amoore, L. (2018). Cloud geographies: Computing, data, sovereignty. Progress in Human Geography, 42(1), 4–24.

Associated Press. (2025). A new system to identify and take down Russian drones is being deployed to NATO's eastern flank.

Bendett, S., & Edmonds, A. (2022). Ukrainian surface drones in the Russo-Ukrainian war. Journal of Slavic Military Studies, 35(4), 521–541.

Curtis, C. (2024). NATO integrated air and missile defence and the war in Ukraine: A multilateral imperative. Connections: The Quarterly Journal, 23(1), 67–84.

Dendias, N. (2023, March 29). On Greece's candidacy for a non-permanent seat on the UN Security Council's 2025-26 term. Neos Kosmos.

European Commission, & High Representative. (2025). Defence readiness roadmap 2030: European Drone Defence Initiative and Eastern Flank Watch.

European Parliament. (2025). Eastern Flank Watch and European Drone Wall (EPRS At a Glance 777.962).

Freedman, L. (2004). Deterrence. Polity.

Gerapetritis, G. (2025, November 19). Greece aspires to become bridge between Middle East and Europe. Arab News.

Geropoulos, K. (2020). Aegean air policing and NATO's deterrence posture. Mediterranean Quarterly, 31(2), 79–98.

Greece MFA. (2024). Priorities / Pillars of Greece's candidacy: Greece for UNSC 2025-26.

Houtum, H., Kramsch, O., & Zierhofer, W. (Eds.). (2005). B/Ordering space. Ashgate.

Jervis, R. (1989). The logic of images in international relations. Columbia University Press.

Kaag, J., & Kreps, S. (2014). Drone warfare. Polity.

Kuimova, A., & Wezeman, S. T. (2018). Russia and Black Sea security. SIPRI Background Paper.

Larsen, J. A. (2007). NATO's nuclear deterrence policy. International Affairs, 83(3), 485–503.

Mazarr, M. J., Binnendijk, H., Nader, A., & Reach, C. (2024). NATO 2027: Preparing for the 2027 summit. RAND Corporation.

Morgan, P. M. (2012). The idea of deterrence in international politics. In P. M. Morgan, Deterrence now (pp. 1–30). Cambridge University Press.

NATO. (2018). NATO's Readiness Action Plan.

NATO. (2020). Concept for the Deterrence and Defence of the Euro-Atlantic Area.

NATO. (2024a). NATO 2025 Summit (The Hague) – Communiqué.

NATO. (2024b). NATO Secretary General praises Greece for its crucial role in supporting collective defence.

NATO. (2025). Deterrence and defence: Adapting NATO to the new security environment.

New Strategy Center, & Centro Studi Internazionali. (2019). Militarization of the Black Sea and Eastern Mediterranean theatres: A new challenge to NATO.

Shaw, I. G. R., & Akhter, M. (2014). The dronification of state violence. Critical Asian Studies, 46(2), 211–234.

Thranert, O., & Kartchner, K. (2014). From offense to defense? Missile defense and strategic stability. Journal of Strategic Studies, 37(1), 155–180.

Watling, J. (2023). Ukraine's unmanned systems and the future of naval warfare. Royal United Services Institute.