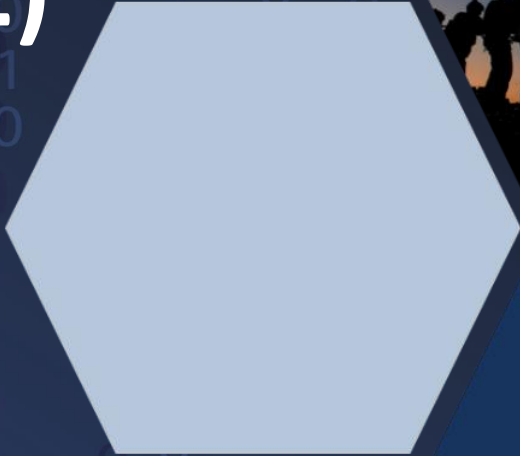# PAN-DOMAIN COMMAND & CONTROL (PDC2)

Concept Paper

DECISION ADVANTAGE IN A DANGEROUS WORLD

Canada

Pan-Domain Command and Control (PDC2)
Concept Paper

FOREWORD

The world is witnessing a resurgence of strategic competition, and Canada's adversaries present a concerted, sustained, and harmful challenge to the rules-based international order upon which the nation's security and prosperity depends. Canada can no longer rely on geography for its security. Furthermore, the global security environment is changing because of a multitude of disruptors such as climate change, demographic and disruptive technologies. Those threats are unprecedented and present one-in-a-generation challenges to our way of life. The time for reflection is over, we must now act.

The Pan-Domain Force Employment Concept (PFEC) recognized imperatives to change and described the broad ways that the CAF must adapt and transform in the face of the evolving global security environment. Our closest Allies have also understood the changing threat landscape requires a new approach to compete, contest and defeat adversaries. The entire Defence Team must transform its approach to be completely interoperable, across all domains of military operations, with our closest allies. 'Day Zero' interoperability at the service level is no longer sufficient to effectively defend Canada's national interest. The complexity and integrated nature of synchronizing effects across all domains will require a new mindset. Pan Domain Operations will not achieve the objectives if the CAF conducts C2 in the same manner it has for the past decades.

This Pan-Domain Command and Control (PDC2) Concept Paper establishes a transformative framework for how the CAF conducts C2 across all the domain of military operations to deliver coherent and synchronized effects. Key aspects developed in this Concept Paper include: Establishing Pan-Domain Situational Awareness (PDSA), Linking Sensors and Sources to Effects through a Decider, Enabling Pan-Domain Operations with National Security Partners, and Enabling a National Campaigning Approach to the Defence of Canada. The transformative aspect of Pan-Domain C2 must be comprehensive and focused on providing decision advantage to CAF leaders. To achieve those goals, PDC2 must be seen as a capability that is made up of five components: People, Process, Structures, Data, and Technology. The CAF must be able to develop an effective PDC2 capability to be able to compete, contest, confront, and if necessary, defeat adversaries, or it risks becoming irrelevant to Allies. In the near term, the priority will be to participate in allied experimentation for CJADC2, such as the US-led Project Olympus, to align the development of the PDC2 capability and improve interoperability with the US and other Allies.

Thus, the CAF, together with its Allies, must face the increasingly complex challenge of strengthening deterrence and posturing for competition by demonstrable and credible offensive capabilities. The CAF must adopt a more proactive and deliberate mindset to prevent high-intensity conventional armed conflict while preparing to win such a conflict should it occur. As the CAF adapts to the future operating environment, the PDC2 Concept provides a comprehensive framework for transforming our approach to C2. It emphasizes leadership, adaptability, critical thinking, and calculated risk-taking, while embracing technological advancements and process evolution. Realizing this vision requires profound institutional changes across the entire Defence Team, and it is essential to prevail in a complex and dangerous world.

M.A.J. Carignan, CMM, MSC, MSM, CD
General
Chief of the Defence Staff

Pan-Domain Command and Control (PDC2)
Concept Paper

Contents

1. Executive Summary

The global security environment is complex and dangerous, characterized by the re-emergence of strategic competition, proliferation of advanced technologies, and evolving multi-domain threats. Traditional domain-centric approaches to command and control (C2) are inadequate to address these evolving challenges. The Pan-Domain Command and Control (PDC2) concept establishes a transformative framework for how the Canadian Armed Forces (CAF) conducts C2 across complex operating environments.

Aim and Drivers

The aim of PDC2 is to deliver holistic, agile, data-driven decision and operational advantage. PDC2 needs to be interoperable with allies from Day Zero of an operation, enabling the CAF to prevail in an era of perpetual competition and conflict. Key drivers impacting this change include:

Evolving Threats: Resurgence of great power rivalry, potential use of nuclear weapons, regional instability, and state/non-state actor disruptions challenging the rules-based international order.

Multi-Domain Battlespace: Adversaries contesting all domains (maritime, land, air, space, cyber and the information environment) with advanced capabilities, demanding integrated pan-domain effects.

Emerging Technologies: Rapid diffusion of emerging technologies like AI, autonomous systems, hypersonic weapons, quantum computing, and counter-space capabilities across state and non-state actors.

Allied Interoperability: Maintaining relevance and seamless integration with allies developing similar C2 concepts.

Conceptual Approach

PDC2 is about transcending historical stove-piped domain-centric approach to operations and seeks a more holistic, synchronized approach to delivering military effects in support of the Government of Canada (GoC). Key tenets include:

Decision Cycle: The Pan-Domain Decision-Action cycle will enable the CAF to sense, make sense, decide and take conscious action on a continual basis. This involves leveraging data, technology, and decision makers to deliver decision advantage and operational initiative to the CAF.

Information Environment: Leveraging a foundational information environment drives efficiency and scalability. By ensuring comprehensive data access, it supports informed decision making and strategic planning, vital for maintaining operational advantage in a complex multi-domain landscape.

Components: PDC2 comprises five interdependent components: People, Processes, Structures, Data, and Technology, which must collectively be advanced in support of C2 Interoperability and C2 Agility with a mindset that embraces calculated risk-taking.

Human-Machine Teaming: Processes and structures need to evolve to enable greater automation leveraging Artificial Intelligence (AI)/Machine Learning (ML) methods to augment human cognition, make sense of vast data and support decision making.

Implications

Realizing the PDC2 vision requires profound institutional change across the entire Defence Team:

Mindset Shift: Implementing PDC2 requires a profound cultural change to how we see an integrated C2 capability unbounded by domain constraints, emphasizing leadership, adaptability, critical thinking, willingness to take calculated risk, and empowerment at all levels.

Process Evolution: Existing processes must be updated or replaced and new ones created to support pan-domain operations and leverage automation (including AI, ML and advanced analytics).

Capability Development: PDC2 will be a pillar of the Force Command concept, a foundational structure of the National Defence Operations and Intelligence Centre (NDOIC) and will guide related capability programs and initiatives.

Partnerships: Achieving C2 interoperability with allies and National Security Partners is crucial, therefore, aligning with concepts like US Combined Joint All Domain Command and Control (CJADC2), UK Multi Domain Integration (MDI), and NATO Multi Domain Operations (MDO) concept.

The PDC2 concept provides a framework for transforming the CAF's C2 to meet the challenges of the future operating environment. It fosters agility, integration, resiliency, and decision advantage through data- and technology-enabled decision making and operational advantage through integrated effects.

2. Aim

The aim of this paper is to establish a conceptual framework that redesigns the way the CAF executes C2 across the pan-domain operating environment. This framework will be used to deliver an agile, data-informed decision advantage over our adversaries and credible Day Zero interoperability that maintains relevance with our allies and National Security Partners.

This PDC2 concept will shape the development of the Force Command concept, enable aspects of the CAF's *Concept for the Future Force*, and inform the development of the Concept of Operations for the National Defence Operations and Intelligence Centre (NDOIC). It will also guide the way we revisit doctrine and the development of new concepts, programs, projects and initiatives related to PDC2 across the Force.

The PDC2 concept supports the *Pan-Domain Force Employment Concept* (PFEC) and aligns with the *CAF Digital Campaign Plan* to ensure it leverages current and emerging technology and the institutional changes that accompany them. This concept is also aligned with other key CAF strategic guidance documents, including the *VCDS C2 Operating Concept*, *Joint Intelligence Surveillance and Reconnaissance (ISR) Future Operating Concept*, and the *DND/CAF AI Strategy.* It is intended to be aligned with the upcoming *DND/CAF Digital Transformation Strategy* and renewal of the *DND/CAF Data Strategy*.

Finally, this concept is informed by our allies and partners who are rapidly developing their C2 concepts, such as the US (CJADC2), the UK MDI program, and the NATO MDO concept.

Figure 1 - PDC2 is shaped by Threats; aligned with Defence Strategies; and informed by Allies and Partners

CAF must be: "**Ready**, with sufficient numbers of well-trained, motivated and supported people, enabled by the right equipment in the right timeframes, and working with safe and effective infrastructure; **Resilient**, with forces that are sustained on operations for as long as necessary, can operate across the land, sea, air, cyber and space domains, and are digitalized and networked for the information age; and **Relevant**, with forces making robust contributions where it matters most to Canada, with capabilities that are suited to the type of contributions we need to make."

Our North, Strong and Free

3. Imperative for Change & Problem

Imperative for Change

The global security situation is complex and dangerous with the re-emergence of strategic competition and the growing multipolarity in the international system, where revisionist states are becoming more assertive and increasingly willing to act aggressively, and even non-state groups can disrupt the rules-based international order (RBIO). Ongoing conflicts, along with the rising proliferation and increased potential use of both conventional and nuclear weapons, have created an environment of persistent global competition that Canada must contend with.

The Russia-Ukraine war continues to pose a significant geopolitical risk with impacts on NATO cohesion, the Alliance's posture, and long-term consequences for global defence supply chains. China's military buildup, technological advancements, and ongoing trade disputes and friction points have given rise to geopolitical tensions. Taiwan remains a significant flashpoint, as recent Taiwanese presidential elections and Beijing's ongoing reunification ambitions demonstrate. The Israel-Hamas War has exacerbated regional tensions in the Middle East with the potential for greater escalation and an expansion of the conflict to the Red Sea, Iraq, Iran, Syria, and Lebanon. North Korea has increased provocations, recently renouncing peaceful reunification with South Korea as a key policy goal, while its nuclear and ballistic missile programs continue unabated.

Domestically, the CAF needs to be able to assert and defend Canada's sovereignty, with emphasis on the Arctic which is becoming increasingly accessible and contested due to climate change, as recently highlighted in 2024 Defence Policy: *Our North, Strong and Free*. The CAF currently lacks the military presence and capabilities required to effectively respond to threats and challenges in the North. Increased military activity in the region, including adversaries' capability to project air, naval surface and sub-surface, and missile forces, poses a challenge to keep the Arctic as a cooperative, non-militarized zone.

Threats against RBIO traditionally were linked to land, air, and maritime domains. In the new battlefield these threats have engulfed cyber and space domains. Aggressive infringement in these domains has led to assaults on Canada and its Allies. Our adversaries are harnessing all instruments of national power to mount a concerted and sustained challenge to Canada's security and prosperity. Unfortunately, the CAF's current C2 capabilities are not able to address these challenges.

The evolving operating environment is dynamic and requires diverse combinations of capabilities from across industry and Whole of Government (Diplomacy, Information, Military, Economic). The CAF cannot deter and defeat the aggression of our adversaries without working closely with our allies, National Security Partners, and broader Canadian society. This requires frequent collaboration with close Allies and partners as their concepts evolve.

Emerging digital technologies are pervasive and accessible, with a lower cost and complexity threshold. Their rapid adoption by our rivals has reduced the advantages we used to have in terms of capabilities and methods. This, along with an exponential growth in data and increasingly complicated and variable geopolitical tensions, has helped create an operating environment that is uncertain and subject to rapid change. In response, allies are adopting agile delivery policies and processes to commission new technology-enabled capabilities. They are focused on ensuring the proper doctrinal changes are in place to execute C2 in a pan-domain operating environment. Unfortunately, long lead times for the CAF to acquire new capabilities impacts both our ability to train and deploy forces capable of operating in a pan-domain environment, and the capacity of those forces to integrate and be interoperable with our Allies and partners.

Problem

The CAF faces a critical challenge in adapting to the rapidly evolving landscape of modern warfare and strategic competition, particularly in the realm of pan-domain C2. Allies and adversaries are adapting and developing capabilities to execute C2 in the pan-domain operating environment. The CAF's current C2 capability gaps, paired with an inability to field new capabilities in a timely manner, puts at risk its ability to respond to threats and conduct core missions with integrated effect. This, in turn, jeopardizes the CAF's ability to maintain interoperability with National Security Partners and Allies.

Without sufficient C2 capabilities we are unable to pose a credible threat which undermines our ability to deter potential adversaries. If we don't have the capabilities and operational concepts to oppose adversaries, we are not a threat, and are therefore incapable of deterrence.

This complex challenge requires modernizing and augmenting existing C2 capabilities, making use of emerging technologies, and redesigning processes and structures to empower our personnel in the pan-domain operating environment.

The CAF is at an inflection point. Either the CAF modernizes its ability to command and control to be able to compete, contest, confront, and if necessary, combat adversaries in a pan-domain operating environment, or it risks becoming irrelevant to Allies.

Vision

A CAF that is relevant to our National Security Partners, with Day Zero interoperability with our Allies, and decision and operational advantage over our adversaries.
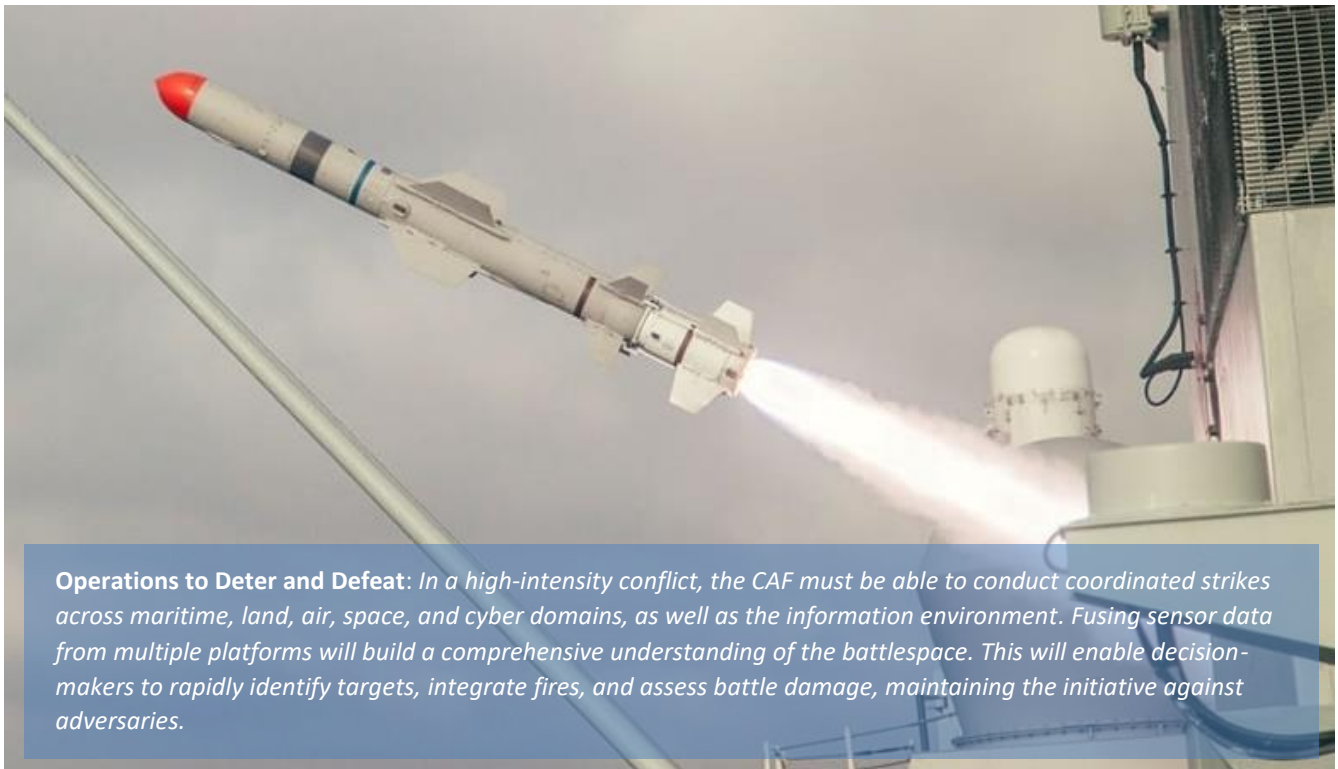
Operations to Deter and Defeat: *In a high-intensity conflict, the CAF must be able to conduct coordinated strikes across maritime, land, air, space, and cyber domains, as well as the information environment. Fusing sensor data from multiple platforms will build a comprehensive understanding of the battlespace. This will enable decision-makers to rapidly identify targets, integrate fires, and assess battle damage, maintaining the initiative against adversaries.*

4. Conceptual Framework

Approach to PDC2

The PDC2 concept provides the intellectual foundation for the C2 of operations in a pan-domain environment as described within the PFEC. The PFEC outlines how the CAF must adapt to deter and counter the aggressive actions of adversaries across all domains through an integrated, whole-of-government approach collaborating with allies and partners. It seeks to prioritize investment in advanced technologies, evolve planning and C2 processes, and takes a campaigning mindset focused on long-term competition.

PDC2 is mission-driven and threat-informed to ensure the CAF remains relevant to our Allies and capable of protecting Canadian national security and interests. PDC2 applies to all eight (8) core CAF missions, across continental, expeditionary, and cyber defence contingencies, in all domains, as well as the information environment, and throughout the full spectrum of conflict (including sub-threshold warfare).

Realizing the vision will require a change in how C2 is conducted for operations. This involves innovations in C2 related technologies, modification and adaptation of our processes, and structural renewal. Broad aspects to consider in the approach to pan-domain C2 include:

Establishing Pan-Domain Situational Awareness (PDSA). PDSA will be enabled by myriad sensors and systems to make sense of the overall situation and operating picture. PDSA is established by ingesting data from sensors and sources, and persistent monitoring them in real time. The value of data is extracted through curation, analysis, and synthesis with the aid of AI/ML, cued to critical information requirements, and directed to better inform decisions. PDSA also includes understanding ourselves and our evolving situation. CAF platforms, infrastructure, sustainment systems, and potentially people will need to automatically report their status, such as ammunition, fuel, personnel health etc., to create an understanding of what the force is capable of, at any moment, in contested environments.

Operational Support: *The CAF must be able to deploy personnel, equipment, and supplies to forward operating locations. Beyond strategic transport capabilities, this requires a modernized Defence Supply Chain (DSC) and resilient Strategic Lines of Communications (SLOC) to ensure sustained operations. Future sustainment information systems that support the DSC and SLOC need to be interoperable with our allies, enable visibility and real-time status, provide trusted data insights, and digitally empower sustainment practitioners, so that PDSA can be provided to CAF leadership at all levels.*

Linking Sensors and Sources to Integrated Effects. C2 applications must link myriad institutional and operational datasets from sensors and sources to decision makers to enable the execution of Command decisions. This includes functions to transmit orders, process data, and share and publish information. This will support the generation of insight from data to inform decision makers and thereby provide direction to achieve integrated effects. Based on holistic understanding of the operating environment, decision-makers will be enabled to make evidence-based decisions at the speed of relevance that dictate the tempo to adversaries and maintain the initiative.

Driving Integration and Partnerships. The ever-changing operating environment is challenging traditional notions of supported/supporting relationships and demand that PDC2 seek to achieve effects in Environment-- and platform-agnostic manner. National Security Partners are important as adversaries challenge the traditional barriers between national defence, national security, and national prosperity. Within the Defence Team, the linkages between the CAF and DND will also need to become even stronger. These trends will drive greater integration across Defence and Whole of Government.

Enabling a Campaigning Approach. Pervasive competition, along with the requirement to posture the force and shape the environment prior to conflict, challenges our traditional approach to operations. While traditional approaches of single-service contributions commanded by other nations remain valid, national campaigns will be required to assure that Canadian strategic objectives are achieved. Such campaigns will need to align with key allies' extant regional and global campaigns as well as the Government of Canada (GoC) objectives. This approach will require a robust assessment mechanism, leveraging the vast datasets operations will leverage to ensure operations remain aligned with objectives.

Development of these aspects will have direct results in achieving the Vision for the PDC2 concept. The CAF will become increasingly able to achieve decision advantage over its adversaries, enhance its value to Allies, and improve its ability to achieve national objectives.

> *"Our growing reliance on cyberspace, cloud computing, and interconnected technologies for daily life and economic growth greatly complicates the defence of Canada and Canadian interests."*
>
> **Our North, Strong and Free**

Principles of PDC2

Realization of the PDC2 concept will be a substantial undertaking for DND/CAF. The following principles will be useful in building a common operational mindset and unity of effort in pursuit of this capability:

C2 Interoperability. The CAF does not fight alone and is a member of alliances and partnerships that are critical to Canada's national security and interests. Enabling the CAF to act coherently, effectively, and efficiently toward shared goals as part of these collective endeavours means that interoperability is vital, particularly as it relates to the sharing of information and synchronization of actions. At the same time, our thinking about interoperability must evolve as it relates to PDC2. Processes, structures, and technology must consider priorities for how commonality, compatibility or interchangeability will best enable pan-domain information to be shared across the CAF and with partners. Likewise, our people must possess the right skills and mindsets to bridge different organizational cultures so shared awareness can be produced and actions efficiently coordinated to achieve desired integrated effects.

Integration and Alignment. PDC2 demands significantly greater integration than the CAF is accustomed to. The complexity of the operating environment requires that the CAF adopt an integrated operational approach and act deliberately in conjunction with all government departments, allies, and partners. This will help position the CAF to train, conduct exercises, and carry out campaigns more effectively.

Legacy C2 models built on a conception of jointness that leveraged service or domain specific components to achieve effects will need to evolve to reflect that no service nor domain is isolated from others, and they are in fact mutually supporting and dependent.

C2 Agility. Traditional requirements of C2 structures change from mission to mission. The ability to anticipate, effect, cope with, and/or exploit changes in circumstances is more complex in a pan-domain context. C2 agility is required to employ CAF resources effectively and efficiently. Mission command C2 structures including the delegation of authorities must be tailored to the specific context and to battle manage as a scalable, dispersed C2 force element. There is no one-size-fits-all approach.

Cognitive Resilience. Change in mindset is required to deliver integrated effects across all domains to address challenges posed by a much more complex operating environment. PDC2 must enable informed decision making in an environment that is rich in data and operate within an increasingly faster decision cycle. Human cognition and decision-making ability are likely to be the limiting factors. Despite this reality, accountability will remain with human decision-makers, therefore, PDC2 must acknowledge this in design and implementation. Additionally, knowing that threat actors will purposely target the human cognitive processes of staff and commanders to derive advantage, human cognition processes are critical and must be protected.

Humanitarian Assistance and Disaster Relief: *When a major natural disaster strikes, the CAF must rapidly deploy forces to provide aid and support to civilian authorities. Aggregating data from satellites, drones, ground sensors, and reports from personnel builds a detailed picture of damaged infrastructure, displaced populations, and resource requirements. Seamless sharing of the integrated picture with civilian agencies will enable the CAF to prioritize relief efforts and coordinate effectively.*

Trusted and Secure. Cyber resilience is a primary consideration for PDC2 capabilities including infrastructure, core services, and platforms (aircraft, ships, and vehicles, etc.) which are increasingly generating massive amounts of data and are dependent on cyberspace. Canada's adversaries will attempt to exploit vulnerabilities, highlighting the need for confidentiality, integrity, and availability. Our people, processes, structures, data, and technology must be trusted and secured across all networks, classification levels, at all physical and logical endpoints, and within the information environment and across the electromagnetic spectrum.

Centrality of Data. Data and information have always been necessary for militaries to make sense of their environment. The volume, velocity, and variety of data across the pan-domain environment has expanded exponentially in recent years, as has the technology to harness it. Leveraging data depends on how data is governed and managed, as well as a shift in mindset to view and treat data as a shared and strategic asset essential for mission success and operational readiness. Data itself is a significant national and military resource that must be protected and exploited. It must be accessible, secure, accurate, managed ethically, and shared, to drive informed decision making.

Experimentation and Innovation. The required shift to PDC2 is driven by the evolving character of modern warfare, and DND/CAF must be willing to embrace the necessary capabilities to enable PDC2 effectively. To do so, lessons learned, simulations, and experimentation must be incorporated as part of capability development to leverage government, private sector, and academia innovations and a willingness to take calculated risks.

By adopting these principles, and challenging existing conventions and embracing new approaches, DND/CAF can outpace adversaries and ensure our forces are equipped with the most effective tools and systems to adapt to the ever-evolving character of conflict.
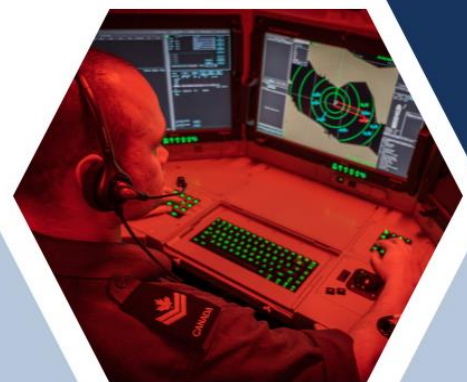
Core Concept: PDC2 Defined

The PDC2 concept is about gaining advantage over our adversaries through the optimization of the *Sense, Make Sense, Decide, Act* (SMDA) decision cycle. This concept requires empowered **People**, agile **Processes**, resilient **Structures,** and diverse decision-support **Technology,** all of which will enable the rapid leveraging of **Data.** Collectively, these components support allied interoperability and integrated effects across all domains. The evolution of these five (5) components are foundational to the PDC2 concept.

Critical to understanding the function of C2 is the fact that it is both an *action* and a *capability*. It is an *action* which manifests in the planning, preparation, execution, assessment, and adaptation of operations.

C2 is where a decision maker, commander, or staff, evaluates, describes, and directs the necessary actions to achieve the mission. It is also a *capability* that entails five components: People, Processes, Structures, Data, and Technology. Like any other capability it needs to be managed, developed, generated, and sustained. This duality must be understood to chart the path forward to operationalize the PDC2 concept and a force capable of employing it. These dual aspects are explored in the following sections:

- *Section 5 - C2 as an Action (Decision Cycle)*
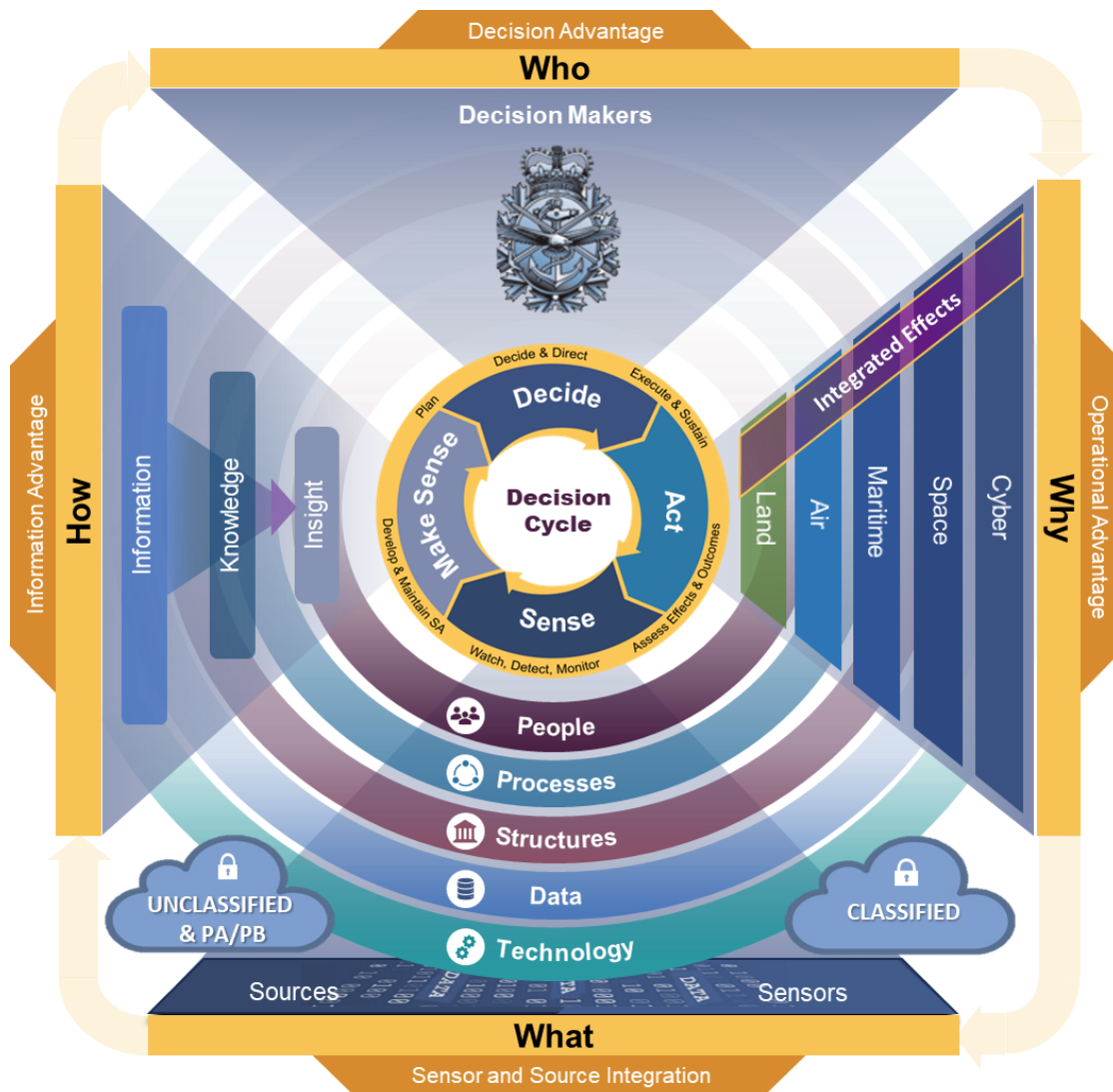- *Section 6 - C2 as a Capability (Components)*

Figure 2 – Connecting Sources & Sensors to achieve Integrated Effects through the SMDA Decision Cycle

5. C2 as an Action: Pan-Domain Decision Action Cycle

Sense-Make Sense-Decide-Act (SMDA) is at the heart of achieving the decision advantage required to effect CAF mission outcomes. In its simplest form, a decision cycle is simply a sequence of steps or activities used by an individual or organization to make decisions on a repeatable basis.
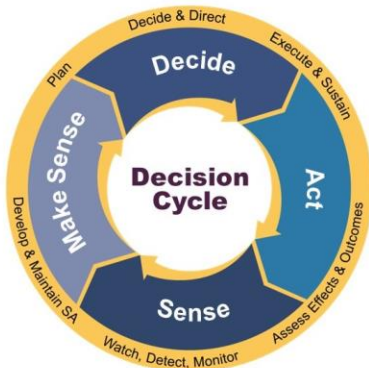

Figure 3 - Decision Cycle

While depicted as a sequential cycle, each phase can occur concurrently, and multiple cycles can be occurring simultaneously throughout the operating environment. This Decision Cycle (an evolution of the *Observe-Orient-Decide-Act* loop adopted by CAF to align with our allies) drives disciplined, integrated, and informed decisions and action at a scale and speed to achieve decision and operational advantage. The four (4) phases of SMDA are:

Sense. The *Sense* phase is driven by the decision-makers' data requirements to gain insights about the operating environment. This phase is used to gather data from sensors and sources required to understand the evolving situation. The *Sense* phase will generate such a high volume of data that making it accessible, sharable, and available to support decision making across the entirety of the operational environment is essential. This will require new and advanced digital tools and technology, paired with integrated processes and structures that forms the foundation for PDSA. The *Sense* phase is comprehensive, persistent, and continuous, and as such the remainder of the decision cycle may need to be reassessed when new data indicates a significant change in the situation.

Make Sense. The *Make Sense* phase entails the fusion, analysis, and synthesis of the sensed data and information into relevant knowledge and understanding of the operating environment. This includes making sense of data and assessments of actions already taken. Given the volume, variety, and speed of incoming data from across the integrated operating environment, digital tools and technology will be required to aid in the *Make Sense* phase, along with people, structures and processes that ensure that the right information is shared with the right decision-makers in a timely manner (**Information Advantage**). These tools and applications will include the use of advanced technologies (including AI, ML, digital automation, etc.), enabling decision-makers to gain insights and enhanced visibility of the operating environment, adversary, and friendly situations. The *Make Sense* phase provides a comprehensive view of the pan-domain environment allowing for better understanding and decision making.

Continental Defence: *The CAF must work closely with the United States and other allies to defend North America against threats like aircraft, cruise missiles and hypersonic weapons. Integrating data from early warning radars, satellites, and other sensors across the continent will provide a unified picture of the airspace. This will enable rapid decision making and coordinated responses to protect Canada and North America.*

Decide. Human decision-makers will continue to be central to the *Decide* phase and will be increasingly enabled by technology like AI which will support planning processes through methods such as rapid development of Courses of Action (COA) and COA evaluation. Likewise, decision-support processes will leverage AI, simulation, visualization, and critical thinking methodologies like wargaming and alternative analysis to overcome biases and make best use of gathered data. Aided by technology and structures which support appropriately delegated decision making, the *Decide* phase will produce timely, evidence-based decisions at speed (**Decision Advantage**), reducing the lag between Sense and Act.

Act. The *Act* phase allows decision-makers to issue direction or orders and take conscious actions to achieve the effects that lead to, or contribute to, desired objectives and outcomes (**Operational Advantage**). Decisions and subsequent actions (human and human-machine paired) impact the operational environment and generate additional data and information to be re-assessed. Assessment is a continuous process that takes place at all levels and includes measures of performance and measures of effectiveness that evaluate outcomes of missions, battle damage, tasks, and effects, which initiates another iteration of the decision-action cycle.

> *"To prepare to respond to faster, harder-to-detect incursions, we are increasing the speed of our operational decision making, leveraging advances in cloud-based computing, artificial intelligence and machine learning."*
>
> **Our North, Strong and Free**

6. C2 as a Capability: Components

C2 as a capability is made up of five components: *People, Process, Structures, Data*, and *Technology*. An effective PDC2 capability must cope with the complexities of these components in the contemporary operating environment and consider the cross-cutting aspects of C2 Interoperability and C2 Agility.

C2 Interoperability and C2 Agility

As Canada rarely operates alone, interoperability is a critical requirement of most capabilities. C2 is no exception, and the CAF's goal is to achieve the highest level of interoperability possible with Allies and key partners such that data and critical information can be shared seamlessly prior to the first day of conflict to achieve shared understanding and unity of effort from the outset.

Missions and operations exist on a spectrum of complexity with differing contexts and requirements. To be as effective as possible faced with this reality, the CAF needs more than a one-size-fits-all approach to C2. Instead, the components of a PDC2 must be able to adjust to changes in the environment and be able to operate within and recover from degrading conditions.

The CAF must also be able to employ different C2 approaches, act in a timely manner, maintain effectiveness across a range of tasks, and be able to do new things (e.g. expand and contract and share tasks with coalition partners).

Change and uncertainty are the dominant characteristics of the contemporary operating environment and an organization better enabled to use its SMDA cycle to anticipate, successfully effect, cope with, and/or exploit changes will have a competitive advantage. To be effective in the contemporary operating environment, C2 as a capability must be agile.

With interoperability scaling between compatibility to commonality, and manifesting differently across the components, key considerations for *People, Processes, Structures, Data,* and *Technology* are highlighted in the following sections.
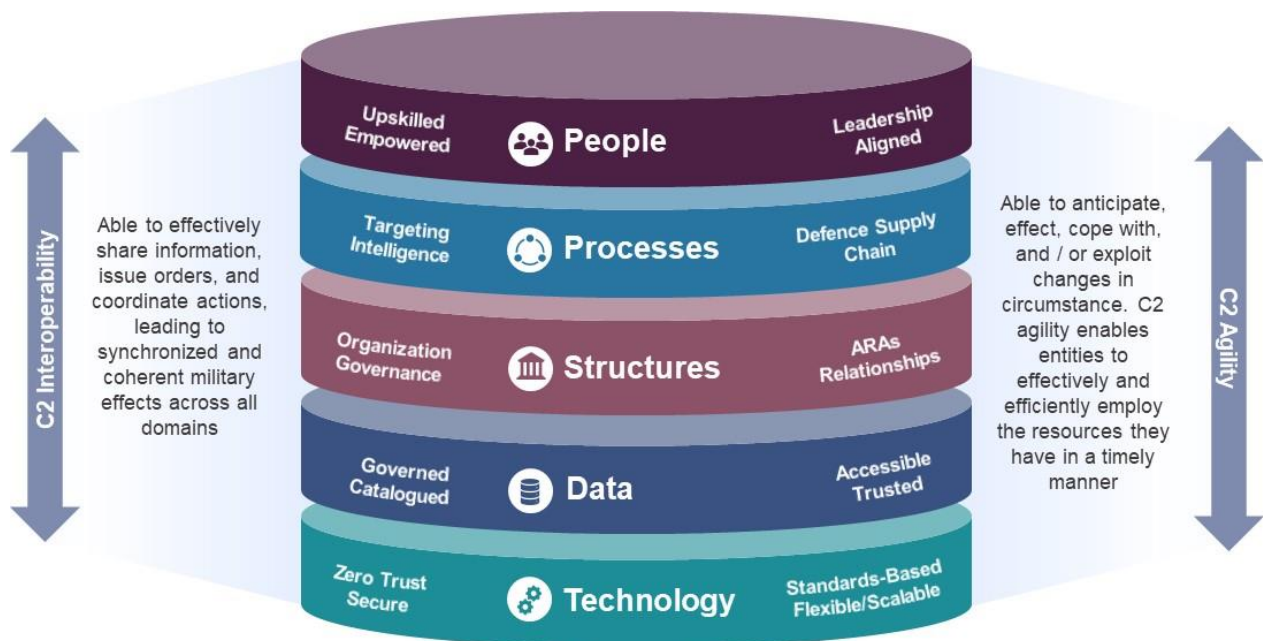

Figure 4 - PDC2 Components

People

Adopting PDC2 requires that Defence Team members become critical enablers of a sophisticated, interconnected C2 ecosystem that spans across maritime, land, air, space, and cyber domains, as well as the information environment. CAF personnel and the system must also integrate with multinational partners, Allies, and other elements of the Canadian Government. This paradigm places an unprecedented emphasis on the cognitive, technical, and collaborative capabilities of CAF members, positioning them as the linchpin in the effective execution of C2 in a pan-domain environment.

The PDC2 concept requires a profound shift in operational mindset and strategic orientation. This shift underscores the primacy of human capital, recognizing that the effectiveness of PDC2 is inherently dependent on the ability and willingness of CAF leaders and members at all levels to change. PDC2 hinges not just on technological

advancements but, more crucially, on the leadership, adaptability, competence, trust, respect for, and empowerment of the people within the organization. CAF personnel must train and operate with a pan-domain perspective by default.

CAF must equip its commanders with the 'soft' skills necessary to effectively operate within the modern operating environment, including systems thinking, collaboration, adaptability, and empathy. Without these skills, defence cannot produce military commanders who appreciate the complexities of MDO and, in turn defence will not be able to operate effectively against our adversaries. CAF personnel must adopt an adaptive agile mindset leveraging a diverse array of knowledge, skills, and critical thinking to navigate these varying degrees of complexity.

> **Mindset Shift**: Implementing PDC2 requires a profound cultural change, emphasizing leadership, adaptability, critical thinking, willingness to take calculated risk, and empowerment at all levels.
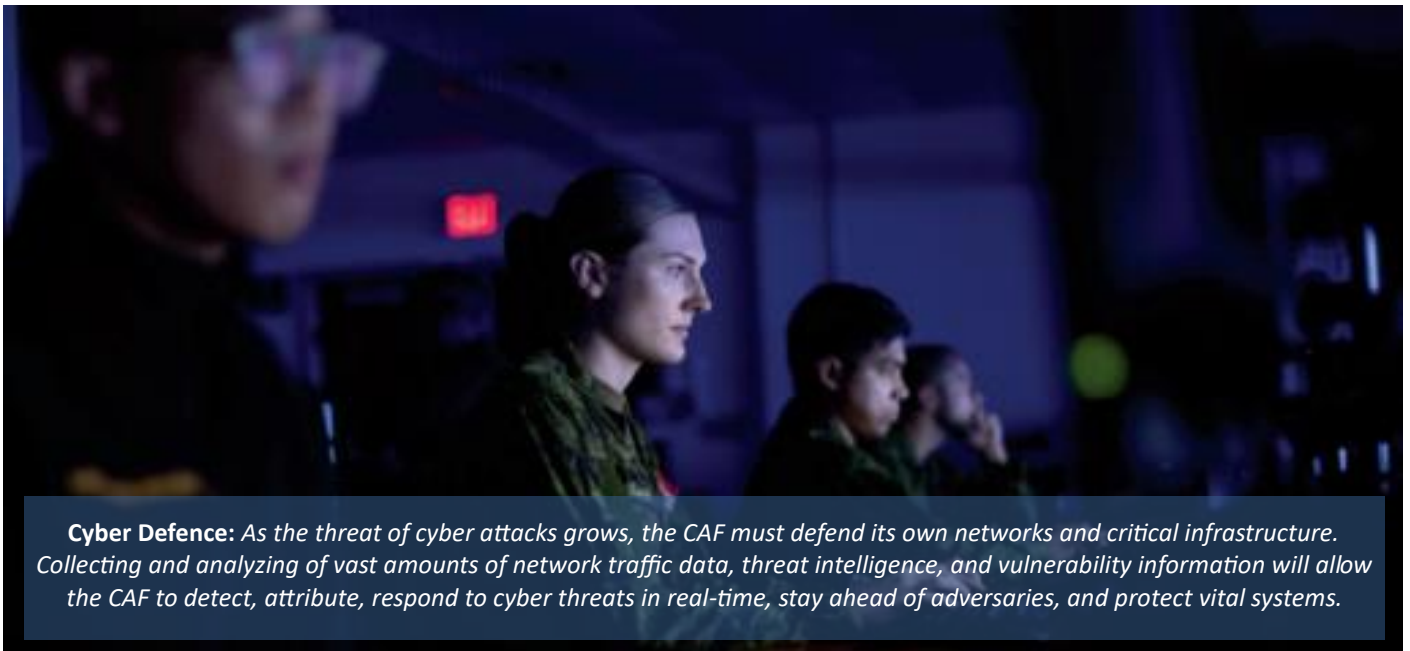
Cyber Defence: *As the threat of cyber attacks grows, the CAF must defend its own networks and critical infrastructure. Collecting and analyzing of vast amounts of network traffic data, threat intelligence, and vulnerability information will allow the CAF to detect, attribute, respond to cyber threats in real-time, stay ahead of adversaries, and protect vital systems.*

Processes

Processes are a series of actions or steps, usually taken in order, by which the individual parts of the decision cycle are achieved. They can be designed in various ways to support decision-makers through the exchange of information through liaison, coordination, collaboration, synchronization and integration of resources, capabilities, activities, and effects.

Processes include the steps to manage accurate and reliable inputs, conduct analysis, and produce relevant outputs. Sensemaking supports human cognition, insight, and reasoning, and to ensure that outputs are timely, valid, and relevant, expand and contract to the tempo of operations. Process and workflow automation will play a key role in the development of insights in support of shared understanding, decision making and actions.

Existing processes, such as those associated with campaigning, targeting, intelligence and operations need to be updated and new ones created and exercised to execute PDC2. While traditional processes already include human, human-to-machine, and machine-to-machine processes, operating in a pan-domain environment brings a demand for greater automation and adoption of human-to-machine teaming.

Process Evolution: Existing processes must be updated, and new ones created to support pan-domain operations, leveraging automation, AI, ML and advanced analytics.

Arctic Sovereignty Patrol: *As climate change opens the Arctic, the CAF must monitor the region for increased activity by adversaries. Sensors across air, land, sea, and space domains will collect vast amounts of data on weather, ice conditions, vessel movements, and airspace activity. Ingesting and analyzing data in real-time, will provide decision-makers with a comprehensive understanding of the operating environment to coordinate responses and assert Canadian sovereignty.*

Structures

While structures include the buildings, workspaces and facilities where the actions of C2 physically takes place, an additional focus within the PDC2 framework is the intangible structures which govern interactions and decision making. Focus areas include policies, authorities, organizational hierarchies, groupings, relationships, and delegated decision rights.

The CAF is faced with the imperative to evolve its C2 structures and supporting systems to meet the challenges of planning, executing, assessing, and adapting military operations in a pan-domain environment. No situation will demand the same C2 structure, hence they will need to be designed based on the relevant factors: whether the operation is continental, expeditionary, or cyber; threat landscape; if it is within an alliance construct; who are the supported/supporting commanders; and what are the strategic and operational objectives. This includes determining the appropriate level of decentralization of authorities.

The National Defence Operations and Intelligence Center (NDOIC) represents the physical embodiment of PDC2 and serves as the nucleus for integrating intelligence and operational activities, enabling effective and sound decision making in complex operational environments at the strategic and operational level. However, PDC2 as a concept does not end with the NDOIC. Its manifestation must also exist in the CAF's Joint Task Forces and National Command and Support Elements, and the various operations centres across the CAF.

These structures will demand that organizational and functional silos be eliminated. Physical, authority and reporting structures should be flexible and responsive to evolving situations and enable the stand up of ad hoc teams. Ongoing doctrine and concept development will need to account for the demands of PDC2.

Data

Data is the foundational component that underpins informed decision making in military operations. The right data needs to be available to the right people, in the right place, at the right time. Quality data needs to be integrated, discoverable, shareable, accessible, secure, trusted, and well-managed.

Within the framework of PDC2, data from various sources will critically influence all decision-makers. The advent and proliferation of sensors and technology-enabled platforms introduces a plethora of datasets previously unavailable to the CAF. The collection, processing, storage, analysis, and dissemination of data with new capabilities built with these technological advancements will significantly transform our reliance on intuition, past training, and operational experience for decision making.

With the deluge of data from sensors and sources across all domains, determining what is relevant and then making it actionable is critical for sound decision making. Advanced data integration and fusion techniques - including AI, ML, deep learning, data virtualization, and analytics - can help identify gaps and determine what data is relevant to collect and manage.

Data will be continuously collected, catalogued, and integrated with foundational datasets. Ultimately, our decisions and actions will produce even more data that must be managed and used for assessments to determine if we achieved the desired integrated effects and outcomes. Clear policies, procedures, and roles/responsibilities for managing data quality, privacy, and security throughout the lifecycle are essential.

DND/CAF is currently undertaking a refresh of its Data Strategy to align with newer policy direction issued by the Treasury Board Secretariat and our international partners, as well as the immediate data-focused operational needs of the CAF. The core pillars are:

- Empower and Equip the Defence Team;
- Manage and Govern Data for a Data-by-Design Approach;
- Exploit Data for Decision Advantage; and
- Enable Data-Driven Services for the User

Data must be understood not merely as raw numbers or facts but as the cornerstone of a continuum that progresses to information, knowledge, and ultimately, insight. This continuum underpins the SMDA decision action cycle.

"Canada will build a data-driven organization capable of transforming data into actionable information that will allow for rapid decision making and near real-time responses. It will also ensure the Canadian Armed Forces can remain interoperable with our most important Allies and partners well into the future."

Our North, Strong and Free

Technology

The latest and relevant advancements in infrastructure, platforms, and applications bring new means to enable CAF C2. The CAF must maintain a forward-looking approach, continually scanning the horizon for new opportunities to innovate, adopt, adapt, and improve.

The CAF must improve C2 interoperability both internally and with Allies. To do so, the Defence Team must focus and accelerate efforts to be interoperable with the US' CJADC2 and Mission Partner Environment (MPE); become, and remain, compliant with NATO's Federated Mission Networking (FMN); and accelerate the adoption of secure cloud (including classified cloud). This will, in part, be accomplished through prioritized and strategic adoption of relevant standards and protocols. The CAF's framework for alignment and interoperability with our allies is the Canadian Deployable Mission Network (CDMN).

Secure cloud is the backbone for both core and community-of-interest services supporting PDC2. It offers the CAF scalable and resilient computing resources accessible from around the world to share data across operational domains, facilitating rapid decision making and breaking down existing silos.

CAF Allies, particularly the US, have advanced their defence cloud solutions. The CAF needs to be a close follower and ensure that its sovereign defence solutions will be robust and secure, enabling Day Zero C2 interoperability with our Allies. To evolve from a network-centric security model, the Defence Team will incorporate various strategies:

- **Data-Centric Security (DCS)** is a concept focused on protecting data directly, enhancing interoperability and secure information sharing. It complements traditional network-centric security by enforcing policy-based access controls and key elements like data discovery and identity management.

- **Zero Trust (ZT)** concept integrates data protection and network security into a unified model that continuously verifies access to all resources.

- **Identity, Credential, and Access Management (ICAM)** integrates digital identities and access controls to enable secure access to critical resources.

- **Attribute-Based Access Control (ABAC)** enhances data security by allowing granular access controls based on user attributes and contextual factors.

Together, DCS, ZT, ICAM, and ABAC form a comprehensive security framework for operating in a pan-domain C2 environment. Collectively, these concepts (Figure 5) are essential for the CAF's emerging secure cloud adoption strategy and are foundational to internal and external interoperability.

From

Network Centric Security (NCS)
- *Protect the network/perimeter*
- *Don't trust outside*
- *Trust inside*

Always Trust, Sometimes Verify

To

Data Centric Security (DCS)
- *Protects data and objects (rather than the perimeter)*
- *Supports dynamic security policy for sharing data*
- *Depends on secure data labelling*

Enables Data Stewards

Zero Trust (ZT)
- *Concept that assumes all users, devices, and applications are untrusted by default*
- *Users verified before granted access to resources*

Don't Trust, Always Verify

Enabled by

Identity Credentials Access Management (ICAM)
- *Enables access across networks internally*
- *Federates access externally with Allies*

Attribute Based Access Control (ABAC)
- *Concept for authorization of operations*
- *Determined by attributes of the subject, object, and/or environment properties*

Figure 5 - Data-centric and access control strategies support path towards Interoperability

Artificial Intelligence (AI) and Machine Learning (ML)

The *DND/CAF AI Strategy* defines AI as "the capability of a computer to do things that are normally associated with human cognition, such as reasoning, learning, and self-improvement". ML is a branch of AI and computer science that focuses on using data and algorithms to enable AI to imitate the way that humans learn, gradually improving its accuracy. While the advantage of ML is its ability to perform quantitative analyses on large datasets, the effectiveness of ML and deep learning depends on access to sufficient, relevant, and high-quality data. Decision advantage will increasingly rely on access to and ability to process overwhelming data using these techniques. CAF must defend against threat actors targeting AI cognition by attempting to degrade and damage sources, services, and processes.

The *DND/CAF AI Strategy* also acknowledges the risks of AI and ML, including lower traceability of decisions and a trend toward homogeneity of thought, opinions, and inputs. In considering the SMDA decision cycle, AI augments the ability to enable data-driven decision making. There is no panacea when it comes to AI, and it needs to be understood that there will be many AI solutions that can automate simple processes in a broader C2 context.

AI can permeate various functions like intelligence, logistics, health services, operations, administration, and training by augmenting human cognition. Continuous updating and improvement will be essential for responsible utilization of AI.

Special Operations: *Elite CAF units require precise, time-sensitive intelligence to execute sensitive missions. Collecting and processing data from human sources, signals intelligence, and other specialized sensors provides decision-makers with actionable information. This will allow special operators to conduct successful raids, hostage rescues, and other critical operations.*

Conclusion

The international system is changing rapidly with technology evolving at an accelerating rate. This demands immediate change. The *Pan-Domain Force Employment Concept* (PFEC) established the foundation to comprehend the new operating environment and started the CAF's evolution. To effect the changes demanded by operating in a pan-domain environment, the CAF must evolve its approach to C2.

The PDC2 concept provides the impetus to transform the way the CAF conducts C2. It demands the CAF make necessary changes to its processes, structures, and technology, while at the same time better empowering its people so that data can be connected in real time with decision-makers to make better decisions. The security environment of persistent competition with a high potential for conflict will require the CAF to posture forces and closely align decision cycles with allies, partners, and stakeholders to successfully achieve strategic objectives. This will require an integrated approach that will increasingly be domain agnostic.

PDC2 considers C2 as both an action and a capability. At its core, PDC2 is based on the SMDA decision-action cycle, which is supported by the components of People, Processes, Structures, Data and Technology. It is built upon a foundation of data acquired from across the integrated operational and sustainment environments, to include both adversary and friendly data and information. Supported by technologies such as ML and AI to process, analyze, and synthesize, this data enables reaching data-driven decisions at speed of relevance.

To make the necessary changes, the CAF will need to take deliberate action across the People, Processes, Data, Structures, and Technology components. It will also need to coordinate changes between these PDC2 components as all military activities and organizations become increasingly harmonized. This process of change will take time, however, there are immediate steps that are ongoing and must be pursued aggressively. Others will be pursued as part of the *Digital Campaign Plan* with a view of the CAF being digitally transformed by 2030.

Critical in achieving the required change is cultivation of a cadre of "pan-domain-minded" leaders, emphasizing the importance of fostering a forward-looking leadership culture capable of navigating the challenges of achieving military effects in a pan-domain environment. These efforts underscore the imperative of adapting to evolving technological landscapes and adopting a campaigning mindset to meet the challenges of contemporary security environments effectively.

PDC2 aligns the CAF well with allied partners, particularly the US CJADC2, the UK MDI program, and NATO's MDO efforts. In the near term, the priority will be to participate in allied experimentation for CJADC2, such as the US-led Project Olympus to align the development of the PDC2 capability and improve interoperability with the US and other Allies.

In the Canadian context, PDC2 must also be a pillar of the Force Command concept and a foundational capability of the NDOIC. The evolution of the PDC2 concept will enable the CAF to remain a trusted and relevant partner in combined operations. Additionally, the operational advantage achieved through evidence-based decision making will enable the CAF to compete, contest, confront and, if necessary, defeat adversaries in combat.

PDC2 Glossary

Air Domain: The atmosphere, beginning at the Earth's surface, extending to an altitude of 100 kilometres.

C2 Action: The exercise of authority and direction by a designated commander over assigned forces in the accomplishment of the force's mission. The functions of command and control are performed through an arrangement of personnel, equipment, communications, facilities, and procedures that are employed by a commander in planning, directing, coordinating, and controlling forces in the accomplishment of the mission.

C2 Agility: Ability to anticipate, effect, cope with, and/or exploit changes in circumstance. C2 agility enables entities to employ the resources effectively and efficiently they have in a timely manner.

C2 Capability: A complex socio-technical system whose purpose is to lead, coordinate, plan, organize and control activities across multiple domains.

C2 Interoperability: The integration of command and control systems to effectively share information, issue orders, and coordinate actions, leading to synchronized and coherent military effects across all domains

C2: The authority, responsibilities and activities of military commanders in the direction and coordination of military forces as well as the implementation of orders related to the execution of operations (*DTB # 13802*).

Campaign: A set of military operations planned and conducted to achieve a strategic objective (*DTB # 18743*).

Capability: The ability to contribute to the achievement of a desired effect in a given environment within a specified time and sustainment of that effect for a designated period. It comprised of functional components, as listed under PRICIE+G (*CBP Handbook, 2019*).

CDMN: Canadian Deployable Mission Network

CJADC2: US Combined Joint All-Domain C2 is a strategic approach for shaping future Combined Joint Force C2 capabilities that uses MPE as the mechanism by which partners integrate with the US

Compete: To seek advantage in the international system through the pursuit of national objectives.

Cyber Domain: The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those that are separated or independent, which process, store, or transmit data (*DTB # 694338*).

Data Management: The life-cycle management of plans, policies, programmes and practices that control and protect data assets. (*DTB # 27521*)

Day Zero Interoperability: Integration into partner and allied networks, systems, concepts, and plans, prior to the commencement of operations to enable the seamless coordination and exchange of data. Note: term is consistent with NATO FMN terminology.

Decision Advantage: The ability of commanders, based upon information superiority and situational awareness, to make effective decisions more rapidly than their adversary, thereby gaining an advantage in the tempo, coherence and effectiveness of operations (*DTB # 41405*).

Digital Interoperability: The exchange of data and information between platforms, sensors, and communication devices.

DIME: Diplomacy, Information, Military, and Economic instruments of national power

Domain: A major part of the operating environment with specific properties that affect the conduct of military operations. The CAF recognizes five domains: maritime, land, air, space, and cyber.

FMN: NATO's Federated Mission Networking establishes common standards and protocols for interoperability among members and partner organizations.

Force Command: Represents the CDS' function of planning, directing, monitoring of all the following five strategic functions with the support from the DM 5Fs +D (CFJP 01 Capstone Doctrine, 2023)

Information Environment: An environment composed of individuals, organizations and systems that collect, process, disseminate, or act on information as well as the information itself (*DTB # 695898*).

Instruments of National Power: The means available to the government in its pursuit of national objectives. Note: They are expressed as diplomatic, informational, military, and economic (DIME).

Interchangeability: The ability of one product, process or service to be used in place of another to fulfil the same requirements (*DTB # 4566*).

Interoperability: The ability to act together coherently, effectively, and efficiently to achieve common objectives. Note: Interoperability may be achieved through the compatibility of doctrine, processes, and materiel (*DTB # 32228*).

Land Domain: The Earth's surface ending at the high-water mark.

Maritime Domain: The Earth's oceans, seas, and navigable waterways.

MDI: UK Multi Domain Integration (MDI) program.

MDO: NATO Multi Domain Operations (MDO) concept.

Mission command: A philosophy of command that promotes unity of effort by means of a clear expression of the higher and superior commanders' intents, and the delegation of authority to subordinate commanders to use their initiative in accordance with these intents. (*DTB # 21037*)

MPE: US Mission Partner Environment facilitates information sharing and interoperability among allied nations and serves as a platform for enhancing communication, coordination, and cooperation to strengthen collective defence capabilities.

Operating Environment: The surroundings in which military operations take place (*DTB # 43606*).

Pan-domain: Across the operational environment as a unified whole. Note: Some of Canada's Allies have adopted similar terms "Multi-Domain" and "All-Domain". These terms have a common objective of achieving coherence across domains as a unified whole.

PDC2 Component: For purposes of the PDC2 concept, areas of key consideration for the overall capability. Includes: *People*, *Processes*, *Structures*, *Data,* and *Technology.*

PDC2: Exercising C2 in a pan-domain environment.

PDSA: Situational Awareness in a Pan-Domain context

Revisionist State: is a term from power transition theory within the wider field of international relations. It describes states whose objective is to change or put an end to the current system.

Rules-Based International Order (RBIO): The cooperative global framework of political and economic rules, relationships, international organizations and regulations put in place at the end of the Second World War.

Secure Cloud: For purposes of this paper includes unclassified, protected, and classified compute and store.

Situation Awareness: An understanding of the operating environment necessary to make well-informed decisions. (*DTB # 41441*)

Space Domain: The area surrounding Earth at altitudes of greater than or equal to 100 kilometres above mean sea level. (*US JP 3-14*).

Whole of Government (WoG) approach: An integrated approach to a situation that incorporates diplomatic, economic, military, and informational instruments of national power (*DTB # 35242*).

Whole of Nation (WoN) approach: An integrated approach to a situation that incorporates government, the private sector, academia, civil society, communities, and individuals.

Zero Trust: An enterprise approach to the security of a system design based on the principle that inherent trust is never granted by default to any subject (*DTB #697017*).

PAN-DOMAIN COMMAND AND CONTROL (PDC2)
Concept Paper