Visibility, Vulnerability, and First-Mover Incentives

Why NATO's Baltic Deterrence Risks a Pre-emptive Strike

Clingendael Report

Erik Stijnman

Clingendael
Netherlands Institute of International Relations

Clingendael

Netherlands Institute of International Relations

Visibility, Vulnerability, and First-Mover Incentives

Why NATO's Baltic Deterrence Risks a Pre-emptive Strike

Erik Stijnman

Clingendael Report
July 2026

July 2026

About the Clingendael Institute

The Netherlands Institute of International Relations 'Clingendael' is a leading think tank and academy on international affairs. Through our analyses, training and public platform activities we aim to inspire and equip governments, businesses, and civil society to contribute to a secure, sustainable and just world.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media
@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Clingendael Institute

Email: info@clingendael.org
Website: www.clingendael.org

About the author

Erik Stijnman is an Army Lieutenant Colonel in active Dutch Service and has been seconded to Clingendael as Senior Research Fellow with Clingendael's Security Unit. He focusses on security-related topics with a geographical focus on Russia and Ukraine and with a thematic focus on Combat and Peacekeeping Operations, Intelligence, Decision-making and Military Innovation and Adaptation and the use of Artificial Intelligence

The author would like to thank René Cuperus, Bob Deen, Kolonel P.A.P. Dekkers, Karen van Loon and Bart van den Berg for their valuable insights and constructive feedback during the peer review process.

Statement on the use of generative AI

In accordance with the European Commission's *Living Guidelines on the Responsible Use of Generative AI in Research*,* this report discloses the use of generative AI during its preparation. AI tools were used to provide language suggestions, editorial feedback, proofreading, and to generate an illustrative figure. All AI-assisted outputs were reviewed and validated by the author. The author remains solely responsible for the analysis, arguments, interpretations, conclusions, source verification, and the accuracy of the content of this publication.

* European Commission, *Living Guidelines on the Responsible Use of Generative AI in Research* (Brussels: Directorate-General for Research and Innovation, 2024), https://research-and-innovation.ec.europa.eu/document/download/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en

Contents

Executive Summary

NATO's forward presence in the Baltic States strengthens political credibility but increasingly undermines operational survivability under conditions of persistent battlefield transparency. As such, military personnel and equipment are under continuous risk to be quickly identified by a vast array of sensors and will subsequently be decisively engaged.

Advances in ISR, unmanned systems, and rapid targeting cycles reduce concealment, compress decision-making timelines, and strengthen first-mover incentives. This exacerbates existing structural tensions between deterrence by punishment and deterrence by denial.

This policy brief argues that current forward deployments in the Baltic States risk enabling a rapid fait accompli rather than preventing it. To address this, NATO should adopt a hybrid posture combining distributed, low-signature systems with a limited but credible human presence, while prioritising ambiguity, signature reduction, and disruption of targeting cycles. Deterrence in this context depends on the ability to remain survivable and operational under conditions of persistent detection.

Introduction

For decades, NATO's forward presence in the Baltic States has been regarded as a cornerstone of deterrence. By stationing multinational forces close to potential flashpoints, the Alliance seeks to reassure allies and demonstrate political resolve. NATO's enhanced Forward Presence (eFP) is explicitly designed to combine deterrence with reassurance[1]. While reassurance fulfils an important political function, it does not in itself generate a military effect. Tripwire forces may signal commitment, but they do not necessarily deter a determined adversary such as Russia.[2]

Since the establishment of the eFP in 2017 – to which the Netherlands has been a contributing nation – the operational environment has changed markedly. The war in Ukraine demonstrates how persistent Intelligence, Surveillance and Reconnaissance (ISR), unmanned systems and increasingly rapid targeting cycles have significantly increased battlefield transparency. What was once conceived as a credible signal of commitment increasingly risks becoming an exposed forward posture under conditions of persistent detectability.

As military personnel, equipment and infrastructure become more visible and targetable, the interval between detection and engagement is compressed. Persistent ISR and integrated sensor-to-shooter networks leave little time for concealment, manoeuvre or reaction, making forward-deployed forces increasingly vulnerable to rapid engagement. As a result, the perceived feasibility of achieving limited objectives quickly increases, strengthening incentives for pre-emptive action and fait accompli strategies before an effective NATO response can be organised.

This development creates a growing tension at the heart of NATO's deterrence posture. While forward presence reinforces deterrence by punishment by strengthening political credibility and signalling Alliance commitment, persistent

1 NATO, "Deterrence and Defence," last modified December 10, 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence.

2 Paul Lushenko and Benjamin Jensen, "The Truth About Tripwires: Why Small Force Deployments Do Not Deter Aggression," *Texas National Security Review* 2, no. 3 (2019), https://tnsr.org/2019/05/the-truth-about-tripwires-why-small-force-deployments-do-not-deter-aggression/.

battlefield transparency simultaneously undermines deterrence by denial by reducing the survivability of forward-deployed forces. In this sense, measures intended to enhance deterrence may inadvertently increase the attractiveness of rapid, limited operations.

Against this background, this policy brief argues that technological developments are creating a structural tension between political credibility and operational survivability. It assesses the implications of this tension for NATO's Eastern Sentry strategic concept at the theatre level in the Baltic States. It examines how deterrence by denial can be restored under conditions of persistent battlefield transparency, while reducing incentives for rapid first-mover or fait accompli strategies which are aimed at achieving limited political-military objectives.

The analysis primarily focuses on deterrence in the land domain and on scenarios involving limited territorial incursions or coercive fait accompli strategies. Although contemporary deterrence increasingly relies on long-range strike, airpower, cyber capabilities and strategic coercion, the Baltic theatre remains uniquely vulnerable to rapid ground-based territorial denial problems due to its limited strategic depth.

The structure of this policy brief is as follows. It first reviews NATO's current deterrence posture in the Baltic States, then analyses lessons from Ukraine, and subsequently develops an alternative hybrid model of linear and non-linear defence, followed by policy recommendations and conclusions.

1 NATO deterrence in the Baltic States

1.1 Structural limitations of forward presence and tripwire forces

A growing body of literature questions whether 'NATO's current deterrence posture in the Baltic States can prevent a rapid Russian incursion when relying on limited forward deployments'.[3] This reinforces concerns that such forces risk functioning primarily as a political tripwire rather than a militarily robust defence. However, the forward deployed forces – in line with the NATO Force Model[4] – are still expected to survive long enough for follow-on forces to reach the theatre of operations. The underlying assumption remains that the current size and concept of forward presence enhance deterrence, yet this assumption becomes increasingly contested under conditions of persistent battlefield transparency.

Subsequent studies have emphasised the need to strengthen deterrence by denial, arguing that NATO must be able to prevent a rapid fait accompli, rather than relying solely on punishment through later escalation.[5] Even with the planned expansion from multinational battlegroups (1,000–1,500 troops) to brigade-sized formations (3,000–5,000 troops), the force design remains insufficient to support denial, particularly as increased battlefield transparency undermines the survivability of forward-positioned forces. As these studies underline, effective denial requires forward forces capable of slowing an adversary, absorbing initial shocks, and holding terrain long enough for reinforcements to arrive.

More recent analyses, however, highlight that the operational environment itself has fundamentally changed. The increasing transparency of the battlefield

3 David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (Santa Monica, CA: RAND Corporation, 2016).

4 NATO Supreme Headquarters Allied Powers Europe (SHAPE). n.d. "NATO Force Model." Accessed May 18, 2026. SHAPE NATO

5 Michael J. Mazarr et al., *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression* (Santa Monica, CA: RAND Corporation, 2018);
Karsten Friis and Benjamin Tallis, eds., *NATO and Collective Defence in the 21st Century* (London: Routledge, 2019).

– driven by persistent ISR, unmanned systems, and integrated targeting networks – has reduced the survivability of traditional command structures and large manoeuvre formations.[6]

These developments create a structural dilemma for forward deployments. On the one hand, multinational forces in the Baltics signal credible political commitment and reinforce NATO's resolve. On the other hand, geographically constrained and highly visible forward forces present attractive targets in the opening phase of a conflict.[7] Under conditions of persistent detectability- what is intended as a deterrent presence – may simultaneously increase vulnerability and reduce operational resilience.

As James Fearon and Robert Powell have shown[8], actors may initiate conflict when they believe that rapid action can decisively shift the balance of power or secure limited objectives before an adversary can effectively respond. Under such conditions, the perceived feasibility of success becomes a central driver of strategic behaviour.

Persistent battlefield transparency compresses decision-making timelines and increases the perceived feasibility of rapid local success, thereby strengthening incentives for pre-emptive action, particularly for wars with limited goals.

Crucially, however, these effects are not symmetrical. While increased transparency enhances situational awareness on both sides, NATO – as a fundamentally defensive alliance – faces significant political and doctrinal constraints on pre-emptive action. Even when detection is achieved, translating this into immediate engagement is far less feasible than for an adversary seeking to initiate hostilities. This asymmetry is further reinforced by political decision-making timelines, which constrain NATO's ability to act on rapidly emerging

6 Jack Watling and Nick Reynolds, *Operation Z: The Death Throes of an Imperial Delusion* (London: Royal United Services Institute, 2022).
Michael Kofman and Andrea Kendall-Taylor, "Russian Military Strategy and Ukraine," *Foreign Affairs*, 2023.

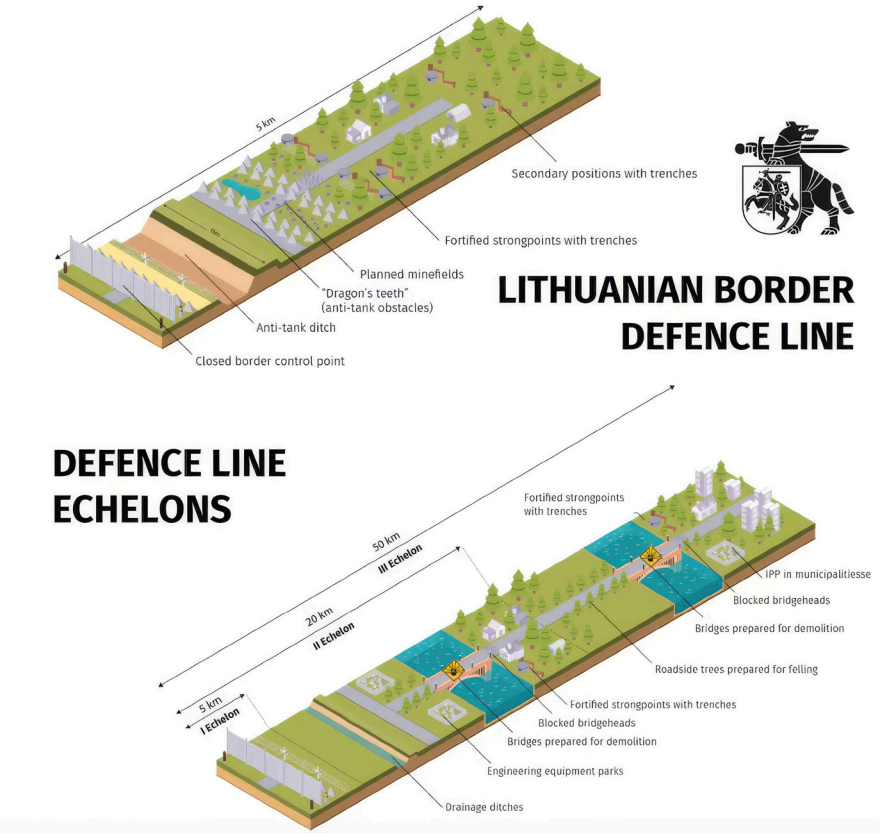
7 Karl Mueller et al., *NATO's Forward Presence: Implications for Deterrence and Defense* (Santa Monica, CA: RAND Corporation, 2018).

8 James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379–414; Robert Powell, *In the Shadow of Power: States and Strategies in International Politics* (Princeton: Princeton University Press, 1999).

targeting opportunities. As a result, battlefield transparency does not simply increase mutual vulnerability, but disproportionately benefits actors willing and able to act first.

In the Baltic theatre, this problem is compounded by limited strategic depth and proximity to Russia and Belarus. This structural constraint is particularly evident in Lithuania, where geography severely limits the ability to absorb an initial attack or manoeuvre in depth.

Figure 1 Lithuanian fortified defensive belts to counter the lack of strategic depth[9]



9 LSM.lv, "Building up Borders: How the Baltic States Are Reinforcing NATO's Eastern Flank," December 22, 2025, https://eng.lsm.lv/article/features/features/22.12.2025-building-up-borders-how-the-baltic-states-are-reinforcing-natos-eastern-flank.a626450/.

Lithuania's development of fortified defensive belts reflects an explicit recognition that classical manoeuvre warfare is difficult to sustain under these conditions. In doctrinal terms, a heavy division typically requires 50–100 km of operational depth and frontage to effectively echelon forces, enabling absorption of shock, manoeuvre in depth, and counterattack[10]. In the Baltic context, such depth is unavailable.

As a result, defensive effects – delay, disruption, and denial – must be artificially generated through layered fortifications, obstacles, and counter-mobility systems. Rather than relying on manoeuvre in depth, Lithuania seeks to impose friction on advancing forces through engineered defensive belts.

This adaptation directly reflects insights from earlier wargaming, which demonstrated that Russian forces could reach the outskirts of Tallinn and Riga within approximately 60 hours.[11] Under such compressed timelines, the ability to delay and disrupt becomes critical.

However, under conditions of persistent battlefield transparency, these defensive measures are also subject to the same structural pressures. As visibility increases, military personnel and installations which are part of the fortified positions and defensive belts become more easily detectable and targetable. This compresses the interval between detection and engagement, reinforces incentives for pre-emptive strikes, and ultimately reduces survivability.

Consequently, several studies argue that NATO's deterrence posture must evolve towards more distributed, resilient, and technologically enabled defence architectures capable of complicating adversary planning rather than presenting clearly identifiable targets.[12] In analytical terms, this reflects an attempt to disrupt the link between detection and engagement by reducing targetability and increasing operational planning uncertainty.

These debates form the broader analytical context for evaluating emerging NATO concepts – such as Eastern Sentry and the Eastern Flank Deterrence

10 NATO, *Allied Land Tactics (ATP-3.2.1)* (Brussels: NATO Standardization Office, 2016).

11 Shlapak and Johnson, *Reinforcing Deterrence on NATO's Eastern Flank*.

12 Andrew F. Krepinevich Jr., *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy* (New York: Basic Books, 2015);
Jack Watling, "The Future of Land Warfare," Royal United Services Institute, 2023.

Line – which seek to restore deterrence by denial under conditions of persistent battlefield transparency through distributed sensors, autonomous systems, and networked fires.

1.2 Changing character of war: operational and tactical lessons learned in Ukraine

Already in the early stages of the war in Ukraine, it became evident that increased battlefield visibility fundamentally altered the survivability of military formations. Static command posts, due to their electromagnetic signatures and logistical footprint, became easily detectable and targetable. As one study notes, "contemporary tented [Russian] command posts – with their radio frequency emitting antennas, dozens of generators and vehicles, and extensive support requirements – proved to be easy targets".[13]

The Ukrainian DELTA system, which reached full operational capability in 2023, exemplifies this transformation. As a combat digital ecosystem, it "enables real-time battlefield awareness, supports operational planning, and facilitates non-hierarchical information sharing within units, brigades, [and] formations".[14]

Detection-to-strike timelines have consequently compressed from days to minutes. As a result, both static and mobile targets become highly vulnerable, as the window for concealment or manoeuvre is significantly reduced.[15]

This dynamic is further illustrated by satellite imagery of electronic emissions from a brigade combat team (BCT) during training at the National Training Center (NTC). Such imagery shows that mobile targets are now nearly as vulnerable as static ones. Electronic warfare units can identify and geolocate

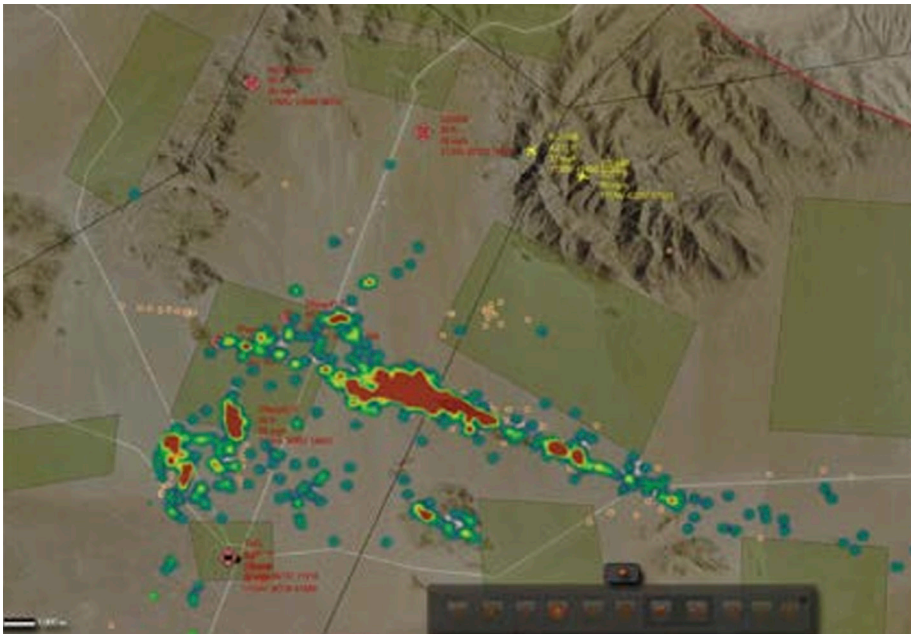
13 *The Graveyard of Command Posts: What Chernobaivka Should Teach Us about Command and Control in the Multidomain Era

14 Ministry of Defence of Ukraine, "The DELTA Combat System Has Been Deployed Across All Levels of Defence Forces of Ukraine," August 6, 2025, https://mod.gov.ua/en/news/the-delta-combat-system-has-been-deployed-across-all-levels-of-defence-forces-of-ukraine.

15 Kofman and Kendall-Taylor, "Russian Military Strategy and Ukraine".

enemy forces without direct line of sight, while near-real-time open-source intelligence further amplifies battlefield transparency.[16]

Figure 2 Electronic emissions signature density plot



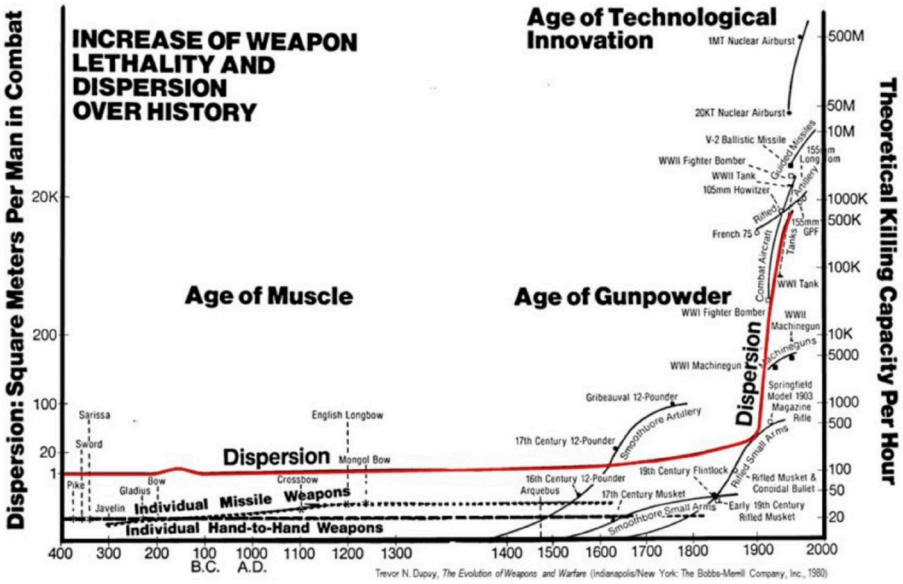
Tactical lessons learned: dispersion is key to survive

Consequently, both Ukrainian and Russian forces have adapted at the tactical level by dispersing their troops. This trend is not entirely new. As demonstrated by historical analysis, force density has steadily decreased over time, with contemporary force densities estimated at approximately one quarter of those observed on the Western Front during the Second World War.[17]

16 Bryan Clark, *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* (Washington, DC: Hudson Institute, 2022); Jack Watling, "The War in Ukraine and the Future of Land Warfare," Royal United Services Institute, 2023.

17 The Dupuy Institute, "*Historical Trends in Force Density and Lethality*" (Washington, DC: Dupuy Institute, 2018).

Figure 3 The evolution of weapons and warfare and dispersion



Technological advances in command and control, combined with the proliferation of drones, have enabled microtargeting, whereby even small tactical units can be identified and rapidly engaged. This further increases the vulnerability of dispersed forces, despite their reduced footprint.[18]

Both Russian and Ukrainian forces have therefore increasingly adopted highly mobile and low-signature platforms, such as motorcycles and all-terrain vehicles (ATVs), prioritising speed, dispersion, and expendability.[19]

Dismounted infantry often operates in small groups of three to five personnel, using terrain and weather conditions to avoid detection and evade first-person-view (FPV) drones and artillery engagement.[20] This underscores that survivability increasingly depends not on protection after detection, but on avoiding detection altogether.

18 Watling and Reynolds, *Operation Z*; Kofman and Kendall-Taylor, "Russian Military Strategy and Ukraine".

19 Watling, "The War in Ukraine and the Future of Land Warfare".

20 Watling and Reynolds, *Operation Z*.

At the same time, the effects of increased visibility extend beyond the frontline. Ukrainian brigades report that approximately 50% of their casualties occur in rear areas due to FPV drones, artillery, and glide bombs.[21] This shows that the distinction between front and rear areas has eroded. As a result, adaptations such as reduced troop rotations -sometimes leaving units in position for over a month – have emerged, with significant implications for fatigue and morale.[22]

In parallel, Ukraine has increasingly replaced human presence with unmanned systems for logistical and medical tasks, including the use of unmanned aerial and ground systems for resupply and casualty evacuation. This reflects efforts to reduce human exposure under persistent detectability.[23]

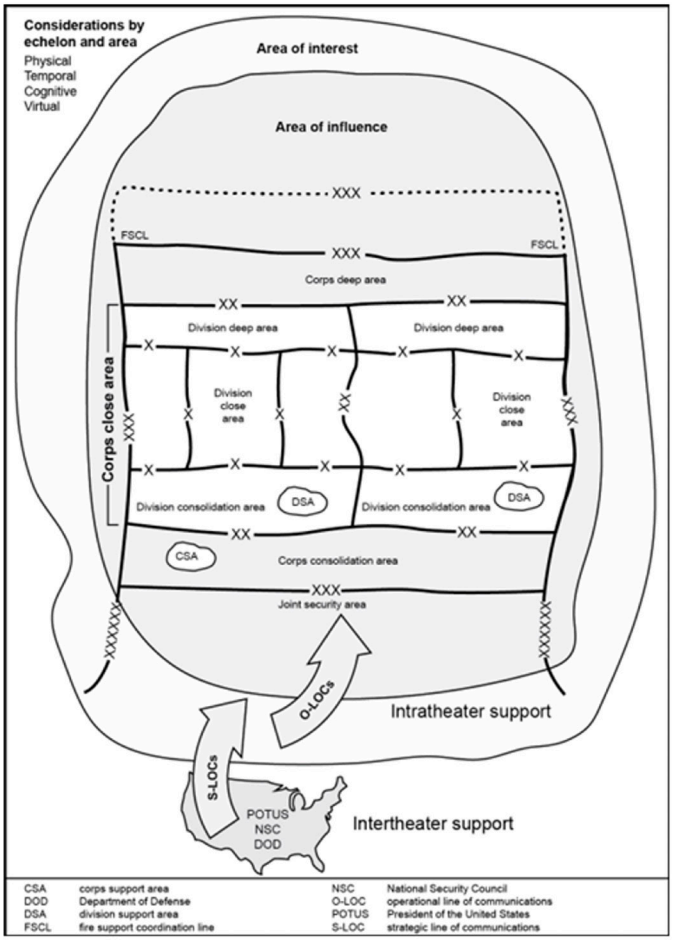
Operational lessons learned; revising the geographical framework

These tactical developments have broader operational implications. The traditional NATO concept of combined arms manoeuvre emphasises the concentration of armour, infantry, and artillery to achieve local superiority and disrupt enemy cohesion.[24]

This model assumes identifiable frontlines and the ability to concentrate forces. However, in an ISR-saturated environment, these assumptions are increasingly invalid. As one analysis notes, “a concentrated force may engage an isolated enemy but instead meets an enemy which can match a concentration of force with a concentration of effect”.[25] Concentration, therefore, no longer guarantees superiority; instead, it increases visibility and targetability, making forces vulnerable even while manoeuvring.[26] As a result, the traditional distinction between deep, close, and rear areas becomes increasingly blurred. Visibility and targeting capabilities extend across the entire battlespace, eroding spatial boundaries and compressing operational depth.[27]

21 Watling, “The War in Ukraine and the Future of Land Warfare”.
22 Watling, “The War in Ukraine and the Future of Land Warfare”.
23 Kofman and Kendall-Taylor, “Russian Military Strategy and Ukraine.
24 NATO, *Allied Land Tactics (ATP-3.2.1).*
25 Watling and Reynolds, *Operation Z.*
26 Kofman and Kendall-Taylor, “Russian Military Strategy and Ukraine”.
27 Watling, “The War in Ukraine and the Future of Land Warfare”.

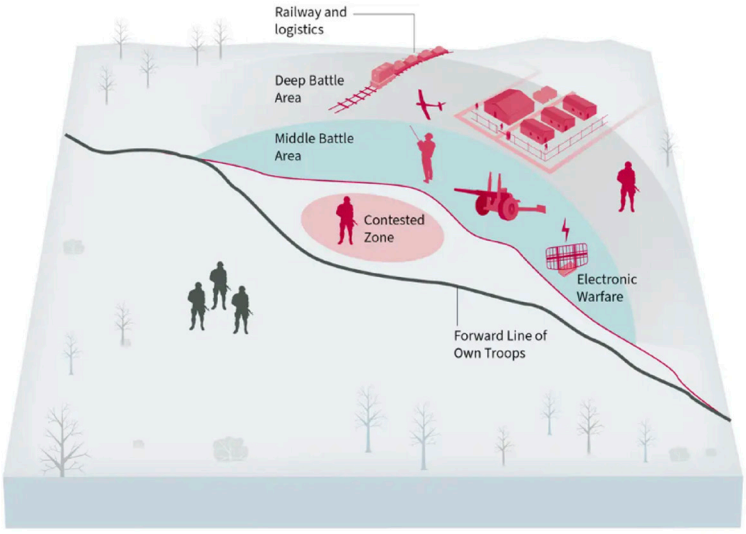
Figure 4 'Geographical Framework US Army FM-3.0 Operations'[28]



Ukrainian military planners have adapted by adopting an alternative framework. Rather than distinguishing between deep, close, and rear areas, they conceptualise the battlespace as consisting of a contested zone, a middle battle area, and a deep battle area.

28 Department of the Army, *Field Manual (FM) 3-0: Operations* (Washington, DC: Headquarters, Department of the Army, October 6, 2017), https://cyberwar.nl/d/20171005_US-Army-Field-Manual-FM-3-0-Operations.pdf

Credit/ figure 5 Ukrainian Battlefield Geometry.
Source: The author. Graphic design: Alex Whitworth Art & Design[29].



The contested zone represents an area of constant exposure and engagement, where both sides operate under persistent surveillance. The middle battle area extends beyond this zone and enables the employment of fires and sensor systems, while the deep battle area encompasses logistics, reserves, and strategic targets.[30]

This framework reflects a battlespace in which visibility extends across all layers, enabling detection and engagement far beyond traditional frontline boundaries. Integrated sensor-to-shooter networks, such as the Ukrainian DELTA system, reduce the need for rigid spatial command structures and enable more distributed and adaptive operations.[31]

29 Jack Watling, "Emergent Approaches to Combined Arms Manoeuvre in Ukraine," *RUSI Insights Paper* (London: Royal United Services Institute, October 23, 2025), https://www.rusi.org/explore-our-research/publications/insights-papers/emergent-approaches-combined-arms-manoeuvre-ukraine

30 Watling, "The War in Ukraine and the Future of Land Warfare".

31 Ministry of Defence of Ukraine, "The DELTA Combat System Has Been Deployed Across All Levels of Defence Forces of Ukraine," August 6, 2025, https://mod.gov.ua/en/news/the-delta-combat-system-has-been-deployed-across-all-levels-of-defence-forces-of-ukraine.

Although NATO doctrine recognises that the contemporary operational environment is characterised by increasing complexity and the blurring of traditional boundaries, this has not yet resulted in an alternative doctrinal framework.[32]

Force Protection and the Onion ring Analogy

These developments have important implications for force protection. NATO doctrine conceptualises protection as a warfighting function aimed at preventing or mitigating detection and threat effects in order to preserve combat power.[33] The "onion ring" analogy further expands this logic, emphasising layered survivability: ''do not be understood, do not be detected, do not be seen, do not be hit, and do not be killed''.[34]

Credit/ Image 6 AI generated, based on the article *The Onion Analogy; Understanding Multi-Domain Operations*, by Master Sgt. Brandon C. Johnson

32 NATO, *NATO Warfighting Capstone Concept* (Brussels: NATO, 2022).
33 U.S. Army, *ADP 3-0 Operations* (Washington, DC: Department of the Army, 2019).
34 Master Sgt. Brandon C. Johnson, "The Onion Analogy: Understanding Multi-Domain Operations," U.S. Army, 2021.

However, in an ISR-saturated battlefield, the outer layers – particularly avoiding detection – become decisive. If detection occurs, the compressed timeline between identification and engagement leaves little opportunity to prevent being hit or destroyed. Survivability is therefore increasingly determined before contact, rather than during engagement.

This dynamic is illustrated by NATO's 2025 exercise Hedgehog. British and Estonian units operated as if full battlefield transparency did not exist. Units moved without sufficient concealment and deployed vehicles and equipment in easily detectable positions, in which a small team of drone operators was able to render two NATO battalions combat ineffective[35]. This highlights that the decisive advantage no longer lies primarily in firepower, but in the ability to remain undetected while detecting and engaging the adversary. This should not only serve as a tactical wake-up call, but also as a military-strategic one for NATO planners tasked with the defence of the Baltic States.

35 Kuczyński, Grzegorz. 2026. "Two Battalions Destroyed? The Truth About NATO's Exercise." *Defence24*, February 14, 2026. https://defence24.com/geopolitics/two-battalions-destroyed-the-truth-about-natos-exercise

2 Strategic Implications

2.1 Eastern Sentry in the Baltic States: The Failure of the Outer Survivability Layers

The operational design of NATO's forward deterrence posture in the Baltic States is increasingly structured around the Eastern Sentry concept and its operational implementation through the Eastern Flank Deterrence Line (EFDL). 'These initiatives aim to strengthen deterrence by denial through a combination of forward-deployed forces, persistent sensing networks, autonomous systems and distributed fires capable of degrading an invading force before it reaches NATO's main formations'.[36]

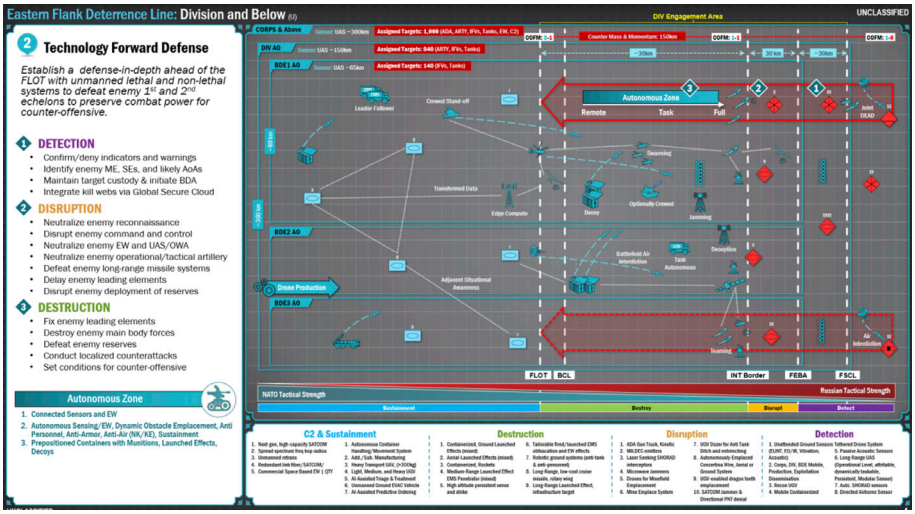
Within this concept, NATO seeks to counter Russia's advantages in geography, readiness and mass. 'The EFDL concept therefore proposes a layered operational architecture in which forward autonomous systems and sensors detect and disrupt advancing formations, while joint multi-domain operations simultaneously degrade Russian Anti-Access/Area-Denial (A2/AD) complexes in Kaliningrad, Belarus and the St. Petersburg region'.[37]

Essentially, NATO just adds another layer into their existing geographical framework, allocating an extra forward engagement area for autonomous and unmanned systems. The closer to the enemy, the more autonomous the systems are proposed to be. This is represented in the doctrinal overlay hereafter.

36 United States Army Europe and Africa (USAREUR-AF), *Transforming the Land Domain: Establishing Deterrence by Denial*, White Paper (Wiesbaden: USAREUR-AF, 2025).

37 NATO and United States Army Europe and Africa (USAREUR-AF), *Eastern Flank Deterrence Line Concept Brief*, G5 Plans Division, Munich Security Conference, 2026.

Figure 7 'Doctrinal overlay Eastern Flank Deterrence Line'[38]



Although this concept incorporates several lessons from the war in Ukraine, particularly regarding the importance of persistent ISR and unmanned systems, it still rests on a fundamental assumption inherited from classical deterrence theory: the belief that forward presence enhances deterrence by increasing credibility. Multinational deployments in the Baltic States function as a political commitment mechanism. By placing NATO troops directly in potential conflict zones, any attack on Baltic territory would automatically involve allied casualties and therefore trigger escalation under Article 5.

At the same time, efforts to reduce the vulnerability of forward deployed forces – by limiting their physical presence almost completely – may reduce the automaticity of allied involvement, thereby weakening the credibility of deterrence by punishment. This may reduce the perceived automaticity of allied involvement traditionally associated with tripwire-based deterrence models, which rely on direct allied exposure to strengthen signalling credibility.

With allied forces no longer directly exposed, the automaticity of collective involvement becomes less certain, potentially undermining reassurance and the

38 Ibid.

perceived credibility of NATO commitment. With a predominantly unmanned forward presence, an adversary may perceive that limited territorial gains can be achieved without triggering immediate allied casualties, thereby increasing the attractiveness of a fait accompli strategy.

When viewed through the survivability onion" model[39], forward deployment therefore still raises significant questions about the outer layers of survivability: *don't be understood*, *don't be detected*, and *don't be seen*. Forward presence undermines multiple outer survivability layers simultaneously: it reveals intent and our operational, defence concept ("*don't be understood*"), exposes location ("*don't be seen*"), and generates detectable signatures ("*don't be detected*").

First, forward deployments in its current form, reduce operational ambiguity. The location, composition and mission of NATO battlegroups and brigade-level formations are widely known through official announcements, exercises, open-source intelligence and satellite imagery, while many units are stationed at fixed locations in near-peacetime barracks. Rather than complicating adversary decision-making, forward presence will therefore provide relatively clear information about NATO's force posture, undermining the outer survivability layer of "*don't be seen*."

Second, forward deployments generate persistent and recognisable signatures, which increase detectability and therefore targetability. This compresses the time between identification and engagement and strengthens incentives for pre-emptive action. Modern brigade formations produce detectable emissions through command posts, communications networks, logistics nodes and electronic warfare systems.

As demonstrated in recent conflicts, such signatures can be stored in databases and rapidly detected and targeted – at a time of the adversary's choosing – through integrated ISR networks and digital battlefield systems capable of linking sensors directly to shooters. In this sense, forward presence also fails to meet the outer survivability layer of "*don't be detected*." Instead, it may produce the opposite effect: the creation of identifiable targets whose location and operational patterns can be monitored long before hostilities begin.

39 See Glossary Definitions and Terminology.

These challenges are further amplified by the geographical characteristics of the Baltic States. Estonia, Latvia and Lithuania lack strategic depth, which means the enhanced Forward Presence is located within range of Russian long-range fires, electronic warfare capabilities and ISR platforms operating from Kaliningrad, Belarus and mainland Russia. Under conditions of persistent surveillance and rapid targeting cycles, large forward formations will therefore become visible and targetable, leaving very little time to react. In this case the attacker still retains the initiative.

These dynamics become particularly problematic when considered in relation to the logic of deterrence. Classical deterrence theory assumes that forward forces increase the political cost of aggression and therefore discourage an attack. Yet under these conditions, the same deployments may simultaneously create incentives for rapid pre-emptive action, as increased visibility and targetability make it rational for an adversary to neutralise these forces early in a conflict. This dynamic does not necessarily create aggressive Russian intent itself. However, it may increase the perceived feasibility and attractiveness of rapid action once escalation is already being considered.

Forward deployments thus generate a structural trade-off: configurations that maximise political credibility tend to increase visibility and vulnerability, while configurations that reduce exposure – such as the EFDL – may weaken the signalling function of deterrence. Under conditions of persistent battlefield transparency, these objectives can no longer be optimised simultaneously.

2.2 First-Mover Incentives and the Baltic Deterrence Problem

This tension can be better understood through the concept of first-mover incentives in deterrence theory. Thomas Schelling famously argued that deterrence often relies on "tying hands"[40], reducing one's own flexibility to signal credible commitment. Forward deployments serve exactly this purpose: they make NATO's political response to aggression more predictable.

However, subsequent scholarship has demonstrated that deterrence dynamics can change significantly when actors perceive an opportunity for rapid local

40 Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966).

success. 'James Fearon and Robert Powell have shown that under conditions of uncertainty and shifting power balances, actors may initiate conflict when they believe that delaying action will worsen their strategic position'.[41]

In the Baltic context this dynamic is particularly relevant. NATO's reinforcement of the Baltic creates a security dilemma, as Russia will perceive this an increased threat. Russian planners could therefore assess that there is a narrow window of opportunity in which a rapid operation might achieve a *fait accompli*, before NATO reinforcement arrives and before the NATO mission itself expands. If forward forces are visible, detectable and geographically constrained, they may become primary targets in such a strategy. If these forces can be neutralised early, the credibility of deterrence by denial collapses at the outset of a conflict, in which case Russia may have already achieved its limited politico-military objectives.

Under these conditions, deterrence by punishment – through later escalation or reinforcement – may occur only after a local defeat has already taken place. Even if NATO retains significant escalation dominance through airpower and long-range strike capabilities, these instruments may not prevent an adversary from achieving limited territorial or political objectives in the critical early phase of a conflict. The war in Ukraine further demonstrates that once terrain has been seized and defensive positions established, reversing such gains can become highly costly, slow, and politically escalatory. Timely deterrence by denial therefore remains strategically critical.

These dynamics highlight the importance of the outer layer of the survivability model, *don't be understood*. Rather than presenting a fixed and predictable defensive posture, operational design can alternatively aim to increase uncertainty regarding the location, composition and operational role of NATO forces. Ambiguity in force posture and operational design can complicate adversary planning and reduce the attractiveness of a rapid fait accompli strategy.

Figure 8 summarises how the current EFDL-based approach interacts with the visibility–vulnerability mechanism and outlines corresponding intervention points for a revised deterrence model.

41 Fearon, "Rationalist Explanations for War"; Powell, *In the Shadow of Power*.

3 Policy implications

3.1 Rebalancing Deterrence under Conditions of Persistent Battlefield Transparency

NATO's forward posture operates within a causal chain in which increased battlefield visibility leads to detectability, targetability, compressed decision cycles, and ultimately heightened vulnerability. Policy responses should target different layers of this mechanism. The following recommendations are structured accordingly.

1. Cognitive Layer: Increase ambiguity to shape adversary decision-making

NATO should increase cognitive uncertainty in adversary decision-making by obscuring the location, composition, and readiness of its forces. This includes deception, irregular deployment patterns, distributed basing, and the deliberate obfuscation of force posture through both physical and informational means.

Increasing ambiguity disrupts the "*don't be understood*" and "*don't be seen*" layers of survivability, complicating targeting processes and weakening incentives for rapid or preemptive action. Greater operational uncertainty raises the risks of Russian miscalculation and reduces the attractiveness of a fait accompli strategy.[42] Alternatively, introducing operational ambiguity will require a strategic risk reduction strategy and a robust military-to-military liaison between NATO and Russia.

2. Detection Layer: Reduce detectability through signature management

NATO should prioritise reducing the detectability of its forces by minimising electromagnetic, thermal, and logistical signatures. This includes low-emission command-and-control systems, dispersed logistics, mobile command posts, and deception-based signature management.

42 Fearon, "Rationalist Explanations for War"; Powell, *In the Shadow of Power.*

Once detected, the compressed timeline between identification and engagement leaves limited opportunity for mitigation. Reducing detectability therefore directly weakens the link between visibility and targetability. This requires a doctrinal shift from protecting forces after detection to preventing detection altogether.

3. Targeting Layer: Break the sensor-to-shooter link

NATO should invest in capabilities that disrupt, delay, or degrade the connection between detection and engagement. This includes electronic warfare, cyber operations, decoys, spoofing, and the saturation of adversary ISR networks.

By reintroducing friction into this process, NATO can slow adversary decision cycles, increase decision-making uncertainty, and reduce the effectiveness of pre-emptive targeting. The objective is not to eliminate detection, but to prevent detection from automatically translating into engagement.

4. Posture Layer: Reconfigure forward presence while preserving credibility

NATO should restructure its forward posture to reduce physical vulnerability while preserving political credibility. Emerging concepts such as the Eastern Flank Deterrence Line (EFDL) reflect this shift by emphasising distributed sensors, autonomous systems, and networked fires in the most forward areas.

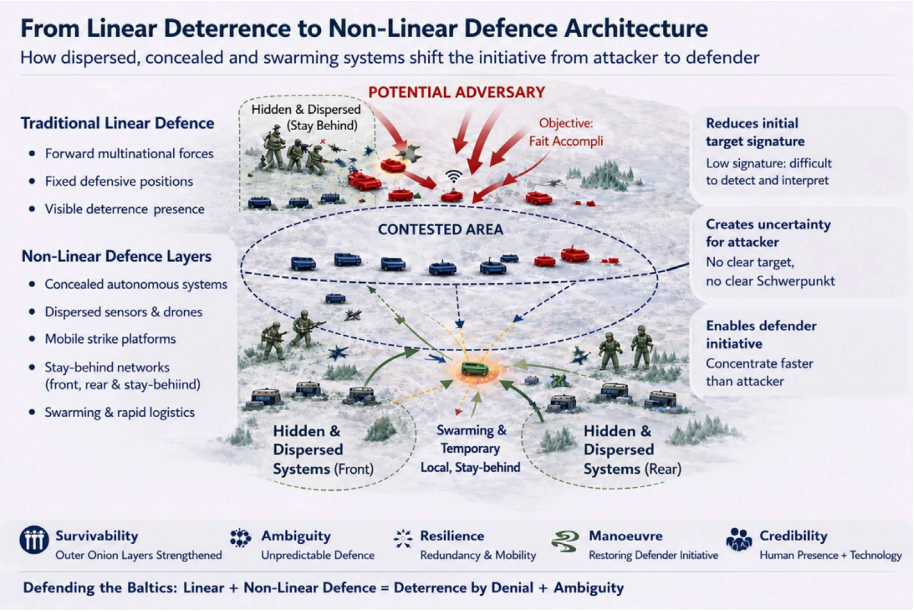
However, this approach introduces a fundamental tension between operational survivability and political credibility. An over-reliance on unmanned systems within the EFDL risks weakening deterrence by punishment. If forward presence consists primarily of unmanned assets, an adversary may perceive that limited gains can be achieved without triggering immediate allied casualties, increasing the attractiveness of a fait accompli strategy. At the same time, such systems depend on vulnerable digital and electromagnetic infrastructures, which may be degraded, disrupted, or deceived in contested environments.

NATO should therefore adopt a hybrid posture, in which distributed unmanned systems and crewed strike teams enhance deterrence by denial, while being complemented by resilient human presence, redundant command structures, and credible reinforcement capabilities.

This requires a shift from concentrated, static deployments towards the inclusion of a more distributed, modular, and partially concealed, highly mobile, non-linear

configurations, combining prepositioned equipment, rapidly deployable forces, and a limited but visible multinational presence. The objective is to decouple political credibility from physical exposure without introducing technological fragility.

Figure 8 AI-generated operations overlay; From Linear Deterrence to Non-Linear Defence Architecture

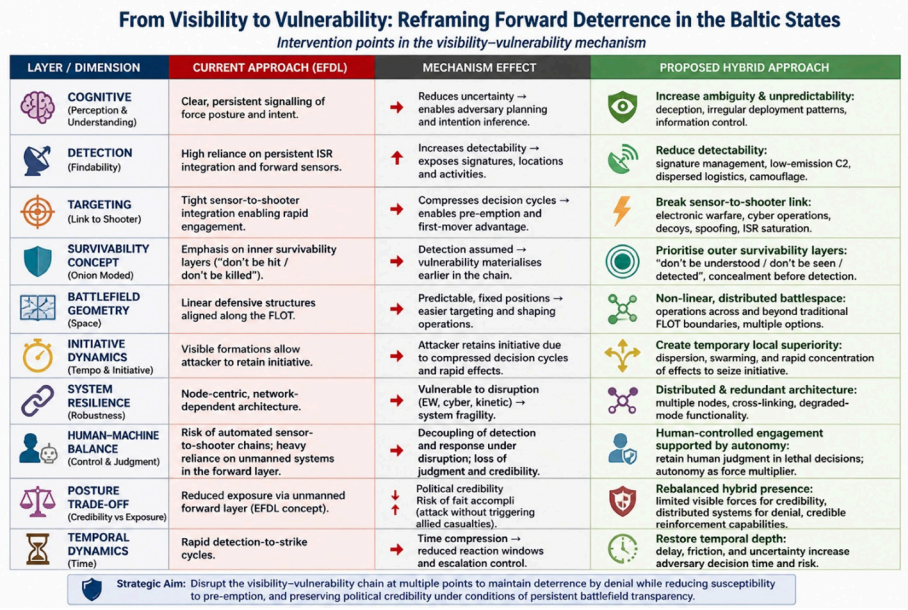


5. Temporal Layer: Restore decision-time advantage

NATO should focus on restoring temporal depth by deliberately slowing adversary targeting and decision-making processes. This can be achieved through dispersion, deception, redundancy, and the creation of multiple, interchangeable targets.

By increasing the time and effort required to identify and engage targets, NATO can reduce the feasibility of pre-emptive or fait accompli strategies. In this sense, time becomes a critical dimension of deterrence: not by accelerating one's own response alone, but by complicating and delaying that of the adversary.

Figure 8 From Visibility to Vulnerability: Reframing Forward Deterrence in the Baltic States



4 Conclusions

NATO's forward deterrence posture in the Baltic States operates under fundamentally altered conditions. Persistent battlefield transparency has transformed the relationship between visibility and survivability: as forces become more detectable and targetable, decision cycles compress and incentives for pre-emptive action increase.

Under these conditions, forward presence no longer unambiguously strengthens deterrence. Instead, it generates a structural trade-off between political credibility and operational survivability. Configurations that maximise visibility may enhance signalling, but simultaneously increase vulnerability, while efforts to reduce exposure risk weakening the perceived commitment underpinning deterrence.

Emerging concepts such as the Eastern Flank Deterrence Line partially address this challenge but introduces new risks if they rely excessively on autonomous and networked systems that remain vulnerable to disruption and may dilute political signalling.

Effective deterrence therefore depends not on maximising forward presence, but on managing the relationship between visibility, targetability, and response. NATO must shift from a logic of presence to a logic of resilience; one that reduces vulnerability while preserving credibility under conditions of persistent battlefield transparency.

Glossary Definitions and Terminology

Anti-Access/Area Denial A2/AD
A set of capabilities designed to prevent an adversary from entering or operating freely within a theatre, typically through long-range fires, air defence, and electronic warfare.

Area Framework
A conceptual structure used to organise the battlespace into distinct areas based on their function and relevance to operations (e.g. contested, middle, and deep areas). It supports planning, coordination, and the integration of effects across different parts of the operational environment.

Battlespace
The operational environment in which military activities take place, including physical and non-physical domains such as cyber and the electromagnetic spectrum.

Battlegroup (BG)
A multinational force package of approximately 1,000–1,500 personnel deployed under NATO's Enhanced Forward Presence, primarily serving a deterrence and reassurance role.

Brigade
A military formation of approximately 3,000–5,000 personnel composed of multiple battalions and supporting units.

Canalization
The shaping of the enemy's movement by restricting manoeuvre options, forcing them into predetermined avenues of approach where they are more vulnerable to engagement.

Command and Control (C2)
The processes, systems, and structures through which commanders direct and coordinate military forces.

Contested Zone
The area of direct engagement where forces are continuously exposed to detection and attack.

Delay
The tactical objective of slowing the enemy's tempo of advance while preserving own combat power and trading space for time, without becoming decisively engaged.

Denial
The prevention of enemy access to, use of, or freedom of manoeuvre within specific terrain, capabilities, or objectives.

Deterrence
The use of military and political means to discourage adversary action by shaping perceptions of cost, risk, and likelihood of success.

Deterrence by Denial
An approach to deterrence that seeks to prevent an adversary from achieving its objectives by making success operationally unfeasible.

Deterrence by Punishment
An approach to deterrence that relies on the threat of retaliation or escalation following an attack.

Dispersion
The distribution of forces across space to reduce vulnerability to detection and targeting.

Disruption
The degradation of the enemy's cohesion, synchronization, and command and control, reducing their ability to execute coordinated operations as planned.

Doctrine
A set of fundamental principles that guide military forces in the planning and conduct of operations. It provides a common framework for action while allowing for flexibility in execution.

Echelonment
The deliberate arrangement of forces in depth and/or laterally to provide mutual support, flexibility, and the ability to absorb and respond to enemy actions across multiple layers.

Enhanced Forward Presence (EfP)
Forward deployment of multinational forces in Eastern Europe intended to strengthen deterrence and reassure allied states.

Eastern Flank Deterrence Line (EFDL)
A conceptual framework for a layered and distributed defence along NATO's eastern flank, integrating sensors, autonomous systems, and networked fires.

Electronic Warfare (EW)
Military activities involving the use of the electromagnetic spectrum to detect, disrupt, or deceive adversary systems.

Fait Accompli
A rapid military action aimed at achieving objectives before an adversary can respond effectively.

Forward Line of Own Troops (FLOT)
The foremost line of friendly forces in a traditional linear defence construct.

First-Mover Incentives
Conditions under which actors are incentivised to act first in order to secure a strategic advantage.

Geographical Framework
The doctrinal division of the battlespace into deep, close, and rear areas for planning and execution purposes.

Intelligence, Surveillance and Reconnaissance (ISR)
Capabilities that collect, process, and disseminate information to support situational awareness and targeting.

ISR-Saturated Environment
An operational environment characterised by persistent sensing and reduced concealment, increasing the vulnerability of forces.

Linear Defence
A defence approach organised around relatively continuous frontlines, typically structured along a Forward Line of Own Troops (FLOT), with forces positioned to control terrain, delay or stop an advancing adversary, and provide visible territorial defence.

Loitering Munitions
Autonomous or semi-autonomous weapons systems that remain in an area until a target is identified and engaged.

Non-Linear Defence
A defence approach characterised by dispersion, flexibility, and the absence of clearly defined frontlines.

Onion Model (Force Protection)
A layered approach to survivability that prioritises avoiding detection and understanding before mitigating physical damage.

Persistent Battlefield Transparency
Continuous observation of the operational environment through integrated sensor networks.

Rear Area
The area behind frontline forces where logistics, command, and support functions are located.

Sensor-to-Shooter Networks
The integration of detection systems and strike capabilities enabling rapid targeting and engagement.

Strategic Depth
The geographic space available to absorb attacks and enable defence in depth.

Swarming
The coordinated use of multiple dispersed systems to achieve local superiority at a specific time and place.

Targeting Cycle
The process of identifying, deciding upon, engaging, and assessing targets.

Tripwire Forces
Forward-deployed forces intended to signal commitment and trigger escalation in the event of an attack, rather than to provide decisive defensive capability.

Unmanned Systems
Platforms operating without onboard human control, used for reconnaissance, logistics, or strike missions.