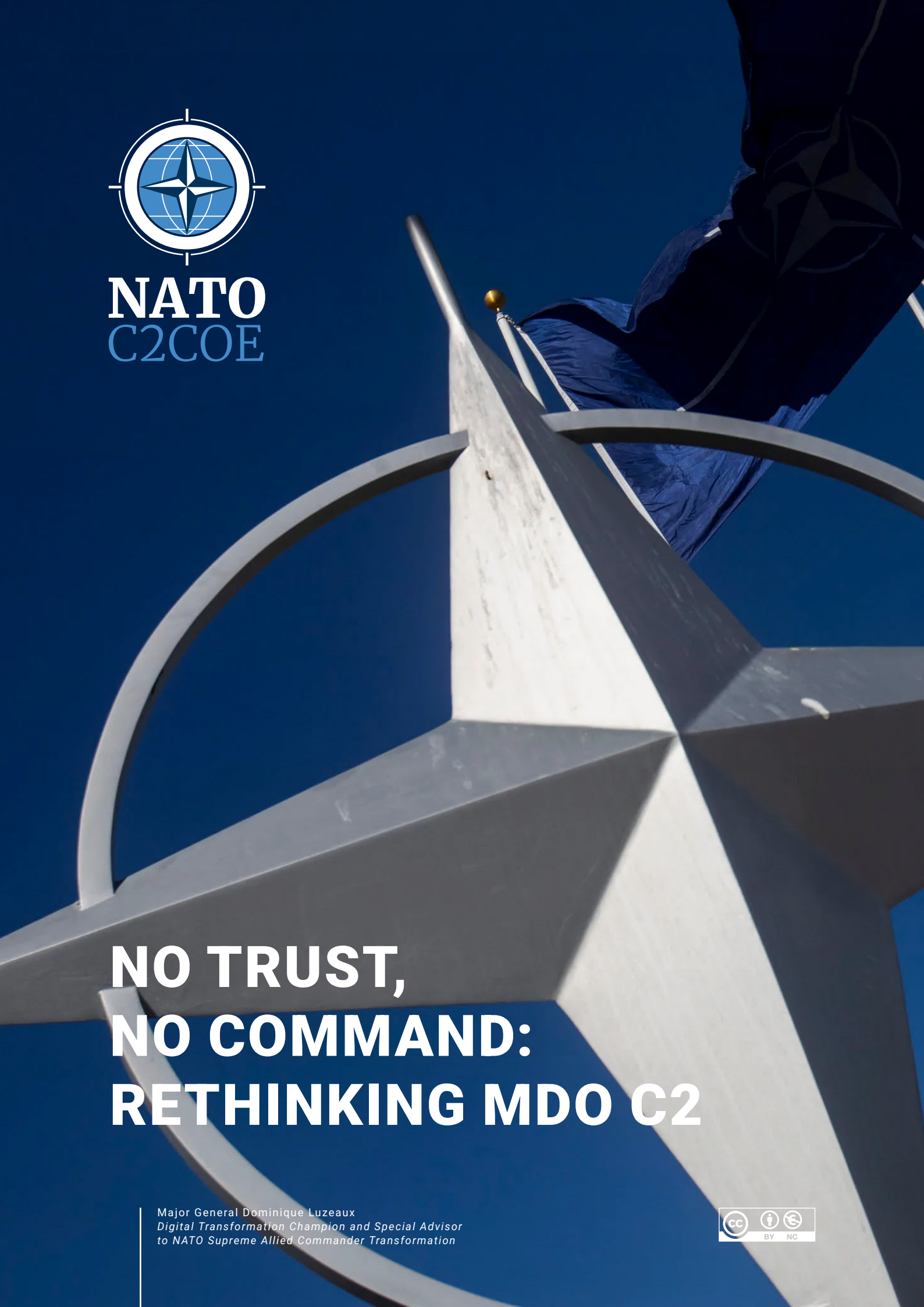


NATO
C2COE

NO TRUST, NO COMMAND: RETHINKING MDO C2

Major General Dominique Luzeaux
Digital Transformation Champion and Special Advisor
to NATO Supreme Allied Commander Transformation

CC BY NC

Introduction

This article defines the essential distinctions between current Command and Control (C2) and Multi-Domain Operations Command and Control (MDO C2) constructs. It reflects a transition from platform-centric to data-centric operations, from hierarchical control structures to adaptive orchestration, and from a focus on technical interoperability toward the achievement of semantic and cognitive coherence. Ultimately, the effectiveness of MDO C2 depends on the ability to sustain shared understanding, maintain trust in distributed systems, and continuously adapt to an operational environment defined by complexity and contestation. This transformation is conceptual, organizational and technological.

A target reference architecture suitable for coalition and multi-echelon employment is derived. It describes MDO C2 as an integrated, distributed system in which shared meaning, governed data products, composable services, and continuous assurance are as decisive as sensors and shooters. It explains the operational contribution of edge computing with specific attention to contested environments and coalition operations, and emphasizes the data, semantic, identity, and assurance fabrics as foundational capabilities, without which MDO C2 turns into a set of connected but incoherent domain systems.

1 - Command philosophy, operational logic and technical implementation of current C2

Current C2 may be understood as a structured, hierarchical system in which decision-making authority is exercised predominantly through structured command chains, operations are organized along domain-specific lines, and execution follows sequential planning cycles supported by platform-centric capabilities.

Command is exercised through well-defined hierarchical chains, within which authority and responsibility are closely linked to organizational position. Decision-making is shaped by sequential processes, and control mechanisms emphasize predictability, stability, and the orderly execution of plans. This model reflects an environment in which information flows could be managed through structured planning, where operational tempos are comparatively stable, and domain boundaries remain clearly delineated.

The operational logic of current C2 is primarily platform-centric, system-specific and domain-oriented. Domain actions are coordinated through deconfliction mechanisms and pre-arranged synchronization. The resulting operational picture is often fragmented in time and across domains, requiring significant human effort to aggregate and reconcile information from multiple sources.

Information management similarly transforms. Current C2 frequently treats data as an input to staff processes, with periodic information flows tied to reporting cycles. Interoperability efforts primarily focus on technical connectivity, enabling systems to exchange data without necessarily ensuring a shared understanding of its meaning. Decision-making is constrained by human cognitive capacity and structured processes. Hence, decisions tend to be reactive, based on the observation and verification of events, and risk is managed through control mechanisms designed to minimize uncertainty.

Current C2 architectures are characterized by centralized command posts and preconfigured communication networks. Systems are often monolithic, with limited flexibility, and resilience is primarily achieved through redundancy measures designed to ensure continuity under degradation.

2 - How does MDO C2 differ?

MDO C2 refers to a distributed, data-centric approach designed to achieve synchronized effects across domains and echelons through continuous, adaptive decision-making. This approach relies on advanced digital infrastructures, real-time data exchange, and increasing levels of machine support.

In MDO C2, authority and control remain anchored in command accountability, but the effective exercise of authority depends increasingly on access to timely data, the ability to interpret it consistently across participants, and the capability to act at operational tempo in conditions of uncertainty, deception, and disruption. The dominant tendency is the orchestration of cross-domain effects, with planning and execution conducted in an integrated manner, enabling actions in one domain to produce decisive outcomes in another. Synchronization becomes continuous rather than pre-scheduled.

The operational environment is represented through unified, data-driven models that allow for persistent awareness and dynamic optimization of actions. Data is made accessible across organizational and domain boundaries through common frameworks, enabling continuous, real-time exchange. Interoperability extends beyond technical compatibility to encompass semantic and cognitive dimensions, ensuring that data is interpreted consistently across systems and actors. The integration of artificial intelligence and machine learning enables automated data fusion, pattern recognition, and decision support. Within this paradigm, data itself becomes a primary maneuver space, shaping the conduct and outcome of operations.

Decision-making becomes a continuous process, capable of aligning distributed actors toward a shared operational outcome in real time, characterized by dynamic delegation, rapid adaptation, and cross-domain integration. Through the integration of machine capabilities, static representations are replaced by dynamic decision-support environments capable of processing large volumes of data in real time. Decision processes become increasingly predictive, allowing commanders to anticipate developments and act proactively when conditions change.

Risk management evolves from verification-based approaches to models based on continuous assurance, where trust is maintained through ongoing validation, transparency, and performance monitoring. As a result, operational advantage shifts toward the ability to achieve faster decision superiority than the adversary, in terms of speed, accuracy, and coherence.

MDO C2 is enabled by a fundamentally different technological foundation. Distributed command nodes operate across a continuum from centralized facilities to forward-deployed edge environments, supported by cloud and edge computing infrastructures. Networks are adaptive and resilient, capable of reconfiguring dynamically in response to disruption. Systems are modular and composable, allowing capabilities to be assembled and reassembled according to operational requirements. Resilience is achieved not only through redundancy but through the capacity for dynamic reconfiguration and distribution, ensuring continuity of function under contested conditions.

3 - Operational Implications

The transition from current C2 to MDO C2 has significant operational implications. Temporal dynamics shift from discrete, cycle-based processes to continuous, adaptive flows of activity, reducing latency between observation, decision, and action. The conceptualization of the battlespace evolves from a geographically segmented and domain-specific construct to a fluid, networked environment in which effects propagate across domains.

At the same time, the nature of vulnerabilities changes. While traditional C2 systems are primarily exposed through physical nodes such as headquarters and communication hubs, MDO C2 introduces new dependencies on data integrity, semantic consistency, and the reliability of algorithms.

In the current C2 paradigm, human operators bear the primary responsibility for processing information, synthesizing inputs, and making decisions. This results in significant cognitive demands and limits the speed at which decisions can be made. Trust in the system is largely based on human verification and control over processes.

MDO C2 redefines the relationship between humans and machines. Machine learning and artificial intelligence tools assume an increasing role in processing information, identifying patterns, and generating recommendations. Human actors retain authority and accountability but act increasingly as supervisors and orchestrators of machine-assisted processes. This redistribution of functions reduces cognitive burden while enabling faster and more informed decisions. Trust is established through mechanisms that provide transparency, quantify confidence levels, and ensure continuous validation of system outputs.

4 - A need for a revised system-of-systems architecture

The effective implementation of MDO C2 depends on: the establishment of federated data architectures that ensure both accessibility and governance; the deployment of edge computing resources enabling low-latency decision-making; the integration of artificial intelligence for advanced data exploitation; the development of robust semantic interoperability frameworks to ensure shared understanding across diverse actors and systems; and finally continuous assurance mechanisms required to maintain trust in systems that are inherently dynamic and distributed.

The enabler of this shift is architecture. The decisive question is how flexibly in-fielded or under development capabilities can be reconfigured under pressure, no longer what type or number of platforms a force possesses. Traditional systems bind functions to platforms, creating fragility when assets are lost or conditions change. In contrast, a system-of-systems architecture decouples functions from hardware, transforming the force into a fluid adaptive network, capable of maintaining function despite attrition and disruption. Within this architecture, software becomes the true center of gravity. Hardware defines what is possible, but software determines what is actually done. It enables real-time reconfiguration, coordination across domains, and the scaling of operations to large numbers of systems. Software allows a platform to change role, adapt to new conditions, and integrate into evolving operational constructs without physical modification. The result is a force whose capabilities are not fixed at procurement but can be continuously reshaped during operations.

A target reference architecture for MDO C2 is therefore intended to serve as a stable conceptual baseline for capability development, interoperability engineering, and force design in contested, data-saturated operational environments. It is designed to deliver persistent cross-domain synchronization of effects by treating data as an operational resource, enabling distributed execution under mission command, and sustaining trustworthy machine-enabled decision advantage. It assumes that the operational environment is characterized by cyber contestation, denial and deception, intermittently available communications, and coalition constraints that impose differentiated access and releasability.

4.1 - Architectural overview

The central architectural proposition is that MDO C2 cannot be achieved through domain-specific C2 systems merely connected by interfaces. It requires a federated data and policy foundation able to sustain shared meaning, continuous assurance, and composable mission applications.

It is defined as a layered and federated system comprising an edge-to-enterprise compute continuum, a unified identity and policy foundation, a federated data plane, explicit semantic and knowledge services, governed analytics and model operations, composable mission services, role-tailored mission applications, and cross-cutting observability and assurance. Therefore it treats the data plane, the service plane, and the assurance plane as foundational elements rather than implementation details.

The reference architecture will be expressed through multiple mutually reinforcing views. The operational view describes what the system must accomplish across the sense–understand–decide–act continuum. The logical view defines the layers of capability required to produce those outcomes and to maintain coherence across echelons and domains. The technical view expresses how those layers are instantiated across an edge-to-enterprise continuum while preserving resilience, governance, and trust.

4.2 - Operational reference architecture

The target MDO C2 construct is organized around a continuous operational cycle in which sensing, understanding, decision support, orchestration, execution, and learning are conducted persistently rather than as discrete, sequential phases. Sensing and collection provide multi-domain, multi-source acquisition and enable collection management, including the tasking of organic, allied, and commercial sources. Data and knowledge functions ingest and curate information as governed "data products" and sustain a unified logical battlespace representation while allowing distributed data ownership and sovereign control. Understanding and fusion functions integrate multi-source information into coherent tracks, while explicitly representing uncertainty, provenance, confidence, and incorporating deception-aware analytics.

Decision support functions generate courses of action and evaluate them against operational constraints, rules of engagement, policy caveats, collateral considerations, logistics feasibility, and risk tolerances. Orchestration and execution functions translate intent into synchronized actions across domains and echelons and maintain real-time coordination between kinetic and non-kinetic effects, including cyber, electromagnetic activities, and space-enabled contributions. Assurance, governance, and learning functions continuously evaluate system posture, model performance, data integrity, and mission outcomes, then feed observations back into tactics, data curation, and analytic models to sustain adaptation and learning.

4.3 - Logical reference architecture

The logical architecture is expressed as a layered stack that separates foundational fabrics from mission services and user-facing applications, ensuring that rapid mission adaptation does not require rebuilding the underlying system.

The fundamental layer consists of an access and edge fabric. It provides computing and networking across tactical edge nodes, operational hubs, and enterprise environments. It is designed to function under intermittent connectivity and to support low-latency processing forward while enabling policy-governed synchronization across the force when connectivity permits. It is the condition for maintaining command continuity when communications cannot be assumed.

On this fabric rests an identity and policy layer consistent with zero trust principles. The function of this layer is to provide identity for personnel, devices, services, and workloads, and to enforce attribute-based access decisions that are continuously evaluated in light of mission context, nationality, clearance, need-to-share, and releasability. Authorization is continuous and context-aware rather than session-based, and it is supported by attestation and cryptographic key management appropriate to both long-lived platforms and contested networks. This foundation is indispensable for coalition operations because it allows differentiated access and controlled sharing to be enforced as a real-time property of the system, rather than as a potentially after the fact predetermined procedure.

The centerpiece of the architecture is the federated data fabric. It provides ingestion of streaming and batch data, cataloguing and discovery of data products, mechanisms for lineage, provenance, labeling, and handling markings, and policy-driven dissemination. It enables event distribution for operational flows and supports query federation and data virtualization so that information can be accessed logically without requiring centralization of storage or ownership. The core requirement is federation without fragmentation: participants must retain sovereign control of data where necessary, but the force must maintain coherence

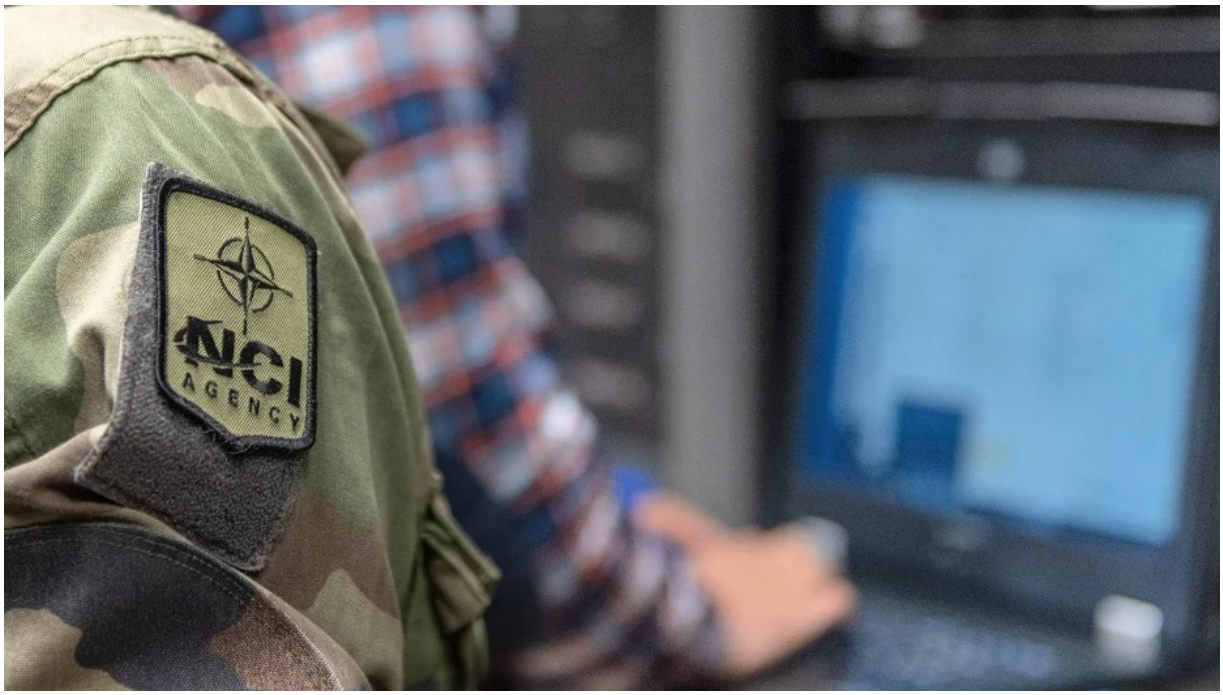
of discovery, timeliness, and usability under agreed governance. This layer must also incorporate integrity mechanisms and deception-relevant indicators so that the system can distinguish absence of data from adversarial manipulation of data.

Because MDO C2 fails when participants do not interpret information consistently, the architecture explicitly includes a semantic and knowledge layer. It maintains operational ontologies and controlled vocabularies, supports mediation between national and platform-specific data models. It also enables entity resolution so that the same object, unit, event, or activity is consistently represented across multiple sources. It represents constraints and policies such as rules of engagement, safety boundaries, and selected procedures as machine-consumable artifacts, to support automated checking, explainability, and traceability.

The analytics and model operations layer provides fusion, prediction, recommendation, and decision-support functions while ensuring governability, and mechanisms for transparency and explanation suitable for operational trust and command accountability through traceability. This requires controlled model registries, evaluation and test frameworks, drift and degradation detection, confidence estimation, red-teaming pipelines.

The mission services layer provides reusable, composable building blocks such as track management, geospatial services, tasking and orchestration services, constraint-aware course-of-action support, and collaboration workflows. These services are accessed through governed interfaces and are designed to be assembled into mission-specific applications without having to rebuild the entire ecosystem: they are API-first, versioned, discoverable, and governed through the identity and policy fabric. Mission applications constitute the user-facing layer and are expressed as role-tailored tools for commanders, staff officers, and operators. They are designed to be thin client applications and can evolve rapidly, while the underlying services remain stable, governed, and interoperable.

Observability, assurance, and compliance span all layers of the entire architecture. This cross-cutting capability provides telemetry, auditability, policy compliance monitoring, cyber defense integration, resilience scoring, and continuous evaluation of both security posture and analytic performance. It is the enabling condition for continuous assurance approaches and for maintaining trust in a system that must adapt quickly, operate under degraded conditions, reconfigure under attack or failure, and incorporate autonomous or semi-autonomous functions.



4.4 - Technical reference architecture and implementation criteria

The technical architecture is defined through three interacting planes: the data plane, the service plane, and the control plane. The data plane standardizes streaming and batch exchanges, including the representation of data products with metadata for provenance, confidence, handling markings, and expiry. The service plane defines service discovery, API gateways, and policy enforcement points attached to service access pathways. It formalizes compatibility and versioning practices so that coalition participants can integrate without destabilizing the ecosystem. The control plane orchestrates workloads across edge, theatre, and enterprise environments and maintains configured posture, identity distribution, key management, and revocation mechanisms consistent with zero trust principles.

Deployment is expressed along a core to edge continuum. Tactical edge instances provide local fusion, filtering, caching, and a minimum essential set of services required for mission continuation under disconnection. Operational and theatre instances provide higher-scale fusion, orchestration, wargaming, and coalition workflows, emphasizing high availability under contested network assumptions. Enterprise and strategic instances support model training, long-horizon analytics, institutional knowledge curation, software delivery pipelines, and lessons-learned integration. Synchronization between these environments is policy-governed and bandwidth-aware, emphasizing controlled dissemination rather than indiscriminate replication.

An implementation is consistent with this target reference architecture only if federation is achieved without operational fragmentation, meaning that participants can retain data sovereignty while maintaining coherent discovery and shared meaning.

Policy-driven sharing must be enforceable, auditable, and adaptable to changing coalition constraints. Degraded modes must preserve meaningful mission capability under partial communications and partial data conditions. Mission capabilities must be composable, such that workflows can be assembled from trusted services without rebuilding the stack. Continuous assurance must be operationally real, meaning that security, safety, and model performance are monitored continuously and can trigger reconfiguration or rollback. Decision acceleration must be accompanied by traceability, ensuring that the system can reconstruct who decided what, under which authority, based on which evidence and confidence levels.

An implementation that provides connectivity but cannot sustain semantic coherence, cannot enforce coalition caveats at machine speed, or cannot continue functioning under partition and disruption does not meet the intent of MDO C2.

5 - Principal architectural challenges

The most operationally critical challenge is resilience under attack and disruption. The reference architecture addresses this challenge through distribution, partition tolerance, graceful degradation, and pervasive observability to enable rapid recovery and adaptive reconfiguration.

The most politically sensitive challenge is coalition releasability and caveat enforcement. This is mitigated by integrating identity, attribute-based access control, and policy decision/enforcement mechanisms with explicit release workflows and data product labeling.

One technical challenge is trust in automation and AI. It is addressed by embedding model operations governance and continuous assurance, including confidence scoring, drift detection, evaluation frameworks, and explanation pathways that support human accountability.

Another technical and coalition challenge is semantic coherence. By explicitly introducing a semantic and knowledge layer and by requiring machine-readable constraints and policy artifacts, the proposed architecture ensures that shared meaning can be enforced and assessed rather than assumed.

However, the main obstacle to enable MDO C2 is the availability of data and how to cope with the absence of reliable and trusted data. MDO C2 must natively be designed for an environment in which data is abundant, fragmented, contested, politically constrained, technically heterogeneous, and only partially trusted. The central challenge is no longer simply to collect more data or to integrate more sensors into a common operational picture. It is to determine what can be acted upon when some data is absent, delayed, degraded, contradictory, inferred, withheld, or supplied by actors whose own systems and incentives differ from those of the coalition.

Uncertainty is not merely an external condition produced by the adversary or the environment. It is also structurally produced by the federation itself. Data may be owned by different nations, governed by different classification rules, generated by different domains, processed by different systems, hosted on different infrastructures, and constrained by different legal, contractual, and political regimes. Some of the most operationally relevant data may come not from military systems, but from civilian organizations such as commercial satellite providers, telecommunications operators, cloud service providers, logistics companies, energy operators, transport authorities, emergency services, and critical infrastructure owners. MDO C2 must therefore operate not on the assumption of data completeness, but on the assumption of permanent partial visibility.

The implication is profound: MDO C2 must evolve from a data-centric command architecture toward a confidence-aware command architecture. It must not merely display what data is known. It must expose how well it is known, how fresh it is, where it comes from, how it was transformed, what dependencies it relies upon, what policy restrictions apply to it, and what level of operational risk would be incurred by acting upon it.

5.1 - The absence of data as operational information

A first requirement is to treat missing data as a first-class operational signal. In many systems, absence of data is invisible. The map simply has fewer tracks, the dashboard shows fewer indicators, or the database lacks entries. This is dangerous because it allows decision-makers to confuse absence of evidence with evidence of absence. In MDO C2, the fact that an expected data source has gone silent must itself become visible, classified, interpreted, and operationally assessed.

The system must distinguish between several different forms of absence. Data may be missing because it does not exist, because the relevant sensor did not observe the event, because a federated partner is technically disconnected, because a classification rule prevents release, because a national caveat blocks sharing, because

a civilian provider is suffering an outage, because a cyberattack has compromised the feed, or because an adversary has deliberately disrupted or spoofed the channel. These conditions have very different operational meanings. A missing logistics update from a civilian transport provider does not carry the same implications as a missing air track from a military radar network or a missing target validation from a national intelligence authority.

Consequently, MDO C2 must represent operational objects, and at the same time the state of the data ecosystem that produces those objects. Commanders should be able to see the disposition of forces, targets, infrastructure, and effects, but also the confidence, freshness, and reliability of the underlying information. The operational picture must be accompanied by a data-quality picture. This does not mean overburdening commanders with technical metadata. It means translating data reliability into operational consequences: which decisions are affected, which areas are now less certain, which courses of action depend on degraded sources, which risks have increased because a specific federated or civilian input is no longer trustworthy.

5.2 - Trust as a computable operational variable

In this environment, trust can no longer remain a purely institutional or political assumption. It must become a computable, contextual, and dynamic variable. Commanders and staff officers must be provided with a disciplined way to assess the reliability of information under conditions of heterogeneity and contestation.

Trust is not a single score. It is a composite assessment that includes the reliability of the source, the freshness of the data, the completeness of the reported attributes, the consistency of the data with other independent sources, the provenance of the information, the robustness of the technical chain that produced it, the assurance level of the system, and the relevance of the data to the specific operational decision. A commercial satellite image, for example, may be highly reliable for confirming physical infrastructure damage, moderately reliable for assessing recent movement if latency is significant, and insufficient on its own for time-sensitive targeting. A civilian traffic feed may be valuable for assessing mobility, congestion, evacuation patterns, or sustainment routes, but may require stringent validation in a contested environment where mobile networks, GPS signals, or digital platforms may be disrupted or manipulated.

Trust must therefore be computed at the level of the data element, not only at the level of the organization providing it. A trusted partner can produce low-confidence information if the data is stale, incomplete, or derived from a compromised dependency. Conversely, a civilian or commercial source with limited military assurance may still provide useful information if it is timely, independently corroborated, and appropriate for a lower-risk decision. The essential question is not whether a source is trusted in the abstract, but whether a specific item of information is sufficiently reliable for a specific decision in a specific context.

This requires a confidence envelope around operational data. Each relevant entity, track, report, event, target, effect, or infrastructure status should carry information about source, timestamp, confidence, completeness, provenance, releasability, transformation history, and dependency chain. Confidence must degrade over time, especially for dynamic objects. It must also degrade when upstream dependencies become unreliable, when sources begin to diverge, when anomalies appear in reporting behavior, or when the broader environment becomes more contested.

5.3 - Continuous trust assurance

Trust assurance is not a one-time accreditation event. Initial certification, security accreditation, contractual assurance, and technical testing remain necessary, but they are insufficient once the force enters a contested environment. Under adversarial pressure, sources that were previously reliable may become degraded, spoofed, compromised, delayed, or selectively manipulated. Trust must therefore be continuously validated.

The first mechanism is cross-source corroboration. Important operational claims should be checked across independent and heterogeneous sources whenever possible. A position derived from one sensor can be compared with another domain, another nation, another collection method, or a civilian source. However, corroboration must not be treated naively: dependencies between different sources must be mapped and hidden common-mode failure must be identified (e.g., several feeds may appear to confirm one another while relying on the same satellite constellation, or the same upstream data broker).

The second mechanism is adversarial consistency checking through anomaly detection, behavioral monitoring, and comparison against independent observations. The system must ask not only whether the data appears plausible, but whether it could plausibly be the result of deception. In contested environments, a clean and coherent data feed may be more dangerous than an obviously degraded one if it has been manipulated to preserve superficial credibility. This is particularly important for positioning, navigation, timing, cyber telemetry, target identification, and digital infrastructure status.

The third mechanism is trust drift monitoring. A source's reliability is not static. Its behavior over time matters. Unexplained gaps, sudden changes in reporting frequency, deviations from historical accuracy, inconsistent metadata, or abnormal patterns of agreement with other sources may indicate degradation or manipulation. Civilian sources require particular attention because their systems may not have been engineered for wartime contestation. They may offer excellent peacetime performance while having unknown failure modes under cyberattack, electronic warfare, legal pressure, business disruption, infrastructure damage, or adversarial infiltration.

5.4 - Civilian data as a strategic enabler and a trust challenge

The integration of civilian data is one of the defining characteristics of modern MDO C2. Military operations increasingly depend on information from civilian and commercial ecosystems. Commercial satellite imagery can provide persistent observation, telecommunications operators can provide network status and mobility indicators, cloud providers can support data processing and resilience, logistics firms can reveal supply chain constraints, energy operators can report grid conditions, and emergency services can provide information about population movement or infrastructure damage. This civilian contribution may become essential to mobility, sustainment, resilience, cyber defense, protection of critical infrastructure, humanitarian coordination, and strategic communication.

However, civilian data enters the military C2 environment with different assumptions. Civilian organizations are not normally organized under military command authority. Their incentives are shaped by business continuity, legal compliance, safety obligations, customer protection, contractual commitments, and national regulation. Their systems may be highly capable but optimized for efficiency, scale, and availability rather than for survival under systematic adversarial attack.

This creates a structural trust asymmetry. Military sources are usually embedded in doctrine, operational procedures, and classification frameworks. Civilian sources are governed by contracts, regulation, technical interfaces, and partnership mechanisms. They may be highly reliable in peacetime, but less transparent under stress. Their data may be affected by privacy law, commercial confidentiality, national jurisdiction, or platform-specific limitations. It may also contain biases: traffic data may overrepresent populated areas, logistics data may reflect commercial flows rather than military priorities, and satellite data may be constrained by revisit rates, weather, collection priorities, or commercial tasking limitations.

MDO C2 must therefore include a confidence translation layer for civilian data. Civilian metadata is rarely expressed in military operational terms. A commercial provider may offer timestamp, resolution, service availability, latency, and contractual service levels. The military system must translate these into operational confidence, mission relevance, dependency risk, and permitted use. Civilian data should be integrated where

it adds operational value, but its influence on decisions must be governed by trust thresholds, validation requirements, risk categories, and explicit confidence constraints.

5.5 - Decision-making under uncertainty and degraded-mode operations

Once trust is computed and validated, it must shape decision thresholds, course-of-action comparison, delegation of authority, synchronization mechanisms, and degraded-mode transitions. The central shift is from deterministic decision-making to trust-weighted decision-making. A commander is not simply presented with a recommendation, he is shown the degree to which that recommendation depends on uncertain, stale, inferred, contested, or civilian-derived data. Two courses of action may have similar expected effects, but one may depend heavily on high-confidence intelligence while another may be more robust under data loss. In a degraded environment, the more robust option may be preferable even if it is less efficient under ideal conditions.

Trust also affects the level of automation. In high-confidence environments, some recommendations, alerts, and coordination actions may be automated or semi-automated. As trust declines, the system should shift toward human-in-the-loop validation, conservative rules, additional confirmation, or mission-command fallback. If trust falls below a critical threshold, the system should not continue to optimize as if the underlying picture were reliable.

This is particularly important for cross-domain synchronization which requires high trust in timing, availability, identity, location, and dependencies. When confidence decreases, the system must shift from tight orchestration to looser coordination. It must preserve coherence through commander's intent, decision envelopes, pre-agreed courses of actions, and delegated authority rather than through continuous real-time optimization.

MDO C2 must assume that degradation is not an exception but a normal operating condition. The loss of data from a federated partner, the degradation of civilian infrastructure, the disruption of a cloud region, the unavailability of commercial imagery, or the silence of a national sensor must not cause operational paralysis. The architecture must support predefined degraded modes and should know what constitutes nominal operation, partial degradation, severe degradation, and autonomous or local-only operation. Each mode should define the minimum viable data required to continue the mission, the decision authorities that shift to subordinate levels, the rules for substituting data sources, the constraints on automated recommendations, and the conditions under which operations must pause, continue, disperse, or revert to pre-planned options.

A degraded mode is not a failure state: it is an alternate command regime. It allows operations to continue with reduced precision, reduced tempo, or reduced ambition, but without losing coherence. It also prevents false precision. A system that continues to display an apparently complete operational picture after key data sources have failed is more dangerous than a system that visibly degrades.

By implementing such a confidence-aware command architecture, the added value is resilience. The force can continue to operate when data is incomplete. It can adapt when trust declines. It can shift from dynamic optimization to mission-command execution. It can preserve tempo without losing sight of risk. It can integrate civilian and commercial capabilities while maintaining operational prudence. It can expose hidden dependencies before they become failures. Above all, it can prevent the most dangerous failure mode in digital command systems: the presentation of certainty where no certainty exists.

Conclusion

The transition from current C2 to MDO C2 is defined by a shift from hierarchical, platform-centric control toward distributed, data-centric orchestration of cross-domain effects, thereby ensuring resilience, adaptability, and effectiveness in highly contested, coalition-based operational environments. This shift requires not merely improved connectivity but a reference architecture that elevates federated data governance, semantic coherence, identity and policy enforcement, composable mission services, and continuous assurance to foundational status.

MDO C2 must be built on the recognition that future operations will depend on data that is distributed, heterogeneous, contested, and only partially trusted. Some of this data will come from military federates, some from national systems, some from commercial providers, and some from civilian organizations whose infrastructures were not originally designed for warfighting. The challenge is not simply connecting these sources. The challenge is to determine how much confidence can be placed in each contribution, how that confidence changes under stress, and how it should affect decisions.

The essential transformation is therefore from a common operational picture to a confidence-aware operational and decision environment. Trust must be computed, validated, displayed, and operationalized. Missing data must be visible. Civilian data must be translated into operational confidence. Degraded modes must be designed in advance. Decision-making must become trust-weighted and risk-aware.

The resulting architecture does not eliminate uncertainty. It makes uncertainty governable. It enables military leaders to act coherently when the federation is incomplete, when civilian dependencies are fragile, when adversaries contest the information environment, and when the data picture is less reliable than the operational tempo requires. In that sense, the decisive value of MDO C2 is not that it provides perfect information. Its decisive value is that it preserves superiority when perfect information is impossible with sustained decision advantage in complex and contested operational environments.

About the Author:

Dominique Luzeaux entered the Ministry of Defense in 1984, as a cadet within the Military Academy of Saint-Cyr from Sep. 84 to Jan. 85, and platoon leader, 43rd Infantry Regiment, from Feb. 85 to Aug. 85. He graduated from École Polytechnique (1987) and École Nationale Supérieure des Techniques Avancées (1989) as an armament engineer.

His first position was a research engineer in artificial intelligence and robotics. He defended his PhD thesis at the University of Paris XI (1991), and was a visiting research scientist at the University of California at Berkeley (1991-1992). Within the DGA (French Armament Procurement Agency), he occupied various positions successively as expert, project manager and director. As Director of the Complex System Engineering Department (2002-2004), he was in charge of the R&T programs in system engineering methods and tools, as well as in modeling and simulation. He was the French representative within NATO/RTO and WEAG technical panels. As Director of the Technical Center for Information Systems (2004-2007) he was in charge of the reorganization of the technical and human resources dedicated to the information system infrastructure of the DGA. 2008-2009, he was appointed Deputy Director for C4ISR systems.

As Director for Land Systems acquisition, he was responsible for the technical and financial execution (yearly payment over 1 billion euros) of the military programs for land systems, and was the French representative for several bilateral and multilateral agreements. He was named Honorary Private First Class of the Army for his personal implication in various armament programs, among them the Unitary Rocket Launcher.

End of 2013 he joined the Joint Staff as Deputy Director within the Directorate for Infrastructure Networks and Information Systems at the Ministry of Defense level, where he acted as the Chief Purchasing Officer (yearly budgetary envelope of almost 1 billion euros) and head of the Acquisition and Supply-Chain Division.

From 2021 to September 2023, he was Director of the newly created Digital Defense Agency within the French Ministry of Defense, in charge of all defense complex digital projects.

Besides, he defended in 2001 his Professor thesis, has directed a dozen of PhD students, has published around hundred articles in conferences and international journals, and has written 10 books in French and in English on nanotechnology, on simulation, on complex systems engineering, and on the formalization of digital AI-assisted debates. He received the “Ingénieur Général Chanson” Award in 2006 for his work on military autonomous unmanned ground vehicles.

Luzeaux is married to Ghislaine and is father of one son, Yvain.


COMMAND AND CONTROL
CENTRE OF EXCELLENCE