Converging Adversary Doctrines: A Systematic Threat

Published: Ambient Stratagem

June 2025

Executive Summary:

Between 2022 and 2025, Russia, China, Iran, and North Korea have evolved from regionally distinct challengers into strategically aligned disruptors. This white paper reveals how these adversaries are converging around a shared doctrine of systemic disruption, designed not to defeat NATO in force-on-force battle, but to paralyse its systems-of-systems through logic-layer attacks, narrative deception, decision latency, and cognitive overload.

Across flashpoints, doctrine, and military exercises, the trend is clear:

- System Destruction Warfare, Reflexive Control, Intelligentised Warfare, and Domain-Flexible Coercion are now formalised into the warfighting logic of our most capable adversaries.
- This convergence is not theoretical, it is operational, real-world and escalating.
- The Grey Zone is no longer beneath war. It is war, executed in slow motion, across command loops, infrastructure dependencies, and allied decision chains.

The paper challenges NATO and its partners to reframe deterrence, doctrine, and procurement for an era where command tempo is more contested than territory, and where the decisive terrain is the space between input and action.

Without urgent doctrinal realignment, the next war will not begin with an attack.

It will begin with decisions that never arrive.

The supreme art of war is to subdue
the enemy without fighting. – Sun Tzu

Preface: 2022 – The Year Convergence Became Visible

The convergence tracked in this white paper did not begin in 2022, but it became undeniable in that year.

Russia's full-scale invasion of Ukraine revealed a battlefield shaped as much by deception, saturation, and tempo disruption as by tanks or missiles. China escalated pressure in the Indo-Pacific through air incursions, maritime harassment, and cognitive warfare simulations, all while publishing strategic material on "Intelligentised" and "System Destruction" warfare.

Meanwhile, Iran operationalised its drone doctrine, not just regionally, but globally. Supplying Russia with low-cost, high-disruption UAVs that blurred the boundary between proxy and peer. At the same time, its cyber units demonstrated cross-domain reach, attacking infrastructure, industry and narrative ecosystems.

North Korea, too, surged missile tests and cyber raids, linking kinetic coercion with digital theft in a way that prefigured its 2025 doctrinal pivot to "domain-flexible coercion."

By the end of 2022, it was no longer accurate to treat these as isolated actors with region-specific doctrines. What emerged instead was a shared logic, one that prioritised system disruption, decision paralysis and logic-layer warfare.

This paper covers the three-year period that followed. **June 2022** to **June 2025**. The phase in which converging doctrine moved from theory to structured execution.

1. From Attrition to Paralysis

The Rise of Strategic Disruption as the Primary Objective

Traditional Warfare

For over a century, the logic of war has prioritised physical attrition, the destruction of enemy forces, infrastructure and supply lines.

New Paradigm

Rather than focus on the opponent's physical capacity to fight, adversary states are now targeting the underlying systems that enable decision-making, tempo and cohesion.

Strategic Objective

Strategic disruption, not territorial gain or force destruction is becoming the central objective of modern warfare doctrine.

This shift is clearest in China's formal articulation of its doctrine. The 2023 update to the Science of Military Strategy, the PLA's principal military theory manual, introduced two decisive concepts: Intelligentised Warfare and System Destruction Warfare. Together, they represent a break from attrition-based logic. Instead of defeating a force in the field, the objective is to paralyse it, by severing the cognitive, digital and organisational arteries that sustain its ability to function in a contested environment [1].

"Intelligentised Warfare" focuses on leveraging AI, machine learning and real-time sensor fusion to achieve decision dominance. But this is not simply about faster reaction. It is about deliberately disrupting the adversary's OODA loop, the observe–orient–decide–act cycle that underpins modern command structures. Chinese doctrine explicitly discusses "cognitive domain operations" that inject ambiguity, overload sensory channels and create latency in command systems. These are not theoretical concepts. PLA warfighting experiments now routinely integrate digital decoys, false data injections and psychological shaping to confuse both autonomous systems and human operators [1].

Complementing this is the doctrine of System Destruction Warfare. Rather than hitting strategic targets in isolation, China seeks to "unravel the web", to identify and attack the dependencies and interdependencies between systems, not just the nodes themselves. This means disrupting communications between forward units and higher command, breaking the links between targeting platforms and strike assets, and attacking trust in the accuracy of incoming information. In short, it is a logic of warfare designed to collapse the system, not just damage its parts [1].

Russia, too, has moved in this direction, though it arrives from a different intellectual lineage. The Soviet-era concept of Reflexive Control has re-emerged not just as a theory, but as an operational technique. Reflexive Control involves shaping the adversary's perception and decision-making process so that they "choose" to act in ways favourable to the attacker. In recent years, Russian military journals have begun to reframe Reflexive Control as a toolkit for modern electromagnetic and information warfare, detailing how false signals, jammed GPS, fake radio chatter and spoofed drone footage can manipulate the adversary's understanding of the battlespace [2].

Reflexive Control and Strategic Engineering

This is not deception for deception's sake. It is strategic engineering of misperception, designed to induce paralysis, hesitation, or misapplication of force. Reflexive Control has been used to lure air defence systems to activate prematurely, to misdirect targeting assets, and to sow confusion in command nodes relying on fused but corrupted data [2]. It represents a form of cognitive attrition: degrading not the platform, but the trust between operator and system.

Together, these doctrines represent an emerging strategic equivalence:

- China disrupts systems to slow or stall NATO's decision-making.
- Russia shapes perceptions to mislead or misalign NATO's intent.

In both cases, the aim is to defeat NATO's ability to decide effectively under pressure.

The convergence here is not incidental. It is a shared recognition among NATO's adversaries that modern military power is not just a function of firepower or troop numbers. It is a function of decision coherence, the ability to generate reliable action from dispersed, often siloed, multi-domain systems. That coherence is fragile. And adversaries are now engineering its failure.

This is not merely academic. NATO's current force posture remains optimised for response, not resilience. Its decision chains are broad but brittle. Its systems-of-systems rely on assumed connectivity, data fidelity and alliance-wide interoperability. Each of these becomes a liability when facing an adversary whose central doctrine is to paralyse, not to penetrate.

The challenge is compounded by the speed of modern warfare. The more NATO invests in fast decision architectures, the more it becomes dependent on predictable system integrity. But it is precisely this integrity that Reflexive Control and Intelligentised Warfare are designed to compromise.

In this emerging context, the traditional logic of deterrence begins to unravel. If the adversary can fracture the cohesion of response before escalation is even recognised, the foundational principle of deterrence by retaliation is degraded. If your adversary can make you hesitate, or misread the battlespace before you act, they do not need to defeat your military. They only need to disrupt your trust in it.

Strategic disruption is thus not simply a new tactic. It is a new purpose in warfare. It demands that NATO rethink not only how it defends, but what it defends.

In a system-disruption paradigm, the primary asset is no longer the platform or the base. It is the integrity of decision-making under pressure.

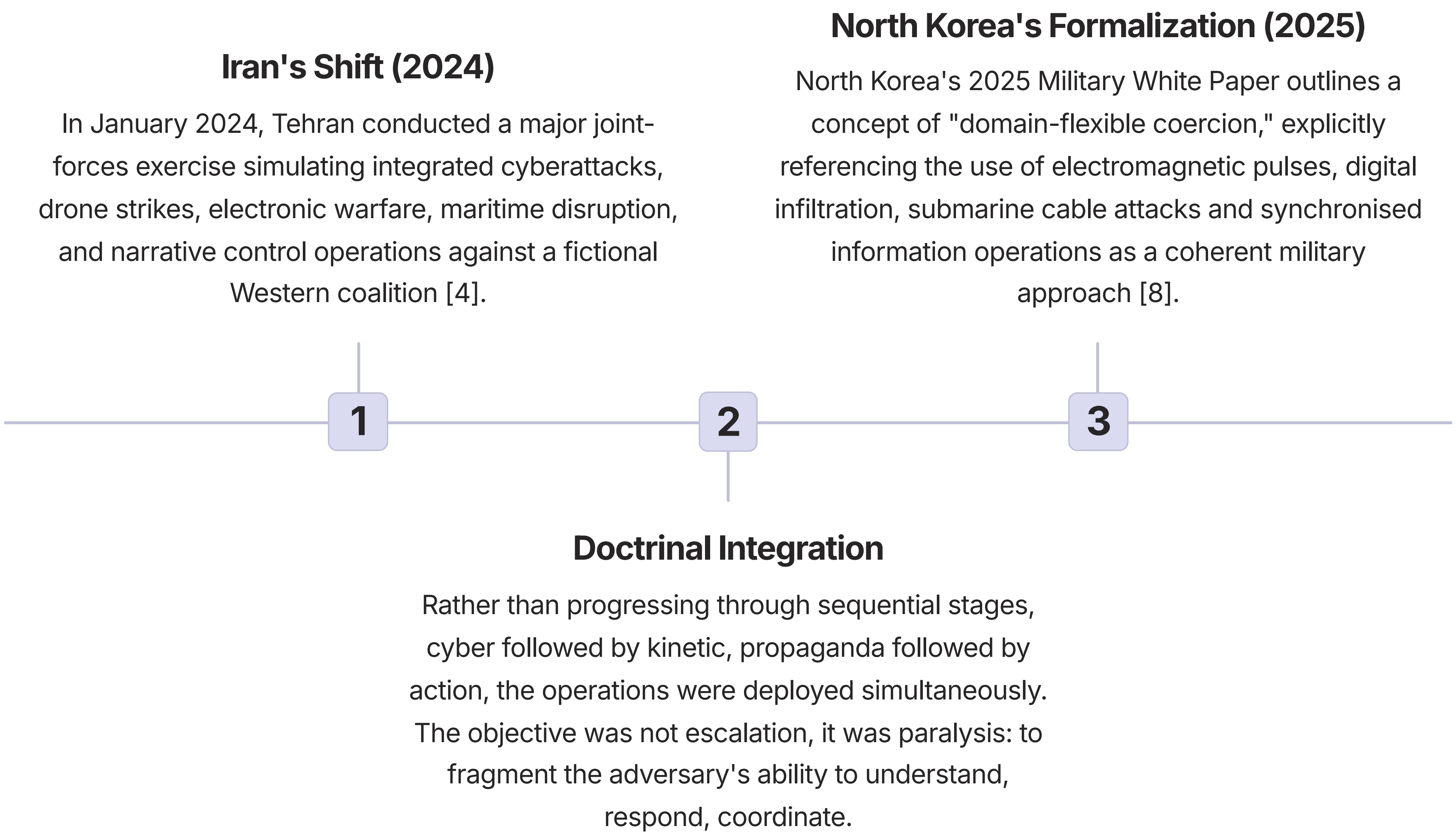
And that asset is under attack.

2. The Grey Zone Goes Formal

How Disruption Has Moved from Tactic to Doctrine

For decades, analysts in Western defence circles described "Grey Zone" conflict as a realm of ambiguity: low-intensity, non-attributable, politically deniable operations that blurred the boundaries between peace and war. These activities were seen as opportunistic, improvised rather than doctrinal. But that framing no longer holds.

Between 2022 and 2025, a doctrinal shift has unfolded across multiple adversary states. Grey Zone tactics have been institutionalised. What were once described as asymmetric or sub-threshold actions are now formalised into military white papers, exercises, and warfighting frameworks. The Grey Zone has moved from the shadows into the field manuals.



1

Iran's Shift (2024)

In January 2024, Tehran conducted a major joint-forces exercise simulating integrated cyberattacks, drone strikes, electronic warfare, maritime disruption, and narrative control operations against a fictional Western coalition [4].

2

Doctrinal Integration

Rather than progressing through sequential stages, cyber followed by kinetic, propaganda followed by action, the operations were deployed simultaneously. The objective was not escalation, it was paralysis: to fragment the adversary's ability to understand, respond, coordinate.

3

North Korea's Formalization (2025)

North Korea's 2025 Military White Paper outlines a concept of "domain-flexible coercion," explicitly referencing the use of electromagnetic pulses, digital infiltration, submarine cable attacks and synchronised information operations as a coherent military approach [8].

This marks a break from previous Iranian patterns of hybrid warfare. The simulated conflict blended domestic disinformation, GPS spoofing, undersea sabotage and information denial into a converged disruption model. Iran, long seen as an opportunistic actor in asymmetric warfare, demonstrated that it had internalised the system-disruption logic articulated by both China and Russia.

The elevation of disruption from tactic to doctrine is also explicit in North Korea's 2025 Military White Paper. An official publication not typically associated with doctrinal transparency. In that document, Pyongyang outlines a concept of "domain-flexible coercion," explicitly referencing the use of electromagnetic pulses, digital infiltration, submarine cable attacks and synchronised information operations as a coherent military approach [8]. This is not ad hoc harassment. It is a structured form of what might be called asymmetric doctrine: using tools of disruption in ways designed to exploit the cognitive and systemic complexity of technologically superior opponents.

What these cases confirm is that adversaries have moved beyond the notion of "operating in the Grey Zone" as a stopgap between war and peace. Instead, the Grey Zone has become the primary theatre of operations. The logic is simple but devastating: if one can achieve strategic effects, denial, delay, destabilisation, without triggering Article 5 or breaching thresholds that compel retaliation, then why fight conventionally at all?

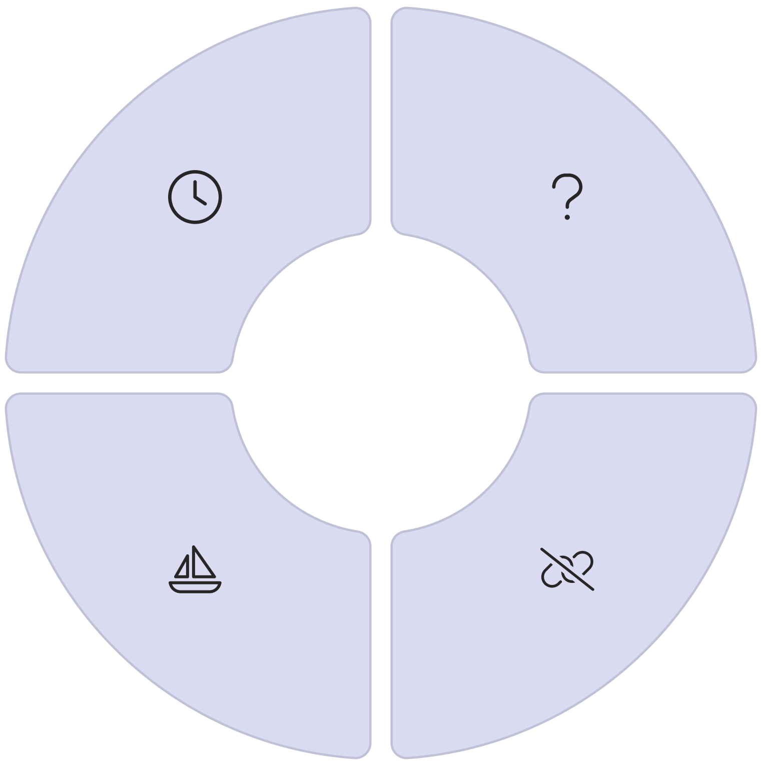
Grey Zone Doctrine Evolution

China and Russia are already doctrinally aligned with this view. But what's significant in this period is the doctrinal diffusion of that logic to middle and smaller powers. These states do not need to match NATO's capabilities. They only need to copy the strategy. One that is far more accessible than high-end kinetic warfare.

This shift also exposes a vulnerability in Western planning doctrine. NATO still treats the Grey Zone as a set of "left-of-boom" activities. Pre-conflict signals that may escalate. But for adversaries, this is the conflict. Their goal is not to breach thresholds, but to render those thresholds irrelevant through continuous, low-detectability disruption that exhausts cognitive, political and institutional will.

Moreover, these activities are not random. They are targeted. Grey Zone doctrine is now being used to strike at:

- Decision latency
- Information confidence
- Civil–military boundary integrity
- Interoperability trust between allies
- The speed and cohesion of mobilisation



Decision Latency

Slowing response time

Information Confidence

Eroding trust in data

Trust Disruption

Breaking alliance cohesion

Mobilization Delay

Hampering force readiness

Each of these, if disrupted in advance of a conventional conflict, can neutralise the adversary's military power without ever firing a shot.

As this doctrinal shift spreads, the very notion of escalation becomes warped. If disruption is continuous and strategic in intent, then crisis becomes the default state, not an exception. The line between competition and conflict is no longer just blurred, it is irrelevant.

The institutionalisation of Grey Zone logic also creates new dynamics in peacetime diplomacy and deterrence. Because these doctrines focus on ambiguity, states can simultaneously claim plausible deniability while signalling resolve to domestic and allied audiences. This creates strategic instability: one side is acting according to an informal, bounded view of war, while the other is operating from a formal, unbounded doctrine of disruption.

For NATO, this doctrinal mismatch is dangerous. If Grey Zone operations are treated as irregular nuisances, rather than formal components of adversary warfighting, then responses will always lag behind design. Worse, Western frameworks for intelligence assessment and deterrence modelling may underweight the strategic intent behind such operations, viewing them through the lens of behaviour rather than doctrine.

This creates an opportunity for adversaries to exploit precisely the frameworks we use to interpret threat. NATO states may ask, "Is this really war?" when confronted with attacks on undersea cables, false flag cyber operations, or narrative manipulation campaigns. Meanwhile, adversaries are asking a different question: "Is this disruption enough to shape your decisions tomorrow?"

Ultimately, the formalisation of Grey Zone doctrine means NATO must reclassify what it defends, and how. The protection of territory, assets, or even cyber infrastructure is no longer sufficient. The target of modern doctrine is trust, logic, and time.

If those systems are not defended and not even seen, then war will be lost before war is declared.

3. Cognition is the New High Ground

Why Command Tempo, Not Territory, is the True Target

The fundamental assumption of most NATO warfighting doctrine is that strategic outcomes follow from superiority in the physical or digital domains. Win the skies, secure the networks, hold the ground and victory will follow. But a new set of adversary doctrines is rejecting this logic entirely. Their new objective is not to hold terrain, but to seize time. Not by accelerating their own decision-making, but by slowing, distorting, or paralysing ours.

This marks a profound shift in the concept of high ground. In the 20th century, control of physical elevation offered visibility, communication advantage and firepower leverage. In the 21st century, that high ground has migrated to the logic layer. The domain where information is observed, processed, filtered, and acted upon. Adversaries have begun to target it deliberately.

Cognitive Delay Injection

The clearest case of this strategic targeting of cognition is seen in China's AI-enabled military research and development ecosystem. In late 2023, reporting from the South China Morning Post revealed that PLA-affiliated labs were actively developing "cognitive delay injection" systems. Tools designed to interfere not with hardware or software, but with human-machine understanding itself [5].

Overwhelming Sensor Fusion

These systems work by overwhelming or misdirecting sensor fusion processes. For example, rather than jamming communications outright, they might introduce high-fidelity false signals into a data stream, triggering misclassification by an AI target recognition system. This in turn generates false alerts or suppresses legitimate ones, causing human operators to question the reliability of their own decision tools. The result is cognitive hesitation, not system failure.

Delay Equals Defeat

It is a quiet form of warfare. Nothing explodes. No data is destroyed. But the adversary's aim is achieved: decision delay. And delay, in high-tempo conflict, is defeat by other means.

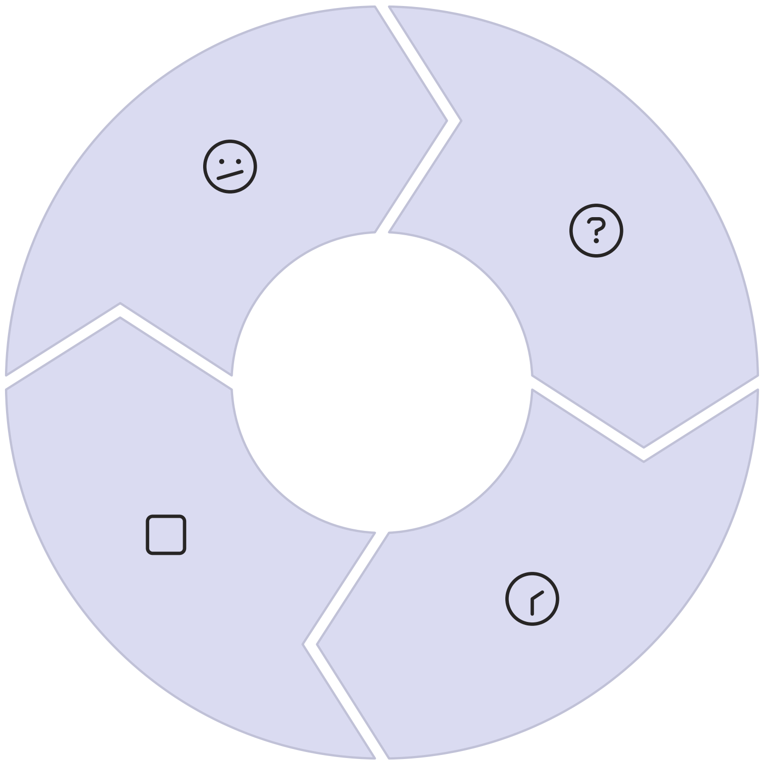
This concept is not confined to Chinese theory. Russian Reflexive Control, as outlined in Section 1, seeks to engineer the adversary's mental model through intentional deception and pre-conditioned reflex responses. It is not just about jamming signals, it is about manipulating the interpretation of those signals. In modern warfare, where machines make suggestions and humans validate or authorise, corrupting what is believed is more impactful than destroying what is used [2].

The Revolution in Cognitive Warfare

From a doctrinal perspective, this is revolutionary. Traditional approaches to C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. Are built on the idea that more information, correctly shared, leads to better outcomes. But adversaries are now targeting the vulnerabilities created by that information flow. By flooding systems with ambiguity or partial truths, they generate decision fatigue. A slow erosion of tempo and clarity.

This is where NATO's structural strength becomes its doctrinal vulnerability.

- Speed of decision is distributed across multiple levels.
- Trust in systems depends on assumed accuracy and minimal adversarial manipulation.
- Operational tempo relies on fused, multi-node awareness.



Ambiguity Injection

Introducing false or misleading data

Trust Erosion

Undermining confidence in systems

Decision Delay

Forcing rechecks and verification

Operational Paralysis

Preventing timely action

In a system where every decision is a derivative of sensor confidence and AI-augmented suggestion, adversaries do not need to breach the system. They only need to dilute the certainty of the input stream. Once that is achieved, the downstream effects cascade:

- Orders are delayed.
- Rules of engagement are rechecked.
- Units second-guess threat assessments.
- Coordination stalls.

It is the algorithmic equivalent of fog and it is being deliberately manufactured.

The Vulnerability of Automated Decision Systems

Compounding the problem is NATO's increasing reliance on automated or semi-automated decision-support tools. These systems are built on assumptions of clean signal input, predictable adversary behaviour and logical escalation pathways. But modern adversaries do not follow logical escalation. Their aim is non-patterned pressure, to introduce ambiguity so deep that it cannot be cleanly classified as threat or non-threat.

In this environment, traditional deterrence calculations, based on visible capabilities and credible thresholds, become ineffective. The adversary is not breaching a threshold. They are delaying our recognition of one. By the time a consensus emerges inside the decision loop, the window for effective response may have closed.

Cognitive Warfare

Not about demoralisation but inducing operational misalignment

Calculated Confusion

Through overload, contradiction, and ambiguity

Deterrence Undermined

When response speed, signal clarity and unity of purpose are compromised

New Strategic High Ground

The space between inputs and action, the logic layer where choices are made

This is the true battlefield of cognition. And it extends beyond systems. It affects operators, analysts and commanders.

Cognitive warfare is not about demoralisation. It is about inducing operational misalignment through calculated overload, contradiction, or confusion.

From a strategic standpoint, this undermines the very foundations of NATO deterrence. Our model is premised on response speed, clarity of signal and unity of purpose. But when adversaries shape the cognitive environment itself and do so at machine scale, then no amount of readiness matters if we cannot decide, or decide in time.

The strategic high ground, then, is no longer a hilltop, air corridor, or satellite orbit. It is the space between inputs and action, the logic layer where choices are made.

If NATO cannot see this clearly, defend it deliberately and design for its resilience, then the next conflict may be lost not in contact but in computation.

4. System Destruction Warfare Has Arrived

And NATO's Interdependencies Are Its Achilles' Heel

Western military power is built on a latticework of interdependent systems. From joint logistics and coalition intelligence sharing to multi-domain C2 and real-time ISR fusion, NATO operates as a systems-of-systems. This structure is its greatest strength and increasingly, also its greatest vulnerability.

Over the last three years, adversary doctrine has shifted to exploit that vulnerability deliberately. The goal is not to strike NATO's platforms, bases, or brigades but to fracture the dependencies that make those platforms effective. This is the heart of System Destruction Warfare a doctrinal evolution most clearly articulated in Chinese military strategy, but now mirrored across adversarial postures [5].

Where traditional warfare aimed to degrade an adversary's physical capability to operate, system destruction aims to collapse the coherence of the adversary's operations. It does this not by targeting any single asset, but by removing the glue that binds assets into an operational whole.

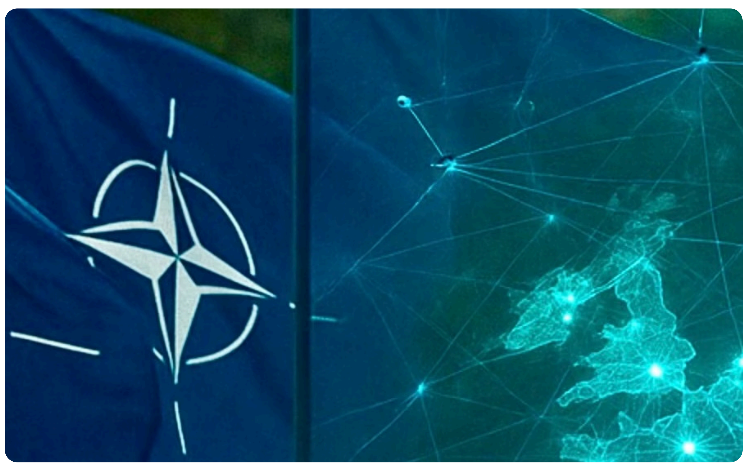
NATO's Network Vulnerability

Communications Disruption

Targeting the interfaces between allied systems, e.g. US satellite ISR uplinking to European command nodes.

Human-Machine Trust

Degrading the handovers between AI detection and human authorisation.



Supply Chain Vulnerability

Exploiting cross-alliance dependencies on supply chain resilience, bandwidth prioritisation and shared intelligence criteria.

In late 2023, a leaked NATO Allied Command Transformation (ACT) report sounded the alarm. It identified a core weakness across NATO's network: the assumption of uninterrupted interoperability between digital, procedural, and human systems. According to the report, NATO's reliance on layered but fragile information flows, spanning sensors, AI inference engines, human analysts, commanders, and political authorities, makes it acutely vulnerable to attacks not on its data, but on its data integrity and trust pathways [3].

This is where system destruction becomes most effective. It targets:

- The interfaces between allied systems, e.g. US satellite ISR uplinking to European command nodes.
- The handovers between AI detection and human authorisation.
- The cross-alliance dependencies on supply chain resilience, bandwidth prioritisation, and shared intelligence criteria.

By degrading these, an adversary can fragment NATO's collective capability without ever needing to destroy a single tank, drone, or warship.

China's Science of Military Strategy formalises this with precision. It outlines how, in future warfare, the emphasis will be placed on striking the enemy's operational architecture, including logistics, C2 infrastructure, data validation systems, and joint force synchronisation, through a combination of cyber infiltration, space denial, AI-generated deception, and electromagnetic disruption [5].

System Destruction Warfare is thus not a supplement to kinetic force. It is a parallel doctrine of effects-based paralysis. The target is not the military system, it is military system function.

What makes NATO especially susceptible is its success. The alliance has, over decades, built an extraordinary level of integration across members. But that integration requires shared protocols, continuous synchronisation, and deep technical trust. All of these are attack surfaces. NATO's command logic is now so distributed, and so reliant on fragile, interconnected digital systems, that it becomes brittle when facing adversaries trained to exploit seams, latency and doubt.

For example, if a NATO decision support platform receives a fused ISR picture that has been subtly manipulated, not hacked, but corrupted through a spoofed upstream sensor, that misinformation will propagate not linearly, but systemically. Targeting cues may shift. Rules of engagement may not trigger. Alliance members may diverge in interpretation. And the entire decision response chain may stall.

Iran, though less technologically advanced, has demonstrated its understanding of this logic through its simulation of joint domain attacks on maritime traffic, communications, and energy infrastructure. In a single 2024 exercise, Iranian forces used cyber probes, drone strikes, and narrative disruption not to break an enemy's defences, but to overwhelm its system capacity to detect, respond, and re-stabilise across domains [4].

North Korea's adoption of "domain-flexible coercion" follows the same logic. It places system pressure ahead of territorial incursion. Sabotage, underwater disruption, and deniable data manipulation are not secondary to warfighting. They are the warfighting doctrine itself [8].

Strategic Implications of System Destruction

The consequences are profound. NATO must now confront a strategic environment in which system survivability matters more than individual force survivability. In this paradigm, platform hardening is not sufficient. Decision path resilience, system handover robustness, and interdependency degradation resistance become primary metrics of operational readiness.

But here lies a structural dilemma. Western procurement and doctrinal development systems are not designed to prioritise connective resilience. They prioritise capability enhancement, new aircraft, better cyber tools, faster comms. But when the adversary targets connectivity itself, then new tools simply add new vulnerabilities unless they are part of a hardened and adaptive system architecture.

System Destruction Warfare also changes the nature of deterrence. Traditional deterrence assumes that major power adversaries will avoid direct confrontation. But if those adversaries can now generate strategic paralysis through system targeting, then they can achieve strategic objectives without triggering a major military confrontation.

In other words, the incentive structure for aggression has shifted. The cost-benefit analysis for adversaries now includes low-cost, high-impact options that fall well below NATO's retaliation thresholds but still deliver effects equivalent to major disruption.

This is how systems fail in the 21st century:

> Not with a bang, but with dislocation.

NATO must therefore rethink what it means to be secure. Security is no longer a function of force ratios, or platform counts. It is a function of system integrity under stress. And unless NATO can harden not only its components but its connective tissue, then future conflicts will be shaped not by battlefield performance, but by the invisible failure of systems no one thought to defend.

5. Adversarial Interoperability

How Convergence Has Replaced Competition Among NATO's Opponents

One of the most underappreciated developments in modern strategic competition is the silent shift in posture among NATO's adversaries, from competition with each other to convergence against us. For decades, Western doctrine has operated under the implicit assumption that Russia, China, Iran, and North Korea each pose distinct, often regionally constrained, threats. Their doctrinal differences, rivalries, and political misalignments were thought to limit their ability to align. That assumption no longer holds.

Between 2022 and 2025, a pattern has emerged. Across military exercises, doctrinal updates, and operational behaviour, a form of adversarial interoperability has begun to take shape, not in equipment, but in effect logic. These actors are converging around a shared understanding of how to contest the West: not by matching NATO platform-for-platform, but by targeting its systems-of-systems with tailored, coordinated forms of disruption.

This is not coordination in the formal sense. There is no evidence of a unified command or joint planning. But there is growing evidence of mutual doctrinal learning, a process of alignment through observation, adaptation and mirrored innovation.

Doctrinal Convergence Among Adversaries

In 2024, the US Department of Defense explicitly recognised this trend in its Annual Threat Assessment. The report described "doctrinal convergence" among peer and near-peer adversaries, highlighting that Russia, China, Iran, and North Korea are now operating under a shared principle: conflict by systemic disruption, not conventional force confrontation [6].

Russia

Continues to develop and refine Reflexive Control as an operational tool, designed to shape NATO perceptions and pre-empt decisions through carefully orchestrated disinformation and electromagnetic deception [2].

China

Has formalised Intelligentised Warfare and System Destruction Warfare as core to its strategic doctrine, leveraging AI, space-based disruption, and logic-layer manipulation to paralyse adversary systems before kinetic contact [3].

Iran

As evidenced in its 2024 simulation, has synthesised multi-domain Grey Zone disruption into a coherent operational doctrine, using cyber, drones, narrative control, and maritime sabotage in an integrated manner that mirrors Chinese system-targeting principles [4].

North Korea

2025 military white paper adopts a remarkably similar framework, explicitly referencing "domain-flexible coercion" and describing the use of digital and undersea disruption tools to deny system functionality rather than territory [5].

Though they differ in capability, each of these actors now operates with a shared logic:

1. Strike the system, not the soldier.
2. Collapse tempo, not infrastructure.
3. Exploit ambiguity, not escalation.

This shared logic is reinforced by shared threat perception. Each of these states views NATO's decision advantage, global sensor–shooter architecture, and alliance coordination as core enablers of Western strategic dominance. Their aim is not to confront NATO's strengths head-on, but to erode its functional coherence through doctrine-driven disruption.

Strategic Implications of Adversarial Convergence

It is important to understand that this is not a coincidence. The convergence is not random, it is a consequence of rational doctrinal evolution under similar strategic pressures. Each of these actors faces a capability gap with NATO. Each must contest a more technologically advanced, better-resourced opponent. And each has discovered that system-level disruption offers an affordable, scalable, and deterrent-resistant path to strategic effect.

What this creates is a multi-polar web of doctrinal alignment, a form of asymmetric coalition-building without formal alliance. One actor may deploy the tactic. Another learns from it. A third iterates. And all benefit from the West's inability to treat these actions as part of a shared threat ecosystem.

The implications are profound.

1 **Eroded Deterrence**

It erodes NATO's ability to apply deterrence through traditional means. These adversaries no longer need to act jointly. Their doctrinal synergy is enough to deliver cumulative systemic pressure.

2 **Global Pressure Continuity**

It creates global strategic pressure continuity. Even if NATO deters or contains one actor regionally, another can apply similar disruption logic elsewhere, keeping the alliance in a state of permanent reaction.

3 **Alliance Cohesion Strain**

It strains alliance cohesion. NATO's organisational structure is optimised for confronting defined adversaries in discrete theatres. But convergent, distributed system-level disruption makes it harder to classify events, assign attribution, or calibrate response. This creates cognitive fragmentation within the alliance, exactly the effect adversaries are designing for.

Finally, it forces a doctrinal rethink. If adversaries have achieved de facto interoperability in their approach to systemic warfare, then NATO must develop an interoperable resilience doctrine in response, one that focuses not only on deterrence and response, but on systemic survivability under convergent pressure.

The term "Adversarial Interoperability" may not yet appear in NATO white papers. But the pattern is already in motion. Strategic alignment need not be declared. It only needs to be designed into doctrine.

6. Call to Action

From Domain Defence to System Resilience

Western defence doctrine is at a crossroads. For over two decades, NATO's strategic focus has been on expanding its multi-domain reach: improving interoperability across land, sea, air, cyber, and space. It has achieved remarkable success, fielding the most integrated command structures, the most connected ISR frameworks, and the most capable allied decision networks in history.

But this strength has become its vulnerability.

The adversaries now confronting NATO are not trying to contest domain supremacy. They are targeting the connective tissue. And they are doing so not through force-on-force engagement, but through doctrine-by-design. Their goal is not to degrade our warfighting capabilities directly. It is to erode our ability to perceive, decide, and respond at the speed and scale modern conflict demands.

This is the moment to reframe how defence is conceptualised.

It is not enough to harden networks. Or to acquire more drones. Or to improve AI targeting. These are tactical adjustments. The real shift required is doctrinal. NATO must move from defending domains to defending decision integrity. From deploying capabilities to ensuring resilience under ambiguity.

Five Immediate Changes Required

This requires five immediate changes in how we think, plan, and build:

1. Redefine the Battlespace

NATO must formally recognise that the logic layer, the space between input and action, is now a contested domain. This is where adversaries are operating. It's not a niche concern. It is the decisive theatre of 21st-century warfare. Reflexive Control, cognitive delay injection, and AI-driven perception management are not sci-fi threats. They are validated doctrines.

The battlespace must be redefined to include not just physical geography or electromagnetic spectrum, but also the decision architectures and tempo synchronisation layers upon which NATO force projection depends.

2. Shift from Platform Dominance to System Resilience

Capability procurement must no longer prioritise the most advanced platform. Instead, it must prioritise the survivability and adaptability of the system as a whole. A next-generation ISR drone is irrelevant if it feeds corrupted data into an unverified logic chain. NATO must evaluate investments not only by their standalone effect, but by their contribution to system-level coherence under pressure.

This means hardening the seams. The handovers. The decision points. Resilience is not redundancy. It is the ability to operate coherently when the network is contested, the signals are ambiguous, and the pressure is non-linear.

3. Develop Strategic Ambiguity Protocols

Adversaries thrive on ambiguity. NATO doctrine, by contrast, is designed around clarity: clear thresholds, clear ROEs, clear attribution. But the convergence of Grey Zone doctrine, Reflexive Control, and System Destruction Warfare means that strategic ambiguity is no longer an exception, it is the default operating condition.

NATO must therefore build protocols not just for deterrence-by-certainty, but for resilience under ambiguity. This includes new forms of crisis signalling, adaptive response frameworks, and pre-authorised decision pathways that acknowledge contested cognition.

4. Create a Logic Layer Defence Command

Just as NATO created air and cyber commands when those domains became decisive, it must now create a Logic Layer Defence Command, responsible for detecting, understanding, and countering attacks that target decision processes, machine-human trust loops, and cross-domain system synchronisation.

This is not a cyber unit. It is not a PSYOPS team. It is a doctrinally-enabled fusion structure built to defend the cognitive and computational coherence of the alliance itself.

5. Reclassify Grey Zone Acts as Strategic Attacks

Finally, NATO must stop treating Grey Zone disruption as "pre-conflict behaviour." The convergence of adversary doctrine shows that these acts are not preludes to war. They are the war, prosecuted through systems, perception, and latency.

To continue viewing pipeline sabotage, undersea cable interference, GPS spoofing, or AI-targeted propaganda as merely hybrid threats is to misclassify the most strategically effective attacks NATO will face.

These acts must be reclassified, as strategic system assaults, with commensurate rules of response, thresholds of concern, and alliance-wide coordination.

The Consequence of Inaction

If NATO fails to adapt, it will continue to lose not on the battlefield, but before the battlefield is even recognised.

It will lose by hesitation.

By confusion.

By divergent interpretation between allies.

By corrupted logic paths and fragmented tempo.

This is how modern war is won, not by destroying the opponent's power, but by nullifying their ability to use it.

Adversaries have understood this. They are writing it into doctrine. They are testing it in exercises. They are executing it in the real world.

The question is whether NATO will adapt in time, or remain optimised for a kind of war that no longer exists.

References

1. China Aerospace Studies Institute (2023) Science of Military Strategy 2023: Translation and Analysis. Air University. November 2023. **https://www.airuniversity.af.edu/CASI/Display/Article/3571856/science-of-military-strategy-2023**
2. NATO CCDCOE / Russian Academy of Military Sciences (2024) Reflexive Control and the Russian Approach to EW Denied Environments. Translated from Russian military journals. March 2024. (Summarised in NATO CCDCOE briefings, unclassified)
3. Breaking Defense (2023) Leaked NATO ACT Memo: Systemic Cyber and Infrastructure Vulnerability. December 2023. **https://breakingdefense.com/2023/12/nato-fears-growing-vulnerability-to-systemic-cyber-disruption**
4. The Diplomat (2024) Iran's Military Drills Showcase Growing Asymmetric Doctrinal Sophistication. January 2024. **https://thediplomat.com/2024/01/irans-military-drills-showcase-growing-asymmetric-doctrinal-sophistication**
5. South China Morning Post (2023) China Developing Military AI Systems to Target Enemy Decision Loops. September 2023. **https://www.scmp.com/news/china/military/article/3235799/china-develops-new-ai-systems-military-command-and-control**
6. Office of the Director of National Intelligence (2024) US Annual Threat Assessment of the Intelligence Community. April 2024. **https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024.pdf**
7. RIA Novosti (2023) Russian Military Doctrine Roundtable: The Age of Strategic Paralysis. October 2023. (Reported summary from Russian defence press. Translated via NATO CCDCOE.)
8. NK News (2025) North Korea's 2025 Military White Paper Signals Doctrinal Shift. April 2025. https://www.nknews.org/2025/04/north-korea-releases-2025-military-white-paper