CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Institutional Command and Control (iC2)

By VAdm (Ret'd) Ron Lloyd

June 2026

POLICY PERSPECTIVE

Institutional Command and Control (iC2)

by

VAdm (Ret'd) Ron Lloyd

June 2026

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute

Suite 2720, 700– 9th Avenue SW., Calgary, AB T9P 3V4

www.cgai.ca

Executing at the Speed of Operations in Modern Defence

Modern defence institutions face a growing structural paradox. Operational decision cycles increasingly operate at machine speed, enabled by advanced sensing, analytics, and decision systems. Yet the institutions responsible for resourcing, sustaining, and governing those operations continue to function at a bureaucratic speed. Defence organizations can generate operational insight in seconds, but may require weeks or months to mobilize the institutional action required to act on that insight.

Institutional Command and Control (iC2) is the enterprise command function through which defence institutions align and direct authorities, resources, and industrial capacity in response to operational demand. It enables the translation of operational intent into synchronized enterprise action across current operations, force regeneration, and future capability development. Concretely, this includes the institutional capacity to convert operational demand into authorized, funded, tested, and fielded capability at operational tempo; to regenerate and sustain forces in contact; and to synchronize the functional offices through which governance is enacted across the enterprise.

The importance of this function is not theoretical. During combat operations in Afghanistan, Canadian defence institutions were able to operate at operational tempo through sustained senior leader engagement across the enterprise. Authorities, resources, and decisions were aligned through direct intervention rather than system design. While effective, this approach depended on leadership engagement alone and is not reproducible at scale in today's more complex, digitally and industrially interconnected defence environment.

Modern defence institutions must operate across multiple time horizons simultaneously. While operational commanders focus on current missions, institutional leaders, military and civilian, must ensure the readiness of the next rotation while stewarding the development of the future force. Institutional Command and Control enables these competing demands to be synchronized without diminishing governance, risk management, or institutional stewardship.

This paper argues that the modern defence enterprise faces a growing execution gap between the speed of operational decision-making and its ability to translate those decisions into coordinated institutional action. It further argues that Institutional Command and Control is the command function required to close that gap, synchronizing authorities, enterprise systems, and industrial capacity at the tempo modern operations increasingly demand.

The Changing Context of Defence Execution

Over the past several decades, structural shifts have altered how defence institutions sustain and adapt military capability. Modern military systems increasingly depend on software, digital architectures, and tightly integrated systems that require continuous modification throughout their operational life.

Historically, integration was addressed within individual platforms. Today, integration occurs across operational architectures that combine sensors, decision systems, communications, and weapons to deliver effects under conditions of extreme time pressure. These architectures are organized around operational problems rather than institutional structures. This integration increasingly extends beyond national institutions to include allied

and partner systems, where interoperability requirements, classification constraints, and data-sharing limitations further complicate execution.

This new model of institutional integration is also now extending across the defence enterprise. Logistics, maintenance, supply chains, personnel, finance, and governance processes are increasingly connected through enterprise digital architectures that link institutional systems to the operational edge. Execution is no longer confined to platforms, but draws upon and is distributed across a wider enterprise of systems, authorities, and even industrial partners.

Defence supply chains have shifted from stockpiles to distributed industrial ecosystems. Capability sustainment increasingly depends on continuous collaboration with industry, including software integration, system updates, and technical support delivered through both domestic and international partners. In some cases, advanced manufacturing capabilities are enabling production at the edge, reducing dependency on traditional supply chains.

For major platforms, the structured, multi-year capability investment framework remains appropriate and necessary. The dollars, the operational consequences, and the level of justification required demand that rigour. But for a growing class of capability, including combat system software, electronic warfare libraries, sensor and decision algorithms, and networked applications, the relevant cadence is iterative, with meaningful updates expected in weeks or months rather than budget years.

Industry partners have traditionally been the ones who do this type of iterative development work on systems. What has changed is the tempo expected of those partners and the extent to which front-line operational feedback now drives their cycles. Institutions whose planning, contracting, and accreditation rhythms are calibrated for infrequent, high-certainty platform decisions will be unable to absorb capability that industry can already deliver, not because institutional processes are lacking, but because they are calibrated for a different cadence.

The operational front line is no longer solely a source of demand; for a growing set of capabilities, including autonomous systems, drones, robotics, sensor and decision algorithms, and networked applications, it is a persistent feedback engine, and industry is an active participant in the execution cycle through which operational demand is translated into continuously evolving capability. Institutional Command and Control (iC2) is the function that synchronizes decisions across this continuum so that capabilities requiring rapid adaptation can be developed, tested, and fielded at operational tempo without being constrained by institutional structures and timelines designed for major capability investment.

As complexity has increased, defence institutions have strengthened functional offices responsible for areas such as cyber security, accreditation, procurement, infrastructure, and personnel management. These offices are essential for managing risk and maintaining standards, but they operate horizontally across the enterprise rather than within operational commands. As a result, the institutional levers required to implement operational decisions are now distributed across multiple functional offices whose processes must be synchronized to deliver timely outcomes. Further exacerbating the challenge is that, in many cases, their requirements are asynchronous or directly contradictory, creating a reconciliation challenge that complicates and further delays effective coordination.

These shifts have not simply increased complexity. They have fundamentally altered the relationship between operational command and the institutional systems required to support it.

Operational Command in the Institutional Enterprise

Operational command carries with it a clear and enduring responsibility: commanders are accountable for the readiness, employment, and performance of the forces they lead. Historically, many of the functional authorities required to generate and sustain military capability were held within the commander's span of control, enabling closer alignment between operational requirements and institutional action.

Over time, however, these authorities have migrated into specialized functional structures across the defence enterprise. The result is a structural divergence: commanders remain responsible for operational outcomes, but many of the institutional levers required to deliver those outcomes are distributed across the enterprise. Operational direction may be clear, yet implementation depends on processes, approvals, and systems operating outside the operational chain of command.

The diffusion of functional authority across the enterprise reflects deliberate institutional design. Functional authorities exist precisely because cyber, safety, financial, and personnel risks require independent and expert judgement, exercised at arm's length from operational pressure. Institutional Command and Control does not seek to consolidate those authorities or override them. Rather, it seeks to ensure that they operate in synchronization rather than in isolation. This creates a fundamental challenge for command that existing institutional structures were not designed to resolve. Commanders must now understand and influence an institutional architecture that lies beyond the operational chain of command, but directly determines operational readiness and adaptability. For joint forces operating within integrated digital and industrial ecosystems, the ability to influence and synchronize the enterprise systems that sustain operational forces is no longer ancillary to command; it is integral to it.

The Institutional Execution Gap

The institutional execution gap is the structured consequence of two command cycles, operational and institutional, operating at fundamentally different speeds and serving distinct but interdependent purposes. Operational command cycles generate mission demand, while institutional processes translate that demand into enterprise action. The challenge is not that these cycles exist separately; they must. It is that they are not synchronized.

Institutional processes exist not only to support current operations, but to manage risk, allocate resources, and steward long-term capability development. These functions are essential to managing risk and maintaining standards across the enterprise. The challenge is not their presence, but their ability to operate with sufficient coherence and speed when operational demand requires rapid action.

Modern defence enterprises are supported by four interconnected domains: operational command and control systems, data and analytic environments, institutional systems of record, and a fourth domain becoming increasingly visible within modern defence enterprises: institutional execution mechanisms. Each performs a distinct function in generating military capability. Operational command and control systems fight the

force. Data and analytic environments generate insight into the operational environment and the state of the force. Institutional systems of record sustain the force by managing the institutional resources upon which military capability depends. Institutional execution mechanisms coordinate enterprise activity by orchestrating workflows across functional offices, authorities, and enterprise systems responsible for implementing institutional decisions. However, their coexistence does not ensure alignment.

The execution gap emerges when these domains operate out of synchronization. Operational decision cycles generate demand at increasing speed, while the institutional offices responsible for execution operate through distributed processes optimized for governance rather than tempo. Where institutions apply a uniform standard across these distributed processes, the effective tempo of the enterprise collapses to the slowest process in the chain.

This gap is not transient, nor is it the result of inefficient processes. It is the predictable consequence of an enterprise in which authority, resources, and accountability are distributed across structures not organized to function as a coherent command system.

Figure 1. Defence Enterprise Command Architecture

Between operational decision and enterprise implementation lies a dense network of institutional workflows spanning multiple functional offices, systems, and governance structures. These offices control the resources required for execution, but operate through distinct processes and timelines. The result is fragmentation not of information, although this too often occurs, but principally of execution.

For operational commanders, this fragmentation obscures how the institutional systems that sustain their forces interact across the enterprise. As operational decision cycles accelerate, the speed of institutional execution becomes a determinant of operational advantage. Operational Command and Control enables commanders to manoeuvre forces. Institutional Command and Control enables defence institutions to manoeuvre the enterprise required to sustain those forces.

Figure 2. Institutional Execution Gap

Institutional Execution as a Strategic Capability

Execution is often reduced to questions of administrative efficiency or process automation. At enterprise scale, execution is fundamentally about synchronizing functional authorities, resources, and industrial capacity to deliver sustained military effects across current operations and the future force.

Defence institutions frequently distinguish between operational and administrative data, implicitly prioritizing systems associated with combat operations while treating enterprise systems as back-office infrastructure. This distinction, while administratively convenient, obscures the strategic reality. In an interconnected defence enterprise, every system that enables a commander to resource, sustain, adapt or regenerate forces is an operational system. The label applied to a system does not determine the operational consequences of its failure. Nor does the institutional arrangement through which it is delivered determine whether its performance is operationally consequential.

When a commander directs a change to force posture, software configuration, or operational employment, execution depends on institutional systems capable of mobilizing resources, authorizing actions, and coordinating industrial support. Absent alignment across these systems, operational risk accumulates beyond the battlespace.

Institutional execution must be exercised before it is required. Commanders routinely wargame operational plans, yet the institutional systems required to sustain those plans are rarely exercised with the same rigour. In conflict, the consequences of misalignment across sustainment, personnel, industrial support, and governance mechanisms may only become visible once operational decisions must be executed at pace and scale, where distance, industrial depth, and distributed operations place exceptional demands on institutional execution. If institutional execution is to operate at operational tempo, these systems must be exercised and measured with the same discipline applied to operational planning. The institution that has not exercised its execution architecture in peacetime will discover its limits in conflict, when the cost of doing so is highest.

Illustrative Operational Scenario

Consider a Royal Canadian Navy task group deployed as part of a multinational maritime operation, a scenario broadly representative of modern allied naval operations. During routine patrol operations, electronic warfare sensors aboard multiple Halifax-class frigates detect previously unobserved adversary emissions capable of degrading the ship's combat system performance.

Operational analysis conducted within the task group quickly confirms the potential vulnerability. The Fleet Commander determines that a modification to the combat system software and associated electronic warfare procedures could mitigate the threat and restore operational effectiveness.

From an operational command perspective, the decision cycle occurs rapidly. Intelligence assessments are updated, operational commanders determine the required change, and direction is issued across the deployed force.

Executing that decision across the defence enterprise, however, requires coordination across numerous institutional authorities. Combat system configuration offices must approve the modification. Cyber and safety accreditation bodies must validate the software update. Program offices responsible for the Halifax-class combat system must authorize the revised configuration baseline. Industrial partners responsible for software integration must prepare the update, while fleet sustainment organizations coordinate its distribution to ships operating at sea. Personnel staffs must also ensure that operators and technicians across the fleet are trained to employ the updated configuration and associated procedures.

The operational decision cycle may occur in hours. The institutional execution cycle, however, is measured in distinct and often uncoordinated intervals: time from threat detection to authorized software modification; time from approval to industrial integration; time from integration to fleet-wide deployment; and time from operational use to validated feedback and subsequent iteration. In current structures, these intervals routinely extend from days to weeks, each governed by separate offices and processes. During this period, the vulnerability remains unmitigated, adversary systems continue to adapt, and operational risk accumulates across the force. The execution gap is not a single delay, but the cumulative effect of these unsynchronized cycles.

Institutional Command and Control is the function that answers this. It operates as a continuously active synchronizing function across the enterprise command cycle, not as an additional governance layer, but as the enterprise mechanism through which operational demand is translated into coordinated institutional action across distributed authorities. Where operational commanders issue direction, Institutional Command and Control provides the visibility and coordination required to ensure that the offices responsible for cyber accreditation, configuration management, sustainment, and industrial coordination are working in concert rather than in isolation. Its effectiveness determines whether operational decisions are translated into coordinated enterprise action or dissipate across the enterprise. Unlike standing committees or project governance structures, Institutional Command and Control is not convened in response to a decision; it is continuously active, translating the ongoing demand signals of the operational command cycle into coordinated enterprise execution.

Architectural Implications

Modern defence architectures have successfully integrated operational data environments and decision systems. The constraint is no longer digital capability, but the ability to synchronize institutional authorities and enterprise systems to execute decisions at operational tempo. Far less attention has been given to the mechanisms required to align governance, resources, and industrial collaboration across the enterprise at operational speed.

Taken together, Figures 1 through 3 describe not just a structural problem, but a structural opportunity. Figure 1 defines the core domains. Figure 2 exposes where the coherence breaks down. Figure 3 shows what restored coherence looks like.

Figure 3 - Synchronized Operational and Institutional Command and Control

The implication is direct. Operational advantage no longer depends solely on the speed of decision, but on the ability of the institution to execute those decisions coherently across the enterprise. Where operational and institutional command cycles are misaligned, adaptation slows, risk accumulates, and advantage erodes.

Institutional Command and Control therefore represents not an additional layer within the architecture, but the function that determines whether the architecture operates as a system. The speed and coherence with which this function translates intent into execution increasingly determine whether forces can adapt faster than their adversaries and sustain advantage over time.

Measuring Institutional Execution

If institutional execution represents a strategic capability, it must be measurable. Defence institutions traditionally track operational readiness through indicators such as force availability, equipment readiness, and training status. Comparable measures rarely exist for the institutional processes that enable those forces to adapt and sustain operations.

Institutional execution can therefore be understood as institutional readiness: the ability of defence organizations to mobilize and execute enterprise action in response to operational demand. Institutional performance depends overwhelmingly on two factors: execution velocity and execution coherence. Velocity reflects the speed at which institutional action occurs. Coherence reflects the degree to which that action is synchronized across authorities, systems, and organizations. Equally important is how decision authority is exercised in practice,

including the extent to which it is delegated forward and the speed with which operational feedback is acted upon across the enterprise.

In practice, this requires concrete, assigned indicators. The most important include the time required to authorize mission-critical changes; the time from identified operational need to funded experiment; the cycle time from industry proposal to live operational trial; the time from operational feedback to fielded software modification; and the time to accredit new capabilities and onboard industrial partners into secure production environments. Together, these measures define execution velocity in operational terms.

However, these measures do not simply provide insight. They determine whether institutional processes enable or constrain operational adaptation. Where execution cannot be measured, it cannot be controlled; where it cannot be controlled, it cannot be aligned to operational tempo.

Institutional readiness metrics of this kind should be integrated into existing defence reporting mechanisms, and, where appropriate, aligned across allied frameworks, rather than treated as a separate analytical exercise. Responsibility for tracking and reporting execution velocity and coherence should be assigned explicitly. Without assigned ownership, these measures remain advisory. With it, they provide commanders and institutional leaders with a direct view of whether the enterprise can adapt at operational tempo and become a command instrument rather than an administrative one.

Strategic Implications

Governance and risk management are not the constraint. The constraint lies in how they are applied. Many of the mechanisms that determine execution speed, including cyber accreditation, supplier onboarding, export controls, and security vetting, are governed by policy frameworks designed for a different operational tempo. These mechanisms are expressed through small-p policy: the procedural rules, approval authorities, and institutional practices through which governance is enacted in practice.

When these mechanisms operate across fragmented processes and distributed offices, delays accumulate across the enterprise. The result is not isolated inefficiency, but a systemic inability to translate operational intent into coordinated action at speed. Defence digital strategies that address data integration while leaving these policy mechanisms unchanged will accelerate the visibility of institutional failure without improving the capacity to resolve it.

The strategic implication is enduring, but its urgency has fundamentally increased. Wars are not decided by battlefield success alone, but by the ability to regenerate capability, mobilize industry, and sustain adaptation over time. The Allied advantage in the Second World War illustrates the principle. German forces demonstrated superior operational command and control in the early years of the conflict, achieving battlefield success that consistently outpaced Allied manoeuvre. Yet the Allies ultimately prevailed because their institutional systems proved more capable of mobilizing industrial capacity, integrating scientific innovation, and sustaining adaptation at scale, advantages that compounded over time and proved decisive.

The critical difference today is time. In the Second World War, institutional advantage accumulated over years of sustained mobilization. Modern adversaries can now contest industrial capacity, digital infrastructure, and institutional systems directly and at speed, as

recent conflicts have demonstrated. If institutional execution cannot activate and synchronize capability at or near operational tempo, industrial and technological depth loses much of its strategic value before it can be brought to bear. The compounding effect of institutional execution remains decisive, but it must now begin immediately and operate continuously alongside operational decision-making.

Conclusion

The conditions under which defence institutions must succeed have fundamentally changed. The distribution of authority, the acceleration of decision cycles, the digitalization of the enterprise, and the deepening integration of industrial partners have collectively outpaced the institutional mechanisms designed to coordinate them. This is not a failure of leadership or governance. It is a structural gap that must to be recognized and addressed.

Institutions that cannot do so do not fail abruptly. They fail gradually, through delayed adaptation, fragmented acceleration, and the steady accumulation of operational risk outside the battlespace. In modern conflict, where advantage depends on the interaction of decision speed and execution coherence, these failures are decisive.

Over time, it is this capacity, not decision alone, that determines whether advantage can be generated, maintained, and exploited. Operational Command and Control wins battles. Institutional Command and Control determines whether those gains can be sustained.

In modern conflict, the defence enterprise that cannot execute at the speed of its own decisions cedes advantage by design.

About the Author

***VAdm (Ret'd) Ron Lloyd**, a native of Taber, Alberta, Vice-Admiral (Ret'd) Ron Lloyd was the 35th Commander of the Royal Canadian Navy from 2016-2019. During that time he was also "double hatted" as the acting Vice Chief of the Defence Staff for almost half a year and as the first Chief Data Officer for the Department of National Defence and Canadian Armed Forces for a full year.*

During his 38 year career in the RCN, he was privileged to have commanded HMCS CHARLOTTETOWN, HMCS ALGONQUIN, the PACIFIC Fleet and the ATLANTIC fleet. He has extensive operational experience having deployed on numerous occasions globally.

Lloyd has over a decade of experience at National Defence Headquarters having also served as the Deputy Commander of the RCN, the Chief of Force Development for the Canadian Armed Forces, the Director General of Force Development for the RCN and Executive Assistant to the Commander of the RCN.

Lloyd holds a Bachelor of Arts in Military and Strategic Studies from Royal Roads Military College (1985) and a Master of Arts in War Studies from the Royal Military College (2004). He is a graduate of both the Command and Staff Course and the National Security Studies Course at the Canadian Forces College in Toronto. He has also attended the HARVARD Kennedy School, Executive Education, Senior Executives in National and International Security.

Today, as Principal of Leadmark Ventures, he shares his experience in leadership, strategic planning and digital transformation with organizations committed to providing innovative solutions that enhance public sector performance in defence and non- defence related activities.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.