Centralised Command, Distributed Control, Disconnected Training?

Why a Unified Battle Management Architecture is Key to NATO's Distributed Operations and Training

By Commandant Peter Vanderostyne, BEL Air Force, JAPCC

Introduction: A New Mantra in Multi-Domain Operations

With the outbreak of the Ukraine-Russian conflict, we have witnessed fundamental paradigm shifts in how modern warfare hinges on distributed and dispersed operations. Traditional conventional operations, though still conceptually valuable, are increasingly struggling to meet the demands of contemporary conflict. Precision strike threats, persistent ISR, electronic warfare, cyber disruption, multi-domain integration, and compressed decision cycles shape today's battlespace.

In this rapidly evolving battlespace, NATO confronts adversaries who leverage speed, ambiguity, and disruption across every domain, Land, Sea, Air, Cyber, and Space. As noted by Generals Mark Milley and Stephen Townsend, 'Commanding across these domains requires an evolution from 20th-century Command and Control (C2) methodology to one that provides Decision Advantage in the rapidly changing environment.'[1]

To maintain superiority, our C2 architecture must match this agility. The emerging doctrine of Centralised Command, Distributed Control, and Decentralised Execution signifies this crucial transformation, balancing unity of effort, operational resilience, and tactical initiative.

© SHAPE

The Joint Warfare Centre is modernising NATO's largest exercises by employing technologies like the Maven Smart System, the Alliance's first AI-enabled warfighting command-and-control capability.

However, this approach presents a C2 dilemma. NATO faces three interconnected challenges: maintaining unity of effort across contested communication channels; translating the hard-won lessons of Ukraine into a coherent battle management architecture; and ensuring that synthetic training environments genuinely reflect the principle of 'train as you fight.' From the perspective of multi-domain operations (MDO), this article will analyse how a unified battle management interface integrates disparate data sources, including multi-tactical data links (TDL), into a single operational picture. These are critical training components that must be integrated into a cohesive battle management system. Ultimately, it asserts that NATO requires a Unified Battle Management Architecture, a hardware-agnostic software framework that fuses multi-domain sensor data into a single, actionable interface for both the warfighter and the trainee. Without this, we risk a 'disconnected' force that possesses the tools for victory but lacks the muscle memory to use them in a contested environment.

Essential Elements Fostering Decisional Advantage:

The Cognitive Dimension and Centralised Command

Decision advantage in modern warfare increasingly hinges on the cognitive dimension, the ability to interpret and act amid uncertainty. As data saturates the battlespace, cognitive overload becomes a critical risk.[2] Centralised Command remains the cornerstone of NATO's strategic coherence in managing this complexity. At the highest level, it ensures that operations, whether reinforcing the Baltics, securing Mediterranean Sea lanes, or defending against cyber intrusions, align with the Supreme Allied Commander Europe's (SACEUR) intent.

'Effective Distributed Control in contested environments requires NATO to align its doctrine with its technology through a unified battle management software interface, one that is used for both training and operations.'

This centralisation is not about micromanaging every move, but rather, safeguarding unity of effort, prioritising resources, and preventing strategic fragmentation. During Exercise DEFENDER 25, the largest US Army exercise in Europe, Centralised Command was vital to stress-test NATO's ability to synchronise logistics, airlift, Cyber defence, and multinational operations under a single strategic vision.[3]

Resilience through Distributed Control and Decentralised Execution

Centralisation alone cannot withstand adversaries who target command nodes through cyberattacks, electronic warfare, or precision strikes. This is where Distributed Control becomes critical. By dispersing planning, monitoring, and coordination across multiple resilient nodes, NATO mitigates the risk of single points of failure. If a primary headquarters is disrupted

The Command and Control Duty Officer (C2DO) in a Joint Force Air Component (JFAC) may send preformatted Link 16 messages such as engagement orders in real-time. This will inform the entire crew on board.

by a Cyber breach, regional commands and battle management centres can continue directing operations without interruption.

Exercise STEADFAST DUEL 2025 was the first operational-level NATO exercise to implement these distributed concepts at scale. It connected NATO's operational commands in a simulated 24/7 battlespace which mirrored the complexity of modern conflict. Participants trained day and night, adjusting their battle rhythm to strengthen NATO's ability to plan, coordinate, and fight as one Allied force across all domains.[4]

At the tactical edge, Decentralised Execution empowers operators to act with speed and initiative. Whether a fighter squadron adjusts its tactics mid-sortie due to unexpected air defences, or a naval task group exploits an opportunity to interdict hostile vessels, decentralisation ensures that decisions occur at the speed of relevance. In contested environments, waiting for higher-level approval is not an option. Initiative on all fronts is the key to maintaining dominance.

Digitalisation and AI-Enabled Decision-Making

The success of NATO's MDO relies on two interconnected pillars: digitalisation and interoperability. Digitalisation enables seamless data collection and processing through advanced technologies like cloud computing, AI, quantum systems, and 5G.

While AI may seem the logical choice for swift decision-making, it must be paired with legal considerations in line with the law of armed conflict (LOAC). Artificial intelligence (AI) mitigates cognitive overload by filtering, fusing, and prioritising sensor inputs, enabling faster and clearer decision-making than adversaries.[5] AI tools highlight anomalies, anticipate threats, and synthesise outcomes, allowing commanders to make rapid and confident decisions.[6]

The use of the NATO Maven Smart System (MSS) during STEADFAST DUEL demonstrated AI-enabled C2 in distributed decision-making. MSS integrates large language models and machine learning to consolidate siloed data sources into a unified and secure software platform. The swift six-month procurement process for MSS underscores NATO's recognition of the urgency in deploying disruptive technologies to enhance operational agility.[7]

The Evolving Commander's Intent

The operational environment requires an adaptable commander's intent that enables mission execution under degraded communication conditions and

information saturation. Beyond task orientation, it must encompass survivability measures and the mitigation of vulnerabilities arising from electronic warfare competition. Central to this is signature management, the systematic reduction of physical, electromagnetic, acoustic, thermal, and cyber emissions that adversaries exploit for targeting.

These factors indicate that a NATO mission commander must possess capabilities far beyond traditional joint operations. They must coordinate military actions across all five operational domains, synchronised with non-military instruments of power, to achieve converging effects at the speed of relevance.[8]

'We must treat our data links and battle management architectures as weapon systems that require constant, high-fidelity exercise.'

However, the resilience of distributed control is only as strong as the proficiency of the operators managing it. If the tools used in high-end synthetic training environments do not mirror the complexities of the live environment, particularly regarding TDL contention and jamming, we risk a cognitive disconnect. This is where the gap between NATO's current training systems and the requirements of a unified architecture becomes most apparent. To understand how to bridge this gap, we must look at current operational models.

Delta vs. CRC System Interface: Two Paths to C2 Excellence

To understand the evolution of NATO's Battle Management, we must examine two distinct yet increasingly convergent models: Ukraine's Delta system and NATO's Control and Reporting Centre System Interface (CSI). While their objectives of speed and resilience are shared, their underlying design philosophies offer distinct advantages for the Alliance.

Ukraine's Delta C2 system exemplifies a cloud-based, decentralised architecture that integrates real-time data from drones, satellites, and sensors. It serves as a unified data exchange platform across devices at all command levels, maintaining operational tempo even under the stress of cyberattacks or heavy electronic jamming.[9] During Exercise REPMUS 2025, Delta coordinated more than 100 unmanned platforms across the Maritime, Land, and Air domains, demonstrating remarkable resilience in contested environments. Deputy Minister Myronenko emphasised that while long-range systems require complex planning cycles, Delta's dispersed nodes enable near-real-time front-line responses, significantly reducing the 'sensor-to-shooter' timeline from days to minutes.[10] This success underscores a critical lesson: in an era where seconds matter, resilience stems from the ability to automate workflows and disperse control across a survivable network.

In contrast, NATO's Control and Reporting software, CSI, demonstrates the Alliance's structured, integrated approach to air C2. This NATO nations' hardware-software platform employs standardised multi-tactical data link protocols, such as Link-16, Link-11B, Variable Message Format (VMF), and Joint Range Extension Applications Protocol (JREAP), to ensure interoperability among aircraft, air defence systems, and command centres. CSI enables real-time mission coordination and a shared operational picture across fighter aircraft, Surface-Based Air and Missile Defence (SBAMD) units, and joint C2 platforms. With its unique governance structure, in which SHAPE also participates as a member state, NATO Communications and Information Agency (NCIA) developed a modular CSI software solution that effectively combines interoperability with cost efficiency.

Beyond its military utility, CSI supports the integration of ATC radars, meteorological data, and Air Traffic Management systems, aligning with Single European Sky ATM Research (SESAR) standards. By operating as a fully integrated solution rather than relying on the CRC as a 'middleman', CSI reduces dependency on voice communication and enhances operational safety through civil-military coordination. Furthermore, it processes critical non-real-time planning directives,

This CSI screenshot highlights enhanced situational awareness enabled by Link 16 over Internet Protocol via JREAP-C. By leveraging Tactical Data Links, operators no longer rely solely on radio communication. Instead, they gain immediate access to critical information, such as surveillance data, type of platform, flight parameters, engagement orders, weapons status, and free text messages, delivered in real time for all operators in the TDL network.

notably the Air Tasking Order (ATO) and Airspace Control Order (ACO), which govern the allocation of missions and the deconfliction of airspace. While Delta excels in the 'bottom-up' agility of the front line, CSI ensures the 'top-down' precision and unity required for complex coalition air operations.

Although not used in practice, Ukraine's adoption of CSI could further enhance joint NATO operations. Integrating the structured interoperability of the NATO standard with the agile, decentralised approach of Delta could yield a hybrid model that combines tactical adaptability with the strategic coherence required for future Alliance missions. Moreover, Delta's dispersed control philosophy allows operators to coordinate and execute tasks from virtually any device, laptops, smartphones, or desktop systems, ensuring continuous operational resilience even in highly contested environments.

Closing the Proficiency Gap: The Training Imperative

The technical sophistication of systems like Delta and CSI reveals the importance of data-driven and decentralised operations. However, as noted in recent iterations of Exercise STEADFAST DUEL, a persistent training gap remains. While our operational architecture is evolving, the synthetic environments we use to prepare our forces often remain disconnected from reality.

Currently, the CSI simulation suite effectively replicates operational conditions for certain ATO execution tasks. However, simulated Article 5 scenarios in the STEADFAST series of exercises can sometimes become audience-driven rather than operationally realistic. A gap analysis of recent exercises reveals that tactical decisions would differ significantly if participants were forced to contend with real-world technical limitations, such as multi-TDL contention or hostile jamming. In a dispersed fight under high-stress conditions, an operator cannot be expected to remain proficient if their training software differs from their operational interface, or if the training environment is 'sanitised' of the electronic warfare complexities they will face in the field.

Effective Distributed Control in contested environments requires NATO to align its doctrine with its technology through a unified battle management software interface, one that is used for both training and operations. Exercise UEDEM AWAKENING 2025 demonstrated the value of this approach through a Danish Air Control Wing initiative that integrated operators from the Swedish Air Force (SAM Allocators) and the Royal Danish Navy (AAW) by utilising Link 16 simulators and procedures for

Air traffic specialists analyse real-time radar data to monitor designated airspace sectors, ensuring safe separation and efficient routing for all aircraft.

Integrated Air and Missile Defence (IAMD) weapons coordination and engagements, while exchanging the Common Operational Picture (COP) through Link 16 over JREAP-C. By treating TDL switch actions and network management as integral combat skills rather than specialist tasks, NATO can build the muscle memory required for combat readiness in MDO. Synchronising higher headquarters with CRC levels and expanding CSI training for both staff and operators will be vital to reinforcing the train as you fight principle.

Finally, the comprehensive integration of EUROCONTROL's Air Traffic Management data and Airspace Management data into CSI provides an additional operational advantage. When seamless data exchange is trained and prioritised over traditional voice communications, decisions regarding IAMD procedures can be made more rapidly, ultimately contributing to safer and more secure airspace in peacetime, crisis, and conflict.

The Road to 2030: The NATO Digital Backbone

As we look toward the future, the NATO Digital Backbone serves as the Alliance's 'North Star' for this C2 transformation. Often mentioned but rarely defined in detail, the Digital Backbone is the federated connectivity and data-transport framework designed to enable MDO by 2030. It is intended to provide a secure, scalable 'cloud-first' environment that interconnects sensors, decision-makers, and effectors across all domains and civilian mission partners.

The Digital Backbone is not just a hardware upgrade; it is a resilience architecture. It integrates advanced cybersecurity, data fabric services, and AI-enabled decision tools into a single, interoperable ecosystem. While the cutting-edge C2 technologies being matured through experimentation today are impressive, we must recognise that MDO is occurring now. The Digital Backbone provides the technical foundation, but its success depends entirely on the proficiency of the personnel operating within it.

Conclusion: Synchronising Architecture and Action

The conflict in Ukraine has provided a humbling reminder that the side that can fuse data and execute decisions fastest holds the advantage. NATO's transition toward Centralised Command, Distributed Control, and Decentralised Execution is the correct

doctrinal response to this reality. Systems like Delta and CSI provide the architectural blueprints for this new way of war, offering the speed and interoperability necessary to secure Allied interests.

However, technical superiority is a hollow advantage if it is not matched by realistic preparation. We cannot afford to have a disconnected force that possesses the tools for victory but lacks the routine practice required to use them in a contested environment. To achieve true Decision Advantage, NATO must bridge the gap between its operational systems and its training simulations. We must treat our data links and battle management architectures as weapon systems that require constant, high-fidelity exercise.

The NATO Digital Backbone will provide the infrastructure, but our commitment to the train as you fight principle will provide the edge. As this new mindset takes hold across the Alliance, we must act now to seize every opportunity to build muscle memory, synchronise our efforts, and ensure that when the next crisis emerges, NATO is not just technically ready, but operationally dominant. ●

1. General Milley, M. and General Townsend S., 'The U.S. in Multi-Domain Operations 2028', US ARMY, [website], February 26/2021, https://www.army.mil/article/243754/the_u_s_army_in_multi_domain_operations_2028, (accessed 2 December 2025).
2. NATO, 'Digital Transformation: Building the Foundations for a Multi-Domain Operations Enabled Alliance', [website], October 02/2025, https://www.act.nato.int/article/data-centricity/, (accessed 15 December 2025).
3. US ARMY Europe and Africa, US assets depart for DEFENDER 25 exercise alongside Allies and partners, United States European Command, https://www.eucom.mil/article/43163/press-release---us-assets-depart-for-defender-25-exercise-alongside-allies-and-partners, (accessed 2 December 2025).
4. NATO, 'NCIA enables Steadfast Duel 25, NATO's largest computer-assisted command post exercise', Newsroom, [website], 29 October/2025, https://www.ncia.nato.int/newsroom/news/ncia-enables-steadfast-duel-25-natos-largest-computerassisted-command-post-exercise, (accessed 2 December 2025).
5. Rand, Morgan Forrest E. et al, 'Military Trends and the Future of Warfare: The Changing Global Environment and Its Implications for the U.S. Air Force', [website], 27 May/2020, https://apps.dtic.mil/sti/html/tr/AD1099436/, (accessed 16 December 2025).
6. Department of Defense, 'Data, Analytics and Artificial Intelligence Adoption Strategy, Accelerating Decision Advantage', [website], June 27/2023, https://media.defense.gov/2023/nov/02/2003333300/-1/-1/1/dod_data_analytics_ai_adoption_strategy.pdf, (accessed 16 December 2025).
7. NATO, NATO acquires AI-enabled warfighting system, Newsroom, [website], 14 April/2025, https://www.ncia.nato.int/newsroom/news/nato-acquires-aienabled-warfighting-system, (accessed 3 December 2025).
8. NATO, 'Multi-Domain Operations in NATO – Explained', Article, [website], 05 October/2023, https://www.act.nato.int/article/mdo-in-nato-explained/, (accessed 8 December 2025).
9. Ministry of Defence of Ukraine, 'Ukrainian combat system DELTA became primary command platform for combined multinational team at NATO exercises', News, [website], 3 October/2025, https://mod.gov.ua/en/news/ukrainian-combat-system-delta-became-primary-command-platform-for-combined-multinational-team-at-nato-exercises, (accessed 15 December 2025).
10. Epstein, Jake Ukraine's digital war tool cut the time between finding and striking Russian targets from days to minutes', Business Insider, 24 November 2025, https://www.businessinsider.com/ukraine-delta-battlefield-tool-slashed-strike-times-on-russian-targets-2025-11, (accessed 16 December 2025).

ABOUT THE AUTHOR

Commandant Peter Vanderostyne
BEL Air Force, JAPCC

Commandant Peter Vanderostyne earned a Master's degree in military and Aeronautical Science from the Royal Military Academy, Brussels, in 1992. He began his career at CRC Glons as a Fighter Controller and Electronic Warfare and Surveillance Specialist and later served as Operations Officer. In 1999, he joined NAEW&CF Geilenkirchen as Weapons Instructor and Fighter Allocator. Returning to the CRC in 2004, he assumed the roles of Operations & Training Officer and Master Controller. At CAOC UEDEM (2006), he held several roles, including Air Surveillance Officer, Fighter Coordinator, Senior Director (AAR control 603rd Sqn at Fungo Radar, Italy), Command and Control Duty Officer, and Air Operations Planning SME. He also served twice as Military Assistant to the Commander, CAOC UE. He supported NATO missions, including Allied Force, Deliberate Guard, ISAF twice, Baltic Air Policing, Eagle Assist, and Unified Protector. Renowned for expertise in Battle Management and Airspace Planning, he pioneered Afghanistan's first Common Operational Picture and revolutionised frequency management from monthly to daily assignments, strengthening NATO's operational agility. Having witnessed interoperability shortcomings during operations, he continues, as a reservist, to support efforts with JAPCC, HQ AIRCOM, and HQ ACT to establish a NATO Joint Interoperability Division and Data Link Training Centre to enhance decision superiority across the modern battlespace.