NATO Multidomain Operations and the Russian Active Defense Response

The North Atlantic Treaty Organization is currently locked in a techno-cognitive confrontation with the Russian Federation that has transitioned from a theoretical competition into a high-intensity struggle for electromagnetic and narrative dominance. The Alliance's shift toward Multidomain Operations (MDO) is intended to neutralize Russian Anti-Access/Area Denial (A2/AD) bubbles by rapidly converging effects across land, sea, air, space, and cyberspace. However, the Russian response has been a sophisticated evolution of "Active Defense" that prioritizes the functional destruction of NATO's command-and-control (C2) architecture. Russian Electronic Warfare (EW) troops, specifically using the Murmansk-BN and Krasukha-4 systems coordinated by the AI-driven Bylina station, have demonstrated the capability to degrade NATO's Link-16 data links and Joint All-Domain Command and Control (JADC2) nodes by seventy to ninety percent within a three-hundred-kilometer radius. Furthermore, Russian cognitive warfare assets, amplified by state-sponsored influencers like Boris Rozhin, are systematically exploiting perspective distortions to frame NATO's defensive posture as a precursor to an "Integrated Massive Air Strike" (IMVU), effectively mobilizing domestic sentiment for a preemptive "Initial Period of War" (NPY) strike. Future escalation paths are trending toward a high-intensity "Gray Zone" campaign culminating in a regional fait accompli attempt on NATO's northeastern flank, where Russian forces will likely use technical surprise and narrative manipulation to paralyze Allied decision-making during the critical first forty-eight hours of conflict.[1]

Technical Dissection and Cognitive Mapping of the Baltic Strategic Narrative

A clash of divergent operational philosophies currently defines the tactical landscape of the Baltic theater. At the center of this friction is the Lithuanian perspective on NATO's transition to Multidomain Operations, a doctrine that seeks to unify the five warfighting domains into a singular, high-tempo engine of destruction.[1] An analysis of the text provided by Major Donatas Palavenis, a chief specialist in the Lithuanian Armed Forces, provides a granular look at how frontline states are absorbing this paradigm shift. The text is technically rigorous, correctly identifying the United States as the lead architect of MDO and the primary source of the five Multidomain Task Forces (MDTF) currently being stood up to support theater commanders in the Pacific and Europe.[1] Palavenis highlights the criticality of the Combined Joint All-Domain Command and Control (CJADC2) initiative, which aims to create a universal data-sharing architecture that allows for the seamless transfer of sensor data to the most effective shooter, regardless of the branch of service.[6]

Copyright 2026



However, applying Treadstone 71's Perspective Distortion Analysis (PDA-2) reveals that the Palavenis text functions as more than a technical brief; it is a cognitive instrument designed to establish a sense of inevitability regarding NATO's technical overmatch.[6] The narrative compels smaller NATO members to prioritize interoperability with US systems, effectively ceding a degree of national tactical autonomy in exchange for the promise of collective survivability.[1] The satisfies the "Justification Narrative" cluster, where the complexity of the threat is used to legitimize the massive capital outlays required for digital modernization.[6]

The technical accuracy of the Baltic narrative is reinforced by its alignment with observed US Army deployments in Wiesbaden, Germany, where the 2nd Multidomain Task Force is actively integrating long-range precision fires (LRPF) with cyber and space assets.[8] Palavenis correctly notes that successful MDO implementation requires not just military synchronization but a "whole-of-government" approach, involving economic, legal, and political pressure tools.[1] The reflects the high-level NATO consensus that modern conflict occurs across the entire "competition-conflict spectrum".[10]

Narrative Marker	Technical Detail	Cognitive Strategic Intent
Domain Convergence	Integration of air, land, sea, space, and cyber.[1]	Establishment of NATO technical inevitability.
C2 Architecture	CJADC2 and Link-16 data link reliance.[7]	Consolidation of U.S.-led command hierarchies.

Copyright 2026

Target Identification	AI-driven sensor-to-shooter loops.[12]	Psychological reassurance of strike precision.
Operational Stages	Phased national resource optimization.[6]	Budgetary alignment toward Western platforms.

In stark contrast, the Russian cognitive environment, dominated by influencers like Boris Rozhin (Colonel Cassad), reinterprets these NATO developments through the lens of historical grievance and existential threat.[13] Using the Treadstone 71 Narrative Convergence Analysis (NCA) technique, it becomes clear that Rozhin's messaging aligns perfectly with the Russian General Staff's "Integrated Massive Air Strike" (IMVU) fear.[6] Rozhin frames the MDTF deployments not as defensive tripwires, but as decapitation platforms designed to conduct a "planetary or non-contact war" against the Russian homeland.[15] The cognitive manipulation uses "memory entrepreneurs" to equate NATO's technical integration with 20th-century fascism, creating a powerful emotional trigger that justifies Russia's "Active Defense" measures.[13]

The Russian Strategic Counter- Active Defense and the Initial Period of War

The Russian Federation does not view NATO's Multidomain Operations as a defensive framework; it perceives it as a refined methodology for an offensive blitzkrieg designed to annihilate Russian fighting forces and decapitate the political-military leadership.[15] The response to this perceived threat is codified in the doctrine of "Active Defense" (*aktivnaya oborona*), a strategic construct that merges defensive posture with preemptive offensive action.[5] Under the leadership of General Valery Gerasimov, the Russian military has prioritized the "Initial Period of War" (NPY), operating under the assumption that the first forty-eight to ninety-six hours of conflict will decide the outcome of the entire campaign.[18]

Active Defense represents a significant departure from Soviet-era attrition models. Instead of relying on massed ground forces to absorb NATO strikes, the Russian military has reversed its internal hierarchy, elevating the aerospace and information spheres to the top of its strategic priorities.[16] The "defensive-offense" relies on three core operational concepts-

1. **Functional Destruction of C4ISR-** Russia focuses on neutralizing NATO's ability to coordinate its multidomain effects, a focus that is not about killing every soldier, but about destroying the "nervous system" of the NATO task force—its radars, satellites, and command centers.[5]

2. **Maneuver Defense-** Russian ground forces are trained to trade space for time, using mobile formations to attrite NATO's offensive momentum while preserving their own combat power for a high-intensity counteroffensive.[5]
3. **Strategic Operations to Repel Aerospace Aggression (SOPVKN) - The defensive construct involves a massive, coordinated effort among** air defense units, EW brigades, and long-range precision fires to disrupt NATO's "Integrated Massive Air Strike" before it can achieve its objectives.[16]

The Russian General Staff believes that by inflicting "unacceptable damage" on NATO's high-value assets and critical infrastructure during the NPY, they can force the Alliance into a conflict with high levels of attrition that Western political structures are ill-equipped to sustain.[5] The strategy is inherently asymmetric, recognizing that Russia is conventionally the weaker party and must therefore rely on "non-standard" innovations to create surprise and exploit NATO's technological dependencies.[16]

Strategic Component	Operational Objective	Tactical Method
Initial Period of War (NPY)	Seize the strategic initiative.[20]	Preemptive strikes on C2 nodes.[5]
Systems Warfare	Disorganize the NATO kill chain.[22]	Saturation of sensors with EW.[21]
Forceful Deterrence	Force war termination on Russian terms.[16]	Hypersonic Kinzhal strikes on infrastructure.[16]
Non-Contact Warfare	Minimize Russian casualties while maximizing fire.[16]	Stand-off precision munitions and UAVs.[16]

The Electromagnetic Siege- Neutralizing NATO's Digital Umbilical Cord

Russian military planners have correctly identified NATO's greatest strength—its hyper-connectivity—as its most significant vulnerability. Multidomain Operations depend on a "digital umbilical cord" that connects the forward observer to the hypersonic battery and the theater commander.[7] If this cord is severed, the MDO machine collapses into a collection of isolated units incapable of synchronized action. To achieve this, Russia has deployed a mature and highly integrated Electronic Warfare (EW) ecosystem that is currently unmatched by individual European NATO members.[21]

Copyright 2026

The Technical Trinity- Murmansk-BN, Krasukha-4, and Bylina

The backbone of the Russian electromagnetic counter-MDO strategy is the integration of long-range, automated suppression systems. The Murmansk-BN is a strategic EW complex comprising seven Kamaz trucks with 32-meter-high antennas.[2] It is capable of conducting electronic surveillance and high-frequency (HF) jamming at ranges up to five thousand kilometers, specifically targeting the HFGCS and NATO Link-16 communications that are essential for long-range C2.[26] In the Baltic theater, a Murmansk-BN unit stationed in Kaliningrad can theoretically silence HF communications across northern Poland and the Baltic states.[27]

Complementing the Murmansk-BN is the Krasukha-4, an operational-level mobile platform designed to neutralize aerial threats and disrupt enemy AWACS (Airborne Warning and Control System) and satellite links.[2] The Krasukha-4 operates across the X, Ku, and S-bands, creating an electromagnetic shield that blinds NATO aircraft and prevents them from providing real-time target data to the MDTFs.[2]

The critical multiplier for these systems is the RB-109A Bylina, an AI-driven automated control system for EW brigades.[2] Bylina can independently analyze the entire electromagnetic spectrum in real-time, identify enemy emissions, and coordinate multiple EW stations to suppress them with surgical precision.[2] The prevents the "fratricide" of friendly signals, a recurring problem in Russian operations during the early phases of the Ukraine invasion.[2]

A2/AD Bubbles and Information Denial

These EW systems are the "invisible hammer" that supports the kinetic A2/AD bubbles created by S-400 and Bastion systems.[23] The tactical goal is "Information Denial," where NATO forces are prevented from accessing the theater of operations through a combination of physical interceptors and electronic noise.[30] The Russian EW capability is deeply embedded into their military doctrine, often paired with artillery strikes in a "find-to-suppress" cycle where SIGINT (Signals Intelligence) units locate NATO emitters and immediately trigger fire missions.[21]

EW System	Operational Tier	Primary Target	Demonstrated Range
Murmansk-BN	Strategic	HFGCS/Link-11/Link-16.[26]	5,000 km.[27]
Krasukha-4	Operational	AWACS/J-STARS/Satellites.[2]	300 km.[2]

Copyright 2026

Bylina	Brigade C2	AI-driven optimization of EW stations.[2]	Theater-wide.[2]
Leer-3	Tactical	Cellular networks/UAV hijacking.[2]	6 km (Orlan-10 radius).[2]
Rtut-2	Protective	Neutralizing radio-fused munitions.[2]	0.5 sq km (Defensive dome).[2]

The rapid modernization of these systems, including the deployment of the Borshchevik platform to target Starlink modems, indicates a relentless Russian focus on neutralizing Western satellite-based connectivity.[2] The Russian EW Troops have achieved a state of "Spectrum Dominance" that threatens to render NATO's technologically advanced platforms blind, deaf, and mute in the initial period of war by 2025.[4]

Adversarial Cognitive Simulation (ACS)- Reconstructing the Kremlin's Strategy

Understanding the Russian response to MDO requires moving beyond static capability assessments and reconstructing the cognitive frameworks that drive their strategic choices. Treadstone 71's Adversarial Cognitive Simulation (ACS) provides a structured method for modeling how the Russian General Staff perceives threats, risks, and opportunities under the pressure of a NATO multidomain buildup.[6]



Step 1- Reconstructing the Russian Worldview

The Russian leadership interprets the global security environment through a lens of "Strategic Encirclement" and historical grievance.[6] They believe that the post-Cold War rules-based order is a mechanism for Western hegemony and that NATO's eastward expansion is a deliberate attempt to neutralize Russia's sovereign influence.[18] Power is perceived as a zero-sum game, and legitimacy is derived from domestic stability and the ability to project force in the "near abroad".[6]

Step 2- Identifying Core Strategic Fears

The Russian General Staff is driven by two primary fears that dictate their "Active Defense" requirements-

1. **C2 Decapitation-** The fear that a US "Prompt Global Strike" or NATO multidomain assault will neutralize the national command hierarchy and the strategic nuclear deterrent before a response can be authorized.[16]
2. **Internal Instability (Color Revolutions)-** The fear that Western influence operations and economic coercion will trigger domestic unrest, leading to regime change.[6]

Step 3- Mapping Strategic Goals

The Kremlin's primary goals remain stable-

- The fracturing of NATO cohesion through separate diplomatic accommodations.[3]
- The establishment of a multipolar international system in which Russia is recognized as a great power.[31]
- The secure control of "buffer zones" in former Soviet territories to prevent NATO encroachment. [31]

Step 4- Cognitive Bias and Stress Modeling

The Russian decision-making process is heavily influenced by "Loss Aversion".[6] They are fundamentally more willing to accept military risks—including the risk of conventional escalation with NATO—to avoid the perceived loss of Ukraine or the Baltics to Western influence.[6] The leads to an "Escalation Bias," where Russian leaders continue aggressive gray-zone activities despite the risk of an Article 5 trigger, believing that the costs of inaction are greater than the costs of confrontation.[3]

Step 5- Game-Theoretic Decision Analysis

In a scenario where NATO positions an MDTF near the Suwalki Gap, the Russian ACS decision tree predicts a high probability of an asymmetric response rather than a direct conventional match.[6]

Scenario- NATO MDTF Buildup	**Option 1- Conventional Buildup**	**Option 2- Diplomatic Protest**	**Option 3- Asymmetric Suppression**

Russian Response	Deploy the 1st Guards Tank Army.	UN Security Council veto.	Pulsed EW and Cyber Sabotage.
Probability	30%	10%	60%
Rationale	Costly and predictable.	Low strategic payoff.	Low attribution, high disruption.

The simulation identifies "Option 3" as the Russian preference, leveraging their EW and cyber supremacy to create a "Contested Information Environment" that prevents NATO from achieving domain convergence.[21]

Cyber Adversary Reflex Mapping (CARM)- Predicting the Tactical Pivot

While ACS models the strategic mindset, Cyber Adversary Reflex Mapping (CARM) identifies the instinctive, near-automatic responses of Russian tactical units to specific operational stimuli.[6] Russian cyber and EW units have developed pre-existing "reflex pathways" based on over a decade of conflict in Ukraine and Syria.[24]

Step 1- Trigger Identification

Historical data points to specific NATO actions that force a Russian reflexive reaction-

- **Stimulus A-** High-profile public attribution of a Russian cyber campaign (e.g., the DNC hack).[34]
- **Stimulus B-** Forward deployment of NATO Aegis Ashore or MDTF units in Poland/Germany.[8]
- **Stimulus C-** Targeted sanctions on Russian microelectronic procurement.

Step 2- Reaction Pattern Analysis

Analysts have observed that Russian units reflexively shift their "Hosting Infrastructure" and "Encryption Protocols" within hours of a major infrastructure takedown.[6] For example, when pro-Russian ransomware groups are disrupted, they consistently fragment into smaller, task-specific cells before rebranding and resurfacing within sixty days.[6]

Step 3- Behavioral Forecasting for MDO

If NATO activates a high-intensity Link-16 network during a Baltic exercise, the CARM model predicts the following Russian reflex-

1. **Automated Spectrum Reconnaissance-** Bylina stations immediately identify the specific frequencies and sequencing of the NATO link.[2]
2. **Pulsed Jamming-** Murmansk-BN executes high-power, intermittent bursts to disrupt synchronization without revealing the station's precise location for prolonged periods.[26]
3. **Narrative Flooding-** Social media bots amplify claims that NATO is using the exercise to hide a "decapitation" attempt, inducing caution in Western civilian leaders.[35]

Step 4- Counteraction Planning

CARM allows NATO planners to design "reflex traps." NATO can lure Russian EW units into activating their high-power emitters, which can then be triangulated and targeted by kinetic fires by intentionally emitting specific electronic signatures.[6] The "SEAD-CEMA integration" is critical for penetrating the Russian A2/AD shell.[37]

NATO Action (Stimulus)	Predicted Russian Reflex	Preemptive Countermeasure
JADC2 Activation	High-frequency noise injection.[26]	Frequency-hopping and directional antennas.[21]
Satcom Links	Borshchevik Starlink suppression.[2]	Redundant fiber-optic and UAV relays.[11]
Armor Movement	Orlan-10 drone reconnaissance.[28]	Mobile EW screens and thermal camouflage.[38]

Adversary Threat Vector Analysis (ATVA)- The Hybrid Offensive

Russian strategy against MDO is not confined to the battlefield; it is a multidomain, hybrid offensive targeting the structural weaknesses of the entire NATO alliance. Treadstone 71's Adversary Threat Vector Analysis (ATVA) maps these pathways before they materialize into full-scale conflict.[6]

Cyber and Technological Vectors

The Russian military has shifted away from building a single, all-encompassing C2 architecture, opting instead for tactical, task-specific software that solves concrete battlefield problems.[12] The

makes their C2 more resilient to Western cyber-attacks because it lacks a central "brain" to decapitate.[12] Key vectors include-

- **Supply Chain Poisoning-** Inserting vulnerabilities into the microelectronics used by small NATO countries through front companies in the "Gray Market" [[6] Page 124, S_S130].
- **AGCP (Adversarial Generative Code Poisoning)-** Corrupting the training datasets for NATO's AI-driven target recognition systems, ensuring they fail in real-world conditions.[6]

Psychological and Human Terrain Vectors

Using Human Terrain Influence Mapping (HTIM), Russia identifies "ideological divides" within populations in the Baltic and Central Europe.[6] They target demographic segments with historical grievances, using deepfake technology and bot networks to amplify social polarization and erode trust in NATO institutions.[36] The is designed to create "internal paralysis" during a crisis, where civilian unrest prevents the rapid deployment of national defense forces.[3]

Geopolitical and Economic Vectors

Russia uses "Energy Blackmail" and "Trade Restrictions" as instruments of economic coercion, specifically targeting nations that provide logistical support for the MDTFs. The Kremlin seeks to influence NATO leaders' political calculus by making the costs of military intervention appear unsustainable through energy supply manipulations to Europe.

Domain	Vector	Tactic	Projected Impact
Cyber	Infrastructure.[41]	Viasat KA-SAT management compromise.	Total SATCOM blackout in theater.
Psychological	Narrative.[36]	"NATO Occupier" disinformation campaign.	Grassroots protests at MDTF bases.
Economic	Dependency.	Restricting rare earth/neon exports.	Stalling of NATO munitions production.
Geopolitical	Alliance.[3]	Diplomatic peeling of "vulnerable states."	Breakdown of Article 5 consensus.

Copyright 2026

Perspective Distortion and Cognitive Dissonance in Information Warfare



The information domain is where Russia most effectively challenges NATO's Multidomain Operations. Applying Perspective Distortion Analysis (PDA-2) reveals that the Kremlin has successfully created an "alternative reality" for its domestic audience and key international partners.[6]

The NPY Perception Paradox

In the Russian worldview, the Initial Period of War is a life-or-death struggle against a "Fascist NATO" aggressor.[13] The creates a state of "Cognitive Dissonance" when compared to NATO's actual capability—while European NATO excels in air superiority, it lacks the armored depth and artillery volume for a credible offensive against the Russian Federation.[4]

Using Cognitive Dissonance Mapping (CDM), analysts can identify the gaps-

- **Stated Position-** NATO is a defensive alliance committed to the territorial integrity of its members. [42]
- **Observed Behavior-** NATO is deploying long-range missiles to Wiesbaden and conducting multidomain strikes near Russian borders.[8]
- **Russian Dissonance Rating-** Extreme.[6] The Kremlin interprets the behavior as offensive, disregarding the stated defensive intent.

Narrative Convergence and Digital Dehumanization

Russia uses Narrative Convergence Analysis (NCA) to detect unnatural alignment between Western media outlets and NATO policy, which it then frames as "totalitarian propaganda" to its own population.[13] The digital warfare lends an "aesthetic dimension" to the conflict, where infographics on body counts and digital mashups are used to dehumanize the opponent.[39] The is a core component of "New Generation Warfare," intended to destabilize the adversary's internal stability through "controlled chaos".[32]

Decompositional Uncertainty Mapping (DUM)- Evaluating the Unknowns

Uncertainty is a constant in a theater as complex as the Baltic Northeast Corridor. Treadstone 71's Decompositional Uncertainty Mapping (DUM) allows analysts to categorize these unknowns to focus intelligence collection and refine probabilistic forecasting.[6]

Tier 1- Confirmed Variables (High Confidence)

- Russian EW supremacy and the deployment of Murmansk-BN in Kaliningrad.[2]
- The stationing of a US MDTF in Wiesbaden, Germany.[8]
- The transition of the Russian military to an AI-enhanced, decentralized C2 hierarchy using Astra Linux.[12]
- NATO's 2025 transition to a 5% of GDP spending target for core defense and critical infrastructure.[45]

Tier 2- Partially Known Factors (Medium Confidence)

- The true effectiveness of NATO's "FrankenSAM" hybrids (Western missiles on Soviet launchers) against modern Russian aircraft.[37]
- The extent of Russian-Iranian technical cooperation regarding the production of the Shahed-136/Geran-2 drone in Alabuga.[46]
- The resilience of the European 155mm ammunition supply chain under high-intensity theater consumption.[4]

Tier 3- Complete Unknowns (Low Confidence)

- The exact "Red Line" for Russian tactical nuclear use in response to a conventional multidomain strike on its C2.[18]
- The existence of hidden "Sleeper Malware" in the power grids of small NATO countries, intended for activation during the NPY.[6]
- The degree to which "Loss Aversion" would cause the Kremlin to launch a suicidal fait accompli in the event of a perceived internal regime threat.[3]

Uncertainty Category	Intelligence Factor	Confidence	Collection Priority
Tier 1 (Known)	Russian EW station locations in MD.[28]	High	Low - Monitor movements.

Tier 2 (Partial)	NATO Link-16 resilience vs. Bylina.[2]	Medium	High - Technical ELINT.
Tier 3 (Unknown)	Threshold for Russian nuclear escalation.[18]	Low	Highest - Strategic HUMINT.

Using Bayesian Probability Updates, the probability of a Russian fait accompli in the Baltics increases as Tier 2 uncertainties regarding NATO's C2 resilience are resolved in Russia's favor.[6] If NATO's data links are proven to be vulnerable to Murmansk-BN suppression, the likelihood of a Russian "Active Defense" offensive rises from thirty percent to sixty-eight percent.[6]

Causal Density and Systemic Vulnerability- The CDM-2 Matrix

Causal Density Mapping (CDM-2) identifies which variables exert the most systemic influence on the outcome of a NATO-Russia conflict.[6] Analysts can pinpoint the "High-Density Nodes" where a small shift triggers a large effect by visualizing the interdependencies.

The analysis reveals that **"Information Dominance during the NPY"** has the highest density.[21] If Russia achieves ninety percent degradation of NATO communications during the first forty-eight hours, it triggers a cascade of secondary effects-

1. **Tactical Disorientation-** MDTF units become incapable of synchronized strikes.[23]
2. **Leadership Paralysis-** Political leaders in Brussels and Washington receive conflicting or delayed reports, preventing an Article 5 consensus.[3]
3. **Domestic Panic-** Russian-amplified disinformation narratives go unchallenged in the absence of verified NATO communications, eroding the will of Baltic populations to fight.[36]

Causal Node	Total Influence Score (1-5)	Primary Systemic Effect
EW Information Denial	5	Total paralysis of multidomain synergy.[21]
Link-16 Integrity	4	The foundation of NATO strike precision.[7]

Gray Zone Sabotage	3	Disruption of European logistical flows.[40]
Regime Loss Aversion	4	Accelerator of preemptive escalation.[6]

The interaction of these nodes suggests that Russia's "Active Defense" is specifically engineered to exploit the electromagnetic spectrum's high causal density. The Kremlin can effectively "de-integrate" the entire NATO multidomain machine by striking this single node.[21]

Escalation Paths and Cones of Plausibility

The future of NATO-Russia stability depends on the interplay between NATO's multidomain integration and Russia's asymmetric adaptation. Using the Cones of Plausibility, we forecast three primary trajectories for the next thirty-six months.

Cone 1- The Permanent Gray Zone (Most Plausible)

In this scenario, Russia maintains its current trajectory of high-intensity hybrid warfare. The threat involves a continuous campaign of cyber-attacks on critical infrastructure, GPS jamming of civilian air traffic, and deniable sabotage operations across Europe.[36] The goal is to raise the political and economic costs of NATO's presence in the Baltics while avoiding a full-scale conventional war that Moscow believes it cannot win in the long term.[31] Russia uses the "Dispersion Paradox," where its forces adapt to NATO drone superiority through radical dispersion, leading to a positional stalemate that exhausts NATO's munitions and political resolve. [18]

Cone 2- The Suwalki Fait Accompli (High-Risk Plausible)

A sudden shift in US priorities or internal NATO disputes (e.g., over Greenlandic sovereignty or defense burden-sharing) leads to a perception of Alliance fragility.[3] Russia launched a rapid, high-intensity offensive to seize the Suwalki Gap, using its EW supremacy to create a "Blackout Zone" that isolates the Baltic states.[3] The operation establishes a fait accompli within seventy-two hours, using unmarked forces and proxies to complicate attribution.[3] NATO is forced to choose between a potentially nuclear escalation to retake the territory or accepting a new geopolitical reality that marks the end of the Alliance's credibility.[3]

Cone 3- Multidomain Deterrence Stabilization (Least Plausible)

NATO successfully implements a decentralized, "loose" command structure that can function under intense EW suppression.[33] The deployment of resilient, low-cost sensor-shooter networks

and "FrankenSAM" hybrids effectively penetrates Russian A2/AD bubbles.[37] Recognizing that its asymmetric advantages have been neutralized, the Kremlin pivots toward a more transactional diplomatic approach, agreeing to theater-range missile moratoriums and de-escalation zones in the Baltic.[8] The requires NATO to maintain a credible conventional mass that Russia cannot "out-asymmetrize".[4]

Strategic Synthesis and Expert Conclusions

The evidence indicates that the primary battlefield of the 21st century is no longer just the physical "Suwalki Gap," but the "Cognitive and Electromagnetic Gaps" that exist within the NATO alliance.[21] NATO's Multidomain Operations, while technically superior on paper, depend on a digital infrastructure that is currently being systematically targeted by Russian "Active Defense" capabilities.[21]

The Technical Asymmetry

Russian EW Troops have moved beyond simple jamming to achieve "Degradation Dominance" through the integration of AI-driven control systems like Bylina.[2] The allows Russia to neutralize NATO's information advantage at the exact moment it is most needed—the Initial Period of War.[2] NATO's reliance on U.S.-led technical enablers creates a strategic vulnerability; if the US is distracted in the Indo-Pacific, European NATO currently lacks the independent EW and ISR depth to counter a Russian multidomain surge.[4]

The Cognitive Threshold

The Russian information ecosystem has successfully weaponized the "Memory of Fascism" to mobilize its population for a long-term standoff.[13] The effort is not merely a propaganda effort but a systematic cognitive warfare campaign designed to "soften" the targets through narrative manipulation and digital dehumanization.[36] NATO's failure to recognize and counter these perspective distortions has allowed the Kremlin to maintain the strategic initiative in the "Gray Zone".[32]

Operational Recommendations for Analytic Dominance

To achieve "Analytic Dominance" and maintain a credible deterrence, NATO must-

1. **Implement Loose Command Structures-** Move away from centralized, "brittle" C2 nodes toward a decentralized model that allows tactical commanders to operate independently under communication blackouts.[7]

Copyright 2026

2. **Harden the Electromagnetic Spectrum-** Mandate open-architecture and interoperability standards for all NATO EW and data link systems, ensuring that future assets are "integrated by design" to withstand Russian suppression.[21]
3. **Neutralize the AI-EW Nexus-** Focus research on Adversarial Generative Code Poisoning (AGCP) to disrupt the machine-learning models that govern systems like Bylina, rendering Russian automated suppression ineffective.[2]
4. **Embrace Total Defense-** Small NATO members must adopt a "whole-of-society" defensive model that includes psychological inoculation against Russian disinformation and the hardening of national economic infrastructure against hybrid sabotage.[50]

The "Dispersion Paradox" of the Ukraine war serves as a final warning- technological adaptation is a race, not a destination.[38] Russian forces may have already evolved to exploit their inherent dependencies by the time NATO fully implements its current MDO doctrine. Continuous, intelligence-driven refinement using Treadstone 71 techniques is the only way to ensure that the Alliance remains several moves ahead on a chessboard already rigged for asymmetry.[6]

Copyright 2026

Works cited

1. Options for Small NATO Countries to Prepare for Multidomain Operations, accessed March 10, 2026, https-//smallwarsjournal.com/2022/06/16/options-small-nato-countries-prepare-multi-domain-operations/
2. Russia's Electronic Warfare Supremacy in 2025- Technological Innovation, Geopolitical Implications and Global Security Dynamics - https-//debuglies.com, accessed March 10, 2026, https-//debuglies.com/2025/04/15/russias-electronic-warfare-supremacy-in-2025-technological-innovation-geopolitical-implications-and-global-security-dynamics/
3. Russian Threats to NATO's Eastern Flank- Scenarios, Strategy, and Policy for European Security | The Belfer Center for Science and International Affairs, accessed March 10, 2026, https-//www.belfercenter.org/research-analysis/russia-nato-baltics-scenarios-europe-security
4. EXCLUSIVE REPORT - European Conventional Military Capabilities as a Threat to Russia- A Comparative Assessment in 2025 - https-//debuglies.com, accessed March 10, 2026, https-//debuglies.com/2025/11/19/exclusive-report-european-conventional-military-capabilities-as-a-threat-to-russia-a-comparative-assessment-in-2025/
5. Russian Military Strategy- Core Tenets and Operational Concepts - CNA.org., accessed March 10, 2026, https-//www.cna.org/reports/2021/10/Russian-Military%20-Strategy-Core-Tenets-and-Operational-Concepts.pdf
6. All Combined.pdf
7. Comparing JADC2 Interoperability And Organizational Processes Between US And Russian Military Forces - Air University, accessed March 10, 2026, https-//www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/2940563/comparing-jadc2-interoperability-and-organizational-processes-between-us-and-ru/
8. American Missiles and Russian Dachas- Tomahawk and the Future of Stability and Deterrence in Europe - Foreign Policy Research Institute, accessed March 10, 2026, https-//www.fpri.org/article/2025/10/tomahawk-and-the-future-of-stability-and-deterrence-in-europe/
9. Germany pursues multi-pronged quest for long-range missiles - Defense News, accessed March 10, 2026, https-//www.defensenews.com/global/europe/2025/09/26/germany-pursues-multi-pronged-quest-for-long-range-missiles/
10. A Comparison of Operational Arts- What NATO Stands to Learn by Looking Outside of Europe, accessed March 10, 2026, https-//www.cfc.forces.gc.ca/papers/csc/csc50/mds/King.pdf
11. Taking Multidomain Operations from Theory to Practice - Istituto Affari Internazionali (IAI), accessed March 10, 2026, https-//www.iai.it/sites/default/files/iai2601.pdf
12. How Russia Is Reshaping Command and Control for AI-Enabled Warfare - CSIS, accessed March 10, 2026, https-//www.csis.org/analysis/how-russia-reshaping-command-and-control-ai-enabled-warfare

Copyright 2026

13. World War II 2.0- Digital Memory of Fascism in Russia in the Aftermath of Euromaidan in Ukraine - Semantic Scholar, accessed March 10, 2026, https-//pdfs.semanticscholar.org/6b5c/c0e00450074cce322ca29b7852b05cf4c604.pdf

14. War on All Fronts- - NATO Strategic Communications Centre of Excellence, accessed March 10, 2026, https-//stratcomcoe.org/publications/download/War-on-All-Fronts-DIGITAL.pdf

15. Download the first - Irsem, accessed March 10, 2026, https-//www.irsem.fr/storage/file_manager_files/2025/03/en-vortex-n-1-int-gral.pdf

16. Russian and Chinese multidomain approaches- the same aerospace battle? - Irsem, accessed March 10, 2026, https-//www.irsem.fr/storage/file_manager_files/2025/03/4-russian-and-chinese-multi-domain-approaches.pdf

17. Full article- Social media users in search of 'facts'- the Trade Union House fire case, accessed March 10, 2026, https-//www.tandfonline.com/doi/full/10.1080/19409419.2021.1893212

18. The Shooting Party- Russia's Evolving Threat Perceptions Since 2022 - CNA.org., accessed March 10, 2026, https-//www.cna.org/reports/2025/09/The-Shooting-Party-Russia-Evolving-Threat-Perceptions-Since-2022.pdf

19. Russian Military Strategy- Core Tenets and Operational Concepts | CNA, accessed March 10, 2026, https-//www.cna.org/reports/2021/08/Russian-Military-Strategy-Core-Tenets-and-Operational-Concepts.pdf

20. Russia's Conduct of War- How and with What Assets - DTIC, accessed March 10, 2026, https-//apps.dtic.mil/sti/trecms/pdf/AD1133627.pdf

21. Electromagnetic Warfare- NATO's Blind Spot Could Decide the Next Conflict | RAND, accessed March 10, 2026, https-//www.rand.org/pubs/commentary/2025/11/electromagnetic-warfare-natos-blind-spot-could-decide.html

22. Rose - Returning Context to Our Doctrine - Army University Press, accessed March 10, 2026, https-//www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2023-OLE/Returning-Context-to-Our-Doctrine/

23. NATO Command and Control Resilience in Contested Environments, accessed March 10, 2026, https-//www.japcc.org/essays/nato-command-and-control-resilience-in-contested-environments/

24. Russia's Electronic Warfare Capabilities to 2025 - International Centre for Defence and Security, accessed March 10, 2026, https-//icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf

25. The Invisible Battlefield- A Technology Strategy for US Electromagnetic Spectrum Superiority - AWS, accessed March 10, 2026, http-//media.hudson.org.s3.amazonaws.com/Clark%20Walton%20Tourangeau_The%20Invisible%20Battlefield%20A%20Tech%20Strategy%20for%20US%20Electromagnetic%20Spectrum%20Superiority.pdf

26. Israel tracks Russian EW systems in Iran - Raksha Anirveda, accessed March 10, 2026, https-//raksha-anirveda.com/deployment-of-advanced-russian-ew-systems-in-iran-being-watched-closely-by-israel/

Copyright 2026

27. Russia's Evolution Toward a Unified Strategic Operation- The Influence of Geography and Conventional Capacity - RAND, accessed March 10, 2026, https-//www.rand.org/content/dam/rand/pubs/research_reports/RRA1200/RRA1233-8/RAND_RRA1233-8.pdf

28. Return of Ground-Based Electronic Warfare Platforms and Force Structure, accessed March 10, 2026, https-//www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2019/Spring-Glace-Electronic-Warfare/

29. Battlefield Mobile Location Tracking Insights | PDF | Radio | Cellular Network - Scribd, accessed March 10, 2026, https-//www.scribd.com/document/774254047/ENEA-Tracking-on-the-Battlefield-Report-Full-Report

30. Russian and Chinese Multidomain Strategies | PDF | People's Liberation Army - Scribd, accessed March 10, 2026, https-//www.scribd.com/document/803222960/4-russian-and-chinese-multi-domain-approaches

31. RUSSIAN MILITARY RESET IN THE HIGH NORTH AND THE BLACK SEA REGION- SIMILARITIES AND DIFFERENCES - NUPI, accessed March 10, 2026, https-//www.nupi.no/content/pdf_preview/30760/file/FINAL-FLANKS-1-REPORT.pdf

32. Russian Hybrid (New Generation) Warfare in the Time of a Systemic Political-Military Transition, accessed March 10, 2026, https-//nonproliferation.org/wp-content/uploads/2025/09/OP65-Russian-hybrid-warfare-occasional-paper-2025.pdf

33. More than Half the Battle - Amazon S3, accessed March 10, 2026, https-//s3.amazonaws.com/files.cnas.org/CNAS+Report-Command+and+Info-2021.pdf

34. Skeptics Doubt Ukraine Hack, Its Link to DNC Cyberattack - VOA, accessed March 10, 2026, https-//www.voanews.com/a/skeptics-doubt-ukraine-hack-link-to-dnc-cyberattack/3649234.html

35. Telegram as a digital front in Russia's war against Ukraine - DFRLab, accessed March 10, 2026, https-//dfrlab.org/wp-content/uploads/sites/3/2024/06/DFRLab_Russian_Telegram_2024.pdf

36. Russia - The Heritage Foundation, accessed March 10, 2026, https-//www.heritage.org/sites/default/files/2026-03/2026_IndexOfUSMilitaryStrength_ASSESSMENT_THREATS_RUSSIA.pdf

37. An MDO Approach to NATO's Counter-IADS Strategy - Joint Air Power Competence Centre, accessed March 10, 2026, https-//www.japcc.org/online-feature/an-mdo-approach-to-natos-counter-iads-strategy/

38. The Dispersion Paradox- When Sound Tactics Become a Death Sentence, accessed March 10, 2026, https-//smallwarsjournal.com/2026/02/13/the-dispersion-paradox/

39. Digital Warfare. The Russian Full Scale Invasion against Ukraine as Enacted on Telegram, accessed March 10, 2026, https-//www.harun-farocki-institut.org/en/2023/12/10/digital-warfare-the-russian-full-scale-invasion-against-ukraine-as-enacted-on-telegram/

40. Deterrence and Defense in the Baltic Sea Region Against the Russian Threat - CDiS SZ, accessed March 10, 2026, https-//cdissz.wp.mil.pl/u/documents/Deterrence_and_Defense_in_the_Baltic_Sea_Region_against_the_Russian_Threat_-_print_off.pdf

Copyright 2026

41. Russia-Ukraine MDO Strategic Analysis | PDF | Electronic Warfare | Cyberwarfare - Scribd, accessed March 10, 2026, https-//www.scribd.com/document/1002210535/Russia-Ukraine-MDO-Strategic-Analysis

42. Evaluating the Enhanced Forward Presence After Five Years - ResearchGate, accessed March 10, 2026, https-//www.researchgate.net/publication/369486214_Evaluating_the_Enhanced_Forward_Presence_After_Five_Years

43. NATO 2027- EUROPEAN LEADERSHIP WILL BE KEY TO DETERRENCE AGAINST RUSSIA - Mitre, accessed March 10, 2026, https-//www.mitre.org/sites/default/files/2025-05/PR-25-1575-NATO-2027-European-Leadership-Key-to-Deterrence-Against-Russia.pdf

44. Profiling the US Army's MDTFs - Euro-sd, accessed March 10, 2026, https-//euro-sd.com/wp-content/uploads/2025/10/ESD_10_2025_WEB.pdf

45. Europe | The Heritage Foundation, accessed March 10, 2026, https-//www.heritage.org/military-strength/assessing-the-global-operating-environment/europe

46. Russia's Changes in the Conduct of War Based on Lessons from Ukraine, accessed March 10, 2026, https-//www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2025/Lessons-from-Ukraine/

47. Russian Military Strategy- Organizing Operations for the Initial Period of War - RAND, accessed March 10, 2026, https-//www.rand.org/content/dam/rand/pubs/research_reports/RRA1200/RRA1233-1/RAND_RRA1233-1.pdf

48. NATO multidomain operations- Near- and medium-term priority initiatives - Atlantic Council, accessed March 10, 2026, https-//www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-multidomain-operations/

49. For NATO in 2027, European leadership will be key to deterrence against Russia, accessed March 10, 2026, https-//www.atlanticcouncil.org/in-depth-research-reports/issue-brief/for-nato-in-2027-european-leadership-will-be-key-to-deterrence-against-russia/

50. TOTAL DEFENSE IN THE BALTIC STATES A thesis presented to the Faculty of the US Army Command and General Staff College in parti, accessed March 10, 2026, https-//cgsc.contentdm.oclc.org/digital/api/collection/p4013coll2/id/4110/download

51. Full article- Navigating the uncertainty of the modern environment- multidomain operations for the defence of small states - Taylor & Francis, accessed March 10, 2026, https-//www.tandfonline.com/doi/full/10.1080/09662839.2025.2540955

Copyright 2026