National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Putting the Human and Its Agility Back Into C4ISR: Implications of the Pan-Domain Force Employment Concept on Command and Control

Lieutenant-Colonel Patrick J.G. Perron

JCSP 47

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2021.

PCEMI 47

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2021.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 47 – PCEMI 47

2020 – 2021

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

PUTTING THE HUMAN AND ITS AGILITY BACK INTO C4ISR: IMPLICATIONS OF THE PAN-DOMAIN FORCE EMPLOYMENT CONCEPT ON COMMAND AND CONTROL

By Lieutenant-Colonel P.J.G. Perron

"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The return of great power competition and the proliferation of technology is changing the character of conflict. Allied militaries are rapidly evolving their warfighting concepts from "jointness" toward "multi-domain." Underpinning these multi-domain concepts is the existence of a ubiquitous "C4ISR spine" connecting all sensors, shooters, headquarters, and allies with the inter-agency enterprise. These concepts, including the proposed Canadian pan-domain concept, appear to evolve from network-centric warfare, which sought information and decision superiority through digital connectivity and information sharing. This paper examines how DND/CAF can evolve its C2 system to prepare itself for a future marked by inter-agency and coalition pan-domain operations. It reviews the American and British multi-domain concepts, C2 definitions, C2 theoretical frameworks and interoperability; then, it examines how organizational culture and trust affect C2 agility. This paper argues that, besides leveraging artificial intelligence, DND/CAF should view C4ISR as an evolving socio-technical network that will require relationship and trust-building with various partners, social interoperability before technical compatibility, and the honest intent to embrace human and organizational agility. Despite the greater scope and complexity of 21st-century operations, over-reliance on technology could exacerbate C2 rather than enable it. While sociological factors such as culture, trust, policies and politics can enable or impede interoperability, no technological solution can offset the lack of social interoperability. 21st-century operations will require developing trusting relationships with various interdependent and heterogeneous partners for which no single individual is in charge of the collective. The

human, organizational, sociological and political aspects discussed in this paper could provide a basis for any future institutional analysis of DND/CAF pan-domain C2.

INTRODUCTION

On 11 July 2014, just outside Zelenopillya, Russian forces launched cyber and electronic attacks against Ukrainian battalions that disrupted their Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system, while simultaneously deploying drones and locating Ukrainian soldiers' cellphones.[1] Subsequently, a combined long-range rocket and artillery strike that lasted less than three minutes destroyed two Ukrainian mechanized battalions.[2] In this example, the Russian forces successfully integrated multi-domain capabilities at the tactical level, under the command of a single Russian battalion commander. The Russians also apply multi-domain concepts at the operational and strategic levels, drawing on a broad range of hybrid and subversive tools, mainly under the threshold of armed conflict, and using the information as a weapon.

The return of great power competition and the information age's continued technological development have changed the character of conflicts. The proliferation of disruptive technology provides an asymmetric advantage to adversaries, whether they be state as in the above case, or non-state like Daesh. Adversaries like Russia and China developed layers of anti-access and area denial (A2AD) capabilities for armed conflict that challenge the United States' (US) superiority in the land, sea, air, space and cyber domains.[3] Examples of A2AD capabilities include electronic, cyber and counter-space

---

[1]Amos C. Fox, *Hybrid Warfare: The 21st Century Russian Way of Warfare* (Fort Leavenworth, Kansas: School of Advanced Military Studies, US Army Command and General Staff College, 2017), 37-38.

[2]Philip A. Karber, *Lessons Learned from the Russo-Ukrainian War, Personal Observations* (John Hopkins Applied Physics Lab & US Army Capabilities Center: 8 July 2015).

[3]Department of Defense, *TRADOC Pamphlet 525-3-1, the U.S. Army in Multi-Domain Operations 2028* (Washington, DC: US Army, 2018): 7-11. According to TRADOC, during armed conflict, China and Russia could employ A2AD systems "to create strategic and operational stand-off to separate elements of the joint force in time, space, and function." The US further defines "anti-access" as "actions and

capabilities, integrated air defence, long-range missiles and communications, including sophisticated levels of C4ISR integration.[4]

In addition to A2AD defences, Russia and China contest international norms and compete below the threshold of armed conflict using, for example, diplomatic and economic actions, unconventional warfare and information warfare.[5] The current chief of the general staff of Russian armed forces, General Valery Gerasimov, described the transformation of warfare from conventional to hybrid as:

> The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian and other non-military measures – applied in coordination with the protest of the population. All this is supplemented by military means of a concealed character, including carrying out the actions of informational conflict and the actions of the special operations forces.[6]

The 2014 annexation of Crimea is a notable example where Russia leveraged information to indoctrinate ethnic Russians living in eastern Ukraine and employed unconventional proxy organizations and "little green men," Russia's special operations forces, to achieve their political objectives.

To compensate for adversaries' levelling of domain capabilities and counter adversaries' multi-domain strategies, the US is evolving its warfighting concept beyond

---

capabilities, usually long-range, designed to prevent an opposing force from entering an operational area" and "area-denial" as "actions and capabilities, usually of shorter range, designed not to keep an opposing force out, but to limit its freedom of action within the operational area. US Department of Defense, *Joint Operational Access Concept* (Washington, DC: 2012), 6.

[4]Terrence K. Kelly et al., *Smarter Power, Stronger Partners, Volume 1: Exploiting U.S. Advantages to Prevent Aggression* (Santa Monica, California: RAND Corporation, 2016): 44, 49.

[5]Department of Defense, *TRADOC Pamphlet 525-3-1 . . .*, 26, 10, GL-6, GL-9. Unconventional warfare is defined as: "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force . . ." Information warfare is defined as "employing information capabilities in a deliberate disinformation campaign supported by actions of the intelligence organizations designed to confuse the enemy and achieve strategic objectives at minimal cost."

[6]Anthony King, *Command: The Twenty-First-Century General* (Cambridge: Cambridge University Press, 2019): 454. The original source is: General Valery Gerasimov, "The Value of Science in Prediction," *Military-Industrial Kurier*, 27 February 2013: 24.

"jointness" toward joint all-domain operations (JADO) as part of a "third-offset" strategy.[7] Central to JADO is the joint force requirement to "rapidly translate decisions into action, leveraging capabilities across all domains and with mission partners to achieve operational and information advantage in both competition and conflict;" in other words, to exercise joint all-domain command and control (JADC2).[8]

JADC2 is the US Department of Defense's concept to connect sensors from all military services into a single "cloud-like" network, processing data using artificial intelligence to identify targets and recommend the best kinetic or non-kinetic weapon to engage the target.[9] Senior military officers often reduce JADC2 to a physical network, or data architecture, enabled with artificial intelligence and machine learning algorithms, to be acquired.[10] In reality, JADC2 is more than a physical network connecting sensors and shooters in all domains. JADC2 aims to achieve information and decision-making superiority over adversaries through greater information sharing between domains, better understanding, and faster decision-making. The US Army and other services recently added "Combined" to the JADC2 concept, or CJADC2, reflecting the requirement to integrate with other coalition nations.[11]

---

[7]The Strategy Bridge, "The Integrated Joint Force: A Lethal Solution for Ensuring Military Preeminence," last accessed 21 January 2021, https://thestrategybridge.org/the-bridge/2018/3/2/the-integrated-joint-force-a-lethal-solution-for-ensuring-military-preeminence. The third-offset strategy emerged from strategic guidance issued by the President and Secretary of Defense in 2012. The third-offset emphasizes on leveraging artificial intelligence and automation.

[8]Department of Defense, *USAF Role in Joint all-Domain Operations* (Washington, DC: US Air Force, 2020): 2.

[9]Nishawn S. Smagh, *Joint all-Domain Command and Control (JADC2)* (Washington, DC: Congressional Research Service: 2020). https://fas.org/sgp/crs/natsec/IF11493.pdf

[10]This was the author's perception during briefings from senior CAF officers who compared JADC2 to a networking technology to be acquired as part of NORAD modernization.

[11]US Army, US Army Future Command, *Project Convergence*, last accessed 18 March 2021, https://armyfuturescommand.com/convergence/.

Similar to JADO/JADC2, the United Kingdom (UK) envisions multi-domain integration (MDI) beyond "jointness" with other government agencies, partners and allies to achieve a competitive advantage over adversaries. As indicated in the recent UK Ministry of Defence joint concept note, "MDI involves a contest for information advantage."[12] According to the British concept, MDI will achieve an advantage through a "command, control, communications, computers, intelligence, surveillance, target acquisition and reconnaissance (C4ISTAR) system that connects everything together and allows the system to function cohesively."[13] In essence, both the American JADO/JADC2 and British MDI concepts are reminiscent of network-centric warfare (NCW), also referred to as "network-enabled capability" in the British case, which sought to achieve enhanced effects, higher operational tempo and faster decision-making through the networking of sensors, decision-makers and shooters using digital technologies.[14]

The new Canadian Pan-Domain Force Employment Concept (PFEC) acknowledges the persistent state of "below the threshold" competition and describes how the Canadian Armed Forces (CAF) will "contest, confront and, when necessary, combat and prevail" against adversaries.[15] The PFEC identifies the imperative to meet

---

[12]Ministry of Defence, *Joint Concept Note 1/20, Multi-Domain Integration* (UK: Ministry of Defence, Director Development, Concepts and Doctrine Centre, 2020): 26.

[13]*Ibid*., 27.

[14]David S. Alberts, John Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd (Rev.) ed. (Washington, DC: National Defense University Press, 2000): 2.

[15]Department of National Defence, *Draft Pan-Domain Force Employment Concept (PFEC), Prevailing in an Uncertain World* (Ottawa: DND Canada, 2020): 4. At the time of writing, the draft PFEC is not authorized for release outside of Canadian Forces College (CFC) Toronto. CFC students are authorized to use PFEC as educational material and for discussion purposes. PFEC defines "pan-domain" as "a military construct that means relating to, affecting, occurring, or conducted across and throughout all domains as a unified whole."

this challenge across the cyber, space and information domains, in addition to the traditional land, air and maritime domains.[16] The PFEC also emphasizes the requirement to coordinate with other national power instruments and align CAF's plans and preparations with allied partners.[17] To enable the vision laid out in the PFEC, the Vice Chief of Defence Staff (VCDS) and the Associate Deputy Minister recently directed the force development community to orient their efforts around "data and digitalization" and establishing "a properly architected Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) spine."[18] The recently created "Chief of Combat System Integration" position within the VCDS organization illustrates the CAF's emphasis on jointly integrating technological systems within its C4ISR enterprise.

Notwithstanding the need to work toward developing an adequate "C4ISR spine" to enable the passage of data and information between services, departments and coalition partners in support of pan-domain operations, other non-technical aspects can challenge or play critical roles in enabling any C4ISR vision. Before providing a technical solution to a complex human and socio-technical problem, it is crucial to understand the implications, challenges and other intangible considerations associated with the PFEC. More importantly, the C4ISR system, comprised of people, processes and

---

[16]Allied countries have varying definitions of warfighting or operational domains. PFEC recognizes land, air, sea, space, cyber and information as operational domains. This paper will refer to land, air and sea as traditional domains, and cyber, space and information as either non-traditional or emerging domains.

[17]Department of National Defence, *Draft Pan-Domain Force Employment Concept, . . .,* 4. PFEC recognizes five imperatives: the CAF must evolve its thinking and planning from a "binary conception of war and peace" toward "competition, contest, confrontation, and conflict," "adopt a mindset able to meet this challenge across multiple domains," including cyber, space and information, coordinate with other instruments of national power, collaborate with and integrate plans with NATO, FVEY and other regional partners, and "strengthen North American defences while remaining globally coherent."

[18]Vice Chief of the Defence Staff, VCDS/DMA *Planning Guidance Data and Digitization* VCD2020-0015391 (Ottawa: DND Canada, 2020): 2.

technology, needs to enable C2 as the chief operational function, especially within a future marked by inter-agency and coalition pan-domain operations.

This paper seeks to answer the following question: as Canada's principal allies are rapidly modernizing their concepts and technologies, how can Department of National Defence (DND)/CAF evolve its command and control (C2) system to prepare itself for a future marked by inter-agency and coalition pan-domain operations? Besides leveraging artificial intelligence and networking technologies, DND/CAF should primarily consider the other human, organizational, and sociological aspects of C2 to make DND/CAF more agile and interoperable for ever-complex pan-domain operations. This approach will require DND/CAF to view C4ISR as an evolving socio-technical network that will require relationship and trust-building with various heterogeneous partners, social interoperability, and the honest intent to embrace human and organizational agility, including adopting mission command when necessary.

As a methodology, this directed research project considers how the US and the UK adapt to the changing character of conflicts by reviewing their published multi-domain concepts. It compares allied multidomain concepts with the draft Canadian PFEC, and previous concepts such as NCW, and discusses implications. After reviewing the definitions, theoretical frameworks and dimensions of C2, this project then considers sociological perspectives on how technology has changed the character of warfare in the 21st century, compared with the 20th century, and, above all, the character of C2 and mission command.

The remainder of this paper contains three chapters and a conclusion. After reviewing and comparing the US and UK multi-domain concepts with the PFEC, the first

chapter discusses that, similarly to the UK, the PFEC emphasizes the requirement for greater inter-agency and alliance/coalition integration in the face of complexifying multi-domain threats. As technological development continues to change the character of conflict, Canada's principal allies are embarking on a potentially elusive quest for information and decision superiority, not unlike the decade-old NCW concept, by investing in all-encompassing C4ISR networking technology connecting all sensors, shooters, as well as artificial intelligence applications. The second chapter reviews the concepts of command, control and C2, exploring historical and emerging definitions, theories, components and processes. It argues that human and organization agility, including the mental flexibility, creativity and intuition to adapt to complex situations, will remain foundational to effective C2. It also suggests that, despite the greater scope and complexity of 21st-century pan-domain operations, over-reliance on technology, including artificial intelligence, has the potential to exacerbate C2 rather than enable it. Despite challenges with decentralizing control authorities within organizations, DND/CAF will need to develop the agility to adopt different C2 approaches from centralized to decentralized, including mission command, depending on the situation and entities involved. After reviewing additional sociological considerations that can enable or impede C2 agility and interoperability, such as culture and trust, the third chapter discusses how the new security environment has forced Western military organizations to adopt a more collective approach to decision-making by carefully distributing authorities to highly professionalized command collectives. Establishing trusting relationships and harmonizing C2 processes with various military and non-military partners will be critical for 21st-century pan-domain operations. Rather than aiming for an all-encompassing

C4ISR network to exchange information, establishing higher levels of trust and interoperability and evolving the military culture to include less risk-aversion and more collaboration and facilitation will likely play a critical role for successful pan-domain operations. The concluding chapter summarizes the central human, organizational, and sociological aspects discussed in this paper, which could provide a basis for any future institutional analysis of DND/CAF pan-domain C2.

CHAPTER 1 – THE ELUSIVE QUEST FOR INFORMATION SUPERIORITY: REVIEW OF AMERICAN AND BRITISH MULTI-DOMAIN CONCEPTS

> *War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth.*
>
> - Carl von Clausewitz, *On War*

INTRODUCTION

Learning from how the US and its allies were fighting in Afghanistan and Iraq for the past two decades, peer adversaries developed technologies that now challenge the US dominance in each domain. The ongoing strategic competition in the "gray zone" blurs the line between war and peace and spans all elements of national power.[19] In response to the increasingly complex and dynamic security environment, many of Canada's allies have proposed "multi-domain" approaches for different levels of warfare. Whereas the US developed multi-domain operating concepts at the tactical and operational levels, the UK focused primarily on strategic and national multi-domain integration.[20] The newly drafted Canadian PFEC provides conceptual alignment with its principal allies.[21] Like the UK, the draft PFEC emphasizes the need for greater joint and pan-governmental integration without providing operational or tactical level multi-domain doctrine. Underpinning the American and British concepts is the renewed emphasis on leveraging

---

[19]Center for Strategic & International Studies (CSIS), *Competing in the Gray Zone*, last accessed 19 March 2021, https://www.csis.org/features/competing-gray-zone. CSIS uses "gray zone" to describe "actions that seek to gain an advantage without provoking a conventional military response," using non-military means such as "election meddling, economic coercion" or unconventional force.

[20]Ministry of Defence, *Joint Concept Note 1/20, Multi-Domain Integration* (UK: Ministry of Defence, Director Development, Concepts and Doctrine Centre, 2020)

[21]Other allies such as Australia are developing multi-domain concepts, e.g., the Australian Army's *Accelerated Warfare* shows similar thinking and doctrinal evolution. This paper limits its scope to the US and UK approaches, which place emphasis on different levels of warfare. Lieutenant-General Rick Burr, *Army in Motion, Accelerated Warfare Statement*, The Australian Army, 22 October 2020. https://www.army.gov.au/our-work/army-motion/accelerated-warfare

networking and artificial intelligence technologies to enhance information sharing and synergy between services, levels of warfare, allies, and other partners and achieve an information advantage in a manner reminiscent of the decade-old NCW concept.

US BOTTOM-UP DEVELOPMENTS ON MULTI-DOMAIN OPERATIONS

Novel threats from peer adversaries and the renewed possibility of major combat operations led the US Army to reintroduce the operational art of Air-Land Battle into a new way of warfighting initially called Multi-Domain Battle, then Multi-Domain Operations (MDO).[22] Acknowledging the changing character of warfare, which presents more interdependencies between traditional and emerging domains, the US Air Force developed the concepts of JADC2 and JADO as the next evolution beyond "jointness."[23] Inherent to JADO is the quest for information and decision superiority and leveraging fleeting opportunities to create local or temporary cross-domain superiority.

US Army Approach: Evolving from Air-Land Battle to Multi-Domain Operations

The US Army Multi-Domain Battle concept evolved from the Air-Land Battle doctrine developed in the 1970s by adding the other warfighting domains and extending

---

[22]Stephen Townsend, "Accelerating Multi-Domain Operations, Evolution of an Idea," *Army University Press,* Military Review Special Edition (Fort Leavenworth, Kansas, September-October 2018). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2018/Townsend-Multi-Domain-Operations/. The US Services have used numerous "buzzwords" that have evolved over the past decade to represent the idea of greater integration within the joint force, e.g., "cross-domain synergy," "joint concept for access and manoeuvre in the global commons," "integrated multi-domain operations," "multi-domain battle," "multi-domain operations," "multi-domain C2," and "joint all-domain C2."

[23]Jeffrey M. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," *Air & Space Power Journal* 30, no. 1 (2016): 61. Reilly describes the greater integration and interdependence of domains due to technological development. For example, actions in the electromagnetic environment or cyberspace could impact satellites in space, which could affect ISR capabilities, navigation, communication or early warning systems used in the land, air or sea domains. The idea of evolving the joint force toward interdependence is not new. Sociologist James D. Thompson described three types of interdependence: "pooled interdependence," where failure threatens all, "sequential interdependence," and "reciprocal interdependence," which requires back-and-forth coordination. See: Christipher R. Paparone, "What is Joint Interdependence Anyway?" *Military Review* (Fort Leavenworth, KS: US Army Combined Arms Center, August 2004). The original source is James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory* (New York: McGraw-Hill, 1967), 45-55.

the range of the battlespace geographically.[24] Air-Land Battle, which had successfully deterred the Warsaw Pact during the Cold War and defeated Saddam Hussein's forces in Iraq, leveraged the exercise of C2 to offset Soviet numerical superiority and sought to enhance combat power by synchronizing effects in both the land and air domains.[25] In the same vein, as peer adversaries began to challenge US superiority in each domain since 1991, Multi-Domain Battle also aims to achieve overmatch by creating and synchronizing effects in both traditional and emerging warfighting domains without increasing the number of military platforms or weapons systems.[26] Whereas the US developed Air-Land Battle to deal with a relatively known enemy, political situation and geographic area, Multi-Domain Battle recognizes the need for a joint, combined and multi-agency approach to counter today's more complex threats across domains during competition and conflict.

In 2018, the Multi-Domain Battle concept was renamed MDO to reflect the broader perspective that includes non-kinetic and non-military instruments.[27] Despite the

---

[24]David G. Perkins, "Preparing for the Fight Tonight: Multi-Domain Battle and Field Manual 3-0," *Military Review* 97, no. 5 (2017). This article is "part of a series of articles by General Perkins." The first article was: "Multi-Domain Battle: Driving Change to Win the Future," followed by: "Preparing for the Fight Tonight: Multi-Domain Battle and Field Manual 3-0," and finally: "Multi-Domain Battle: Advent of 21st Century War." Compared with Air-Land Battle, Multi-Domain Battle added strategic support and deep fires areas.

[25]David S. Alberts, *Operations in Multiple Domains: What's New, what's Not, and the Implications for Command and Control* (Utrecht, The Netherlands: NATO Command and Control Centre of Excellence, 2020): 3. An account of the development of air-land battle was written by: Douglas W. Skinner, *Airland Battle Doctrine*, Professional Paper 463, Strike and Amphibious Warfare Research Department, Center for Naval Analyses (Alexandria, Virginia: September 1988). https://apps.dtic.mil/sti/pdfs/ADA202888.pdf

[26]David G. Perkins and James M. Holmes, "Multidomain Battle: Converging Concepts Toward a Joint Solution," *Joint Force Quarterly,* no. 88 (2018). The requirement to evolve joint integration toward interdependence in a fiscally constrained environment was discussed before the advent of MDO or JADO. E.g., see: Jonathan Greenert, "Navy Perspective on Joint Force Interdependence," Joint Force Quarterly, National Defense University Press 76, 1st Quarter, January 2015 (30 December, 2014): 11. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-76/Article/577581/navy-perspective-on-joint-force-interdependence/

[27]Department of Defense, *TRADOC Pamphlet 525-3-1, the U.S. Army in Multi-Domain Operations 2028* (US Army, 2018). This pamphlet is considered the main reference on MDO according to: Carline Grispen-Gelens, "Cohesion through Convergence?" *Seminar 2020 MDO Read Ahead* (NATO C2COE, 1

change in nomenclature, MDO remains focused chiefly on conventional high-end warfighting in response to A2AD capabilities. MDO envisions US Army forces fighting with the rest of the joint force to "penetrate and disintegrate enemy A2AD systems and exploit the resultant freedom of manoeuvre to achieve strategic objectives."[28] MDO is predicated on three core tenets: calibrated force posture, multi-domain formations and convergence.

"Calibrated force posture" signifies having forward presences with the requisite permissions and authorities to operate in all domains. The US Army is in the process of configuring "multi-domain formations" above brigade with the required capabilities to operate in multiple contested domains. Accordingly, the US Army envisions its division, corps, field army and theatre army echelons capable of "converging" capabilities from various domains, the electromagnetic spectrum and the information environment.[29] Put differently, the US identifies the division as the lowest command echelon with the requisite size to coordinate the heterogeneous capabilities required for MDO. Underpinning the three MDO tenets is the requirement for echelons above brigade or the joint force to have the requisite authorities to exercise C2 effectively enough to generate "cross-domain synergy."[30] While MDO explains how to defeat a conventional peer

---

June 2020): 3. https://c2coe.org/download/seminar-2020-read-ahead-carlina-grispen-gelens-cohesion-through-convergence/

[28]Department of Defense, *TRADOC Pamphlet 525-3-1, . . .*, 17.

[29]*Ibid*., 17-21. The US Army defines "calibrated force posture" as "the combination of position and the ability to maneuver across strategic distances." It includes "basing and facilities, formations and equipment readiness, the distribution of capabilities across components, strategic transport availability, interoperability, access, and authorities." "Multi-domain formations" are "army organizations possessing the combination of capacity, capability, and endurance necessary to operate across multiple domains in contested spaces against a near-peer adversary." "Convergence" is defined as the "rapid and continuous integration of capabilities in all domains, the EMS, and information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative."

[30]Department of Defense, *Joint Operational Access Concept* (Washington, DC: US Department of Defense, 2012), 16. "Joint synergy" focuses on the "integration of service capabilities," whereas "cross-

enemy at the tactical and operational levels of war, it is less precise in describing how this will be integrated into the strategic inter-agency environment or with alliance/coalition members, especially for contingencies not involving all-out warfare.

Although not explicitly mentioned in the MDO papers, the US Army, and the rest of the joint force, would need an all-encompassing C4ISR network to enable the MDO vision.[31] To meet MDO's information communication technology requirements, the US Army is pursuing the development of an "artificial intelligence and machine-learning-enabled battle management system" as part of its project "convergence."[32]

Despite having different, but not mutually exclusive, perspectives on C2, the US Air Force contributed to the US Army multi-domain framework by merging its functional concepts into it.[33] Additionally, the US Air Force contributed to the multi-domain discourse by addressing how to synchronize operations in multiple domains, particularly in the cyber, space and air domains. In other words, the Air Force explicitly considered how to evolve from joint toward multi-domain C2.

US Air Force Emphasis on Information and Decision Advantage: JADC2

The US Air Force focused on enhancing multi-domain command and control (MDC2) in air, space and cyberspace, along three lines of effort: C2 operating concepts,

---

domain synergy" requires the "integration across domains without regard for which Service provides the capability." See also: Department of Defense, TRADOC Pamphlet 525-3-1 . . ., GL-3. The US Army defines "cross domain synergy" as "the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others - to establish superiority in some combination of domains that will provide the freedom of action required by the mission."

[31]After comparing MDO with NCW, Naval War College student Kyle Scott argued that MDO did not appreciate the scope of the C2 support requirements by documenting 28 dependencies of MDO on communication systems. Kyle D. Scott, *Joint-all Domain Operations is Missing all-Domain Command & Control* (Newport, RI: Naval War College, 2020).

[32]US Army, US Army Future Command, *Project Convergence*, last accessed 18 March 2021, https://armyfuturescommand.com/convergence/.

[33]David G. Perkins and James M. Holmes, "Multidomain Battle: Converging Concepts Toward a Joint Solution . . ., 57.

advanced technology and C2 support structures.[34] The MDC2 effort emphasized the requirement for new agile thinking, new training and new technology to enhance situational awareness, decision-making and the direction of forces across domains and missions. The US Joint Staff and Services later renamed MDC2 to JADC2 to reflect US operations' joint and combined nature.[35] JADC2 seeks to evolve from service-centric C2 toward integrating effects across domains, recognizing space and cyber as warfighting domains.

Despite criticisms on the high level of JADC2's technical ambition, the US Air Force envisions using a ubiquitous cloud network environment similar to the commercial ride-sharing service Uber, by connecting with and processing data from multiple sensors, leveraging artificial intelligence applications to identify targets, and recommending the optimal weapon for target engagement.[36] JADC2 seeks to leverage "capabilities across all domains and with mission partners to achieve operational and information advantage in both competition and conflict."[37] There remains confusion within the US defence community regarding whether JADC2 is a communication architecture, a data-sharing

---

[34]Heather Wilson, David L. Goldfein and Kaleth O. Wright, *Memorandum for all Commanders and HAF Staff, Multi-Domain Command and Control (MDC2) Implementation Plan* (Washington, DC: Secretary of the Air Force, US Air force, 2018). See also: Dave Goldstein, *Enhancing Multi-Domain Command and Control…Tying it All Together* (Washington, DC: Chief of Staff United States Air Force, not dated), https://www.af.mil/Portals/1/documents/csaf/letter3/Enhancing_Multi-domain_CommandControl.pdf

[35]Theresa Hitchens, "Joint staff Grapple With JADC2," *Breaking Defense*, 14 November 2020, https://breakingdefense.com/2019/11/osd-joint-staff-grapple-with-joint-all-domain-command/

[36]Smagh, *Joint all-Domain Command and Control (JADC2)* Congressional Research Service, 2020. JADC2 evolved from other similar US Air Force concepts such as "Combat Cloud" and "5th generation warfare." Some authors criticized JADC2's unrealistic goal of creating a "fully immersed, across-the-battlespace network." For example, see: Mark Seip, "Bad Idea: All Sensors, All Shooters, All the Time – a Joint All-Domain Command and Control System That Prioritizes Centralization," *Defense 360*, Center for Strategic and International Studies, 15 December 2020. https://defense360.csis.org/bad-idea-all-sensors-all-shooters-all-the-time-a-joint-all-domain-command-and-control-system-that-prioritizes-centralization/.

[37]Department of Defense, *USAF Role in Joint all-Domain Operations* (Washington, DC: US Air Force, 2020), 2. "Information advantage" is defined as the "application of information capabilities, including space, cyberspace, EMS, and influence, resulting in comparative advantage to support all-domain operations."

approach, a C2 concept, or a decision-making tool enabled by artificial intelligence. Recently, the US Joint Staff characterized JADC2 as the decision-making process for JADO, the emerging joint warfighting concept yet to be published by the US Joint Staff.[38]

JADC2 and JADO: Evolution from NCW?

The US Air Force defines JADO as "actions by the joint force in all domains that are integrated in[to] planning and synchronized in execution, at speed and scale needed to gain advantage and accomplish the mission."[39] JADO seeks to shift away from service-centric stovepiped planning; instead, it "consider[s] all domains from the beginning of the planning process."[40] In addition to all-domain planning, JADO aims to leverage opportunities as they arise, where commanders are empowered to dynamically leverage capabilities from any domain, regardless of service affiliation.[41] Leveraging windows of opportunity requires JADO to achieve an information and decision-making advantage or superiority.

JADO's central challenge in achieving information and decision superiority is "turning large amounts of multi-source data into actionable intelligence, enabling leaders to drive operations by observing, orienting, deciding and acting correctly based on that information."[42] Therefore, in its quest for information superiority, JADO will need a ubiquitous network with high enough bandwidth and artificial intelligence applications to

---

[38]Bryan Clark and Dan Patt, "JADC2 May be Built to Fight the Wrong War," *Breaking Defense*, last modified 14 January 2021, https://breakingdefense.com/2021/01/jadc2-may-be-built-to-fight-the-wrong-war/. At the time of writing, the JADO warfighting concept had not yet been published by the US Joint Staff.

[39]Department of Defense, *USAF Role in Joint all-Domain Operations . . .*, 2.

[40]*Ibid.,* 3.

[41]*Ibid.*

[42]*Ibid.,* 4.

process and exchange data across the battlespace. As such, JADO and JADC2 appear to be an evolution of Network Centric Warfare (NCW), which sought information superiority and better, and faster, decision-making and effects through network connectivity and information sharing. The US Department of Defense C4ISR Cooperative Research Program defined NCW as:

> an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self synchronization. NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[43]

Irrespectively of how realistic achieving information superiority is or not, the CAF will need to align its doctrine, processes and technology with the US to achieve a sufficient degree of interoperability so that forces contributed to US multi-domain coalitions remain relevant.

In summary, to adapt to the changing character of conflict, the US Services have developed multi-domain concepts primarily focused on major combat operations, which aim to leverage advanced networking technology and artificial intelligence to enhance information sharing and synergy between warfighting domains and, aspirationally, generate more combat power. Building on the doctrine of Air-Land Battle, the US Army envisions multi-domain formations operating as part of the joint force, converging effects from multiple domains to create multiple dilemmas for adversaries, as a way to offset adversaries' possible technological parity in each domain. Similarly, the US Air Force

---

[43] David S. Alberts, John Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd (Rev.) ed. (Washington, DC: National Defense University Press, 2000), 2.

seeks greater integration beyond "jointness" as part of JADC2 and JADO, and achieving information and decision-making advantages over adversaries.

UK TOP-DOWN MULTI-DOMAIN INTEGRATION

The UK Ministry of Defence recently released its *Integrated Operating Concept 2025*, which calls for a fundamental transformation to deal with the current era of ongoing sub-threshold competition and the rapidly changing character of warfare.[44] In addition to moving beyond "jointness," the central idea lies with being integrated for advantage across domains, government, levels of warfare, and allies.[45] The British concept also calls for a broader national integration involving the entire British defence industrial base, academia and civil society.[46] Like the US MDO/JADO concepts, the UK integrated operating concept underlines its quest for an information advantage relative to adversaries, improving shared awareness and decision-making.

Multi-Domain Integration Concept

The UK Ministry of Defence subsequently published *Multi-Domain Integration* to create "military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare."[47] In contrast with the US service-centric bottom-up MDO development, the UK focuses on strategic and national integration before getting into detailed operational integration and doctrine. While MDI recognizes the same threats and challenges as US JADO or MDO, MDI differs "in scale

---

[44]Ministry of Defence, *Introducing the Integrated Operating Concept* (Bristol, UK: MOD, 2020): 1.
[45]*Ibid*., 8.
[46]*Ibid*., 9.
[47]Ministry of Defence, *Joint Concept Note 1/20, . . .,* 3, 27. In comparison with John Boyd's observe, orient, decide and act loop, MDI describes its framework "sense, understand and orchestrate" as being less transactional, applicable to all levels of warfare, and more conducive to integrating non-military elements.

and geostrategic ambition."[48] MDI recognizes that increasing its number of platforms, weapons or military personnel is not realistic. Instead, the British Ministry of Defence intends to acquire and synchronize non-military and non-traditional capabilities beyond the land, air and maritime domains to achieve the best possible effects within their existing resources.[49] In that respect, MDI is more a way of thinking and action than a geographically-based doctrinal framework, aimed at coordinating allied capabilities, as well as British instruments of national power, against an adversary's vulnerabilities.

Tenets of Multi-Domain Integration

The UK MDI model comprises four tenets: "information advantage," "strategic posturing," "configuration for the environments," and "creating and exploiting synergies." The UK working definition for "information advantage" is the "credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems."[50] As part of its quest for information advantage, the UK MDI highlights the imperative to sense, understand and orchestrate effects across the spectrum of competition and conflict, coordinating across all levels of warfare, domains, allies and other non-military partners. To meet this unprecedented level of integration and information exchange requirements, the UK envisions a single information environment that fuses both military and non-military information in the form of an all-encompassing C4ISTAR architecture.[51] While both MDI and

---

[48]*Ibid*., 7.

[49]*Ibid*., 8.

[50]*Ibid*., 74. The provided definition for "information advantage" has not been endorsed yet. The UK MOD also published a separate document on "information adavantage": Ministry of Defence, *Joint Concept Note 2/18, Information Advantage* (Shrivenham, UK: Ministry of Defence, 2018).

[51]Ministry of Defence, *Joint Concept Note 1/20, . . .,* 27-31. The UK uses the acronym C4ISTAR, which adds "Target Acquisition" to the usual C4ISR concept. MDI aspires to a secure, low latency, high bandwidth and interoperable C4ISTAR system that uses artificial intelligence and machine learning to process data from multiple sensors.

JADC2/JADO seek information advantage by leveraging C4ISR networking and artificial intelligence technologies, the two concepts differ in their scope and integration level. JADC2/JADO focuses mainly at the operational level, whereas MDI focuses on the strategic and national level, including the joint, interagency, multinational and public (JIMP) enterprise.

"Strategic posturing" means the "strategic calibration and distribution of multi-domain capabilities through force management, apportionment, readiness capacity, permission and authorities."[52] In other words, the second tenet describes the need to continuously assess the balance, readiness and burden-sharing of domain capabilities between own forces, other government partners and allies. "Strategic posturing" is similar to the US MDO "calibrated force posture" tenet, however, with a higher and broader scope that includes other government agencies and allies.

The third tenet introduces the idea of "configuring" multi-domain regional or global operating areas that can span the continuum of competition, levels of warfare and strategic context. This idea contrasts with the traditional organizing of operational-level joint task forces solely operating within a joint operational area. [53] It also reflects the reality that strategic level headquarters, other government partners or allies control some

---

[52]Ministry of Defence, *Joint Concept Note 1/20, . . .,* 32. Posture includes force development policy decisions with a multi-domain mindset, taking into account that some "decisions cannot be divorced from other government departments with whom defence must be integrated."

[53]Ministry of Defence, *Joint Concept Note 1/20, . . .,* 38, 75-76. MDI defines "multi-domain configuration" as "readiness for cross-domain synergy within operating environments, through integrating and synchronizing joint functions and other allies and partners across government." MDI explains that the "strategic context, the continuum of competition" and the boundaryless emerging domains mean that "geographically bounded operating areas are less suitable." An example is the space domain, where critical infrastructure located on Earth may be located outside the JOA, but still required to be protected. In contrast with a traditional JOA, MDI introduces "multi-domain operating area" as "a higher-level battlespace; this may be global, regional or joint and is likely to contain several operating environments, linked by the aims of military and non-military activity."

of the novel domain capabilities like cyber, space, or strategic communications. Therefore, the strategic level must integrate these forces adequately with other allied and non-military capabilities for specific environments or operating areas.

The fourth tenet pertains to "cross-domain synergy," an advantage resulting from the "complementary employment of capabilities in one or more domains," exploiting windows of opportunity in the physical, information or human domains, and across the levels of warfare and instruments of national power.[54] The British definition of "cross-domain synergy" is akin to the American one, but with a broader scope that includes the strategic level and other national instruments of power. The emphasis MDI places on strategic and national integration is not new; MDI builds on the recent British national security strategy called "fusion doctrine."

British Fusion Doctrine

Drawing from lessons of the Afghanistan and Iraq wars, "fusion doctrine" aims to integrate better all British power instruments such as "security, economic and influence capabilities to protect, promote and project" British national goals.[55] This integrated approach acknowledges that many national security capabilities lie outside the government; therefore, it also seeks stronger collaboration with other public partners and private sectors.[56] The UK government fusion model has the potential to provide a more unified and responsive whole-of-government framework to deal with multi-domain and

---

[54]Ministry of Defence, *Joint Concept Note 1/20, . . .,* 42-43.

[55]Her Majesty's Government, *National Security Capability Review, Including the Second Annual Report on Implementation of the National Security Strategy and Strategic Defence and Security Review 2015* (UK: Government Cabinet Office, 2018), 10. Fusion doctrine builds on the Iraq Inquiry (Chilcot Report) and other approaches from the 2000s, e.g., comprehensive, integrated, or full spectrum approach, which all sought to improve the ways in which the different government departments worked together.

[56]*Ibid*. The UK also introduces the idea of "whole-of-nation" integration across the "total force," which includes the private sector, other national power instruments, and allies.

sub-threshold threats to their national security compared with the Canadian approach to national security that lacks integration and responsiveness.[57]

On the other hand, the "fusion doctrine" or multi-domain integration approach, which pursues integration at the highest level and relies on the fusion of large amounts of data and information, can lead to over-centralization of authorities and, therefore, indecisiveness.[58] Roberts notes that, in practice, the British "fusion doctrine" has led to exerting "control on the battlefield by committee" and subordinating command to intelligence.[59] Roberts also argued that the higher levels' quest for information advantage is ill-suited to deal with the level of uncertainty and complexity of the current security environment. The last section of this chapter will discuss the elusiveness of information superiority further.

To summarize, in line with the British national "fusion doctrine," the MDI concept envisions greater integration beyond "jointness" across warfighting domains, levels of warfare, and with allies and partners. MDI is a top-down government vision that aims to achieve a strategic advantage while operating within the British government's means. MDI also emphasizes pursuing information and decision advantage by designing an ambitious C4ISR architecture connecting all non-military and military elements, platforms, and decision-making nodes, providing a single information environment at all levels of warfare, across the government, and with allies. The MDI tenets bear a

---

[57]The lack of cross-government coordination in planning and executing national security activities is discussed in many papers, e.g, see: Navid Hassibi, "Canada Needs a Better National Security Policy," *Policy Options,* 15 March 2021, https://policyoptions.irpp.org/magazines/march-2021/canada-needs-a-better-national-security-policy/. The author describes the lack of legislation governing the role of the National Security and Intelligence Advisor and PCO as a whole in coordinating the federal government response to national security issues.

[58]Peter Roberts, "Command and Control: By Task Or Purpose?" *Whitehall Papers* 96, no. 1 (2019): 10.

[59]*Ibid*., 19-20.

resemblance to ideas inherent with the American concepts of MDO, JADC2 and JADO, however, with much more emphasis placed on the high-level JIMP integration. Both the US and UK concepts view C2, or the orchestration of capabilities and effects based on superior information, as the chief operational function that can substitute scale and capability compared with adversaries.

ALLIED MDO CONCEPTS AND PFEC: DISCUSSION AND IMPLICATIONS

The newly drafted PFEC provides conceptual alignment with allied approaches, especially with the British MDI model. PFEC recognizes the same threats and security challenges as the US and UK, and the imperative for greater integration across all warfighting domains, instruments of national power, as well as with allies and partners, to ensure effective employment of scarce CAF capabilities and resources. Like the British MDI, the draft PFEC proposes a top-down vision for change within DND/CAF, focusing on pan-government and strategic integration before developing operational or tactical multi-domain doctrine. Therefore, *if supported by the government*, the PFEC has the potential to provide advantages due to greater whole-of-government integration. However, the PFEC can present interoperability challenges between the CAF and non-military entities. As such, DND/CAF needs to properly socialize PFEC to ensure that it serves the needs and meets the vision of political and civil authorities. As Canada continues to contribute tactical land, air, and maritime forces to multinational coalitions, strategic capabilities with instantaneous and global reach in the cyber, space and information domains, which other government agencies partly or wholly control, would realistically be organized to support deployed forces mainly from Canada. Despite the potential advantages brought by greater whole-of-government integration, DND/CAF and

its partners must resist the temptation to seek an elusive strategic information advantage and espouse technology over human cognition and agility.

Strategic and Pan-Government Integration

The PFEC stresses that DND/CAF must coordinate its activities with the other instruments of national power, national security partners, and allies to counter today's complex and persistent threats and security challenges. Like the way DND/CAF has supported other government departments during domestic operations, DND/CAF could conceivably support a whole-of-government effort led by another department to counter sub-threshold threats. PFEC proposes that the CAF conduct proactive "pan-domain campaigning" to continuously align and coordinate CAF operations with other Government of Canada activities, notably in the emerging space, cyber and information domains.[60] Accordingly, PFEC envisions the CAF developing its ability to determine strategic military objectives to support national security objectives and designing and executing pan-domain campaigns with other national security partners, if necessary, and independently of alliances and coalitions. This approach contrasts with the traditional Canadian approach, where the sole contribution of tactical forces to alliances and coalitions, which managed joint campaigning in support of alliance or coalition objectives, was sufficient to meet Canada's national security objectives.

PFEC defines Canada's "global theatre" as the "operating space for military activities that span the entirety of maritime, land, air, space, cyber and information," where adversaries compete and contest at all times using all their instruments of national

[60]Department of National Defence, *Draft Pan-Domain Force Employment Concept, . . .*, 50. PFEC defines "pan-domain campaigning" as the "campaign process by which the CAF continually aligns and adapts military action with other Government of Canada and/or alliance and coalition partners' activities to ensure optimal scope, scale, sequencing, and duration of operations across all domains."

power.[61] Within the global theatre, PFEC describes various battlespaces, including "global," "regional," "targeted," "joint" or "joint special" operating areas, all of which could be standing or temporary.[62] According to the PFEC, the CAF, in close coordination with its other national security partners and agencies, would design and execute multiple campaigns in multiple interlacing battlespaces.[63] This idea resembles the UK tenet of strategic multi-domain configuration to ensure optimal integration and employment of limited national capabilities as part of regional or global campaign plans.

Like the UK, DND/CAF cannot duplicate space or cyber capabilities, which other government departments partly or wholly control. For example, CAF cyber operators are working closely with, and receive support from, the Communications Security Establishment (CSE). Similarly, Director General Space maintains a liaison detachment within the Canadian Space Agency (CSA) to coordinate the employment of shared space capabilities such as the RADARSAT constellation.[64] In addition to working with other government agencies, DND/CAF collaborates with allies, international partners and industry to deliver strategic military effects. For example, through the Combined Space Operations (CSpO) initiative, the Canadian Space Operations Centre (CanSpOC) shares information and resources with Canada's closest allies' space operations centres.[65] The

---

[61]*Ibid.*

[62]*Ibid.,* 37-40, 49. According to PFEC, there are three designated GOAs: space, cyberspace, and the information, which are assigned by the CDS to a "Designated Supported Commander" to manage as part of pan-domain campaigning.

[63]*Ibid.,* 40, 52-53. Drawing from the US joint doctrine, PFEC defines "campaign mechanisms" as "operational mechanisms to describe the broad range of supporting activities required to achieve the decisive conditions of a campaign." In addition to the common "defeat" and "stabilize" campaign mechanisms, Annex A introduces new "competition" mechanisms: strengthen, create, preserve, weaken, position, inform, and persuade.

[64]For more information on RADARSAT, see: Canadian space Agency, *RADARSAT Constellation Mission*, last modified 12 June 2020, https://www.asc-csa.gc.ca/eng/satellites/radarsat/default.asp.

[65]Royal Canadian Air Force, Space, *Partnerships,* last modified 08 October 2020, http://www.rcaf-arc.forces.gc.ca/en/space/partnerships.page#:~:text=Combined%20Space%20Operations&text=CSpO%20provides%20opportunities%20to%20enhance,optimize%20resources%20across%20participating%20nations

CanSpOC also collaborates with private companies supporting CAF operations and with other countries' civilian agencies.[66] Given the JIMP nature of the cyber and space operating domains and the limited number of CAF personnel and resources, the planning and employment of cyber, space or even information capabilities will likely remain at the national and strategic level, possibly including the operational level.

Canada's interdepartmental integration has improved since the release of Canada's first national security policy in 2004.[67] However, the Canadian government still cannot holistically integrate defence and security with other national power instruments, especially in countering sub-threshold threats from other states.[68] Having the political desire, commitment, and leadership to evolve the government's policies, strategies, structures, and processes, to better address complex and dynamic 21st-century security challenges, would be the first step. The reality is that PFEC has yet to be socialized with other government departments, agencies and political leaders. Compared with the British Ministry of Defence/Armed Forces, it will be challenging for DND/CAF to integrate with other government departments to the same extent envisaged by the British government in the face of the current threats until this process begins.

---

[66]Royal Canadian Air Force, *Royal Canadian Doctrine Note 17/01, Space Power* (Ottawa: DND Canada: Canadian Forces Aerospace Centre, 2017), 4.

[67]Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: PCO, 2004). Examples of progress include the creation of Public Safety Canada and the Government Operations Center: Public Safety Canada, *Government Operations Center (GOC)*, last modified 14 July 2016, https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/gvrnmnt-prtns-cntr-en.aspx#:~:text=The%20Government%20Operations%20Centre%20(GOC,or%20intentional)%20of%20national%20interest.

[68]Under MDO, militaries need to have the policies and authorities to conduct operations in the EMS, cyber, space and information domains during competition "under-the-threshold." Despite some progress with cyber, Canada still does have the requisite legal framework to undertake operations in the information domain outside of specific named expeditionary operations.

DND/CAF will continue to face challenges synchronizing its operations and activities with other government agencies. DND/CAF will need to continue developing relationships with other government agencies to define appropriate policy and legal frameworks to operate in this new environment, and leveraging those agencies already possessing them, such as CSE or the CSA, to support pan-domain operations. The imperative for greater whole-of-government integration means that the CAF will have to pay more attention to how it interacts and manages operations with entities outside the CAF chain of command, which may have different perspectives and priorities. DND/CAF will necessitate a C2 concept that continues to integrate DND/CAF with other government departments, agencies, and non-traditional partners without compromising operational security.

Contribution to Multi-Domain Coalitions: Integration Beyond Joint?

The Canadian government generally assigns CAF capabilities to alliance or coalition operations. With the rise of Russia and China's military power, the US remains the only allied military power capable of mounting large-scale operations against them.[69] In the event of a protracted war against Russia or China, the CAF would need to integrate to a high degree with the US because it needs most of the American enabling capabilities associated with forcibly entering and securing a theatre for major combat operations. Integrating allies with the US forces for multi-domain operations is a stated ambition in many US publications.[70] Therefore, the CAF needs to continue developing a high degree

[69]Despite recent increases in Russia and China military spending, the US remained by far the largest spender in 2019, accounting for 38 per cent of global military spending, and almost as much as the next 10 highest spenders combined. See: Nan Tian, Alexandra Kuimova, Diego Lopes Da Silva et al., *Trends in World Military Expenditure*, 2019, SIPRI Fact Sheet, Stockholm International Reace Research Institute, April 2020. https://www.sipri.org/sites/default/files/2020-04/fs_2020_04_milex_0.pdf.

[70]Jack Watling and Daniel Roper, "European Allies in US Multi-Domain Operations," *Royal United Services Institute for Defence and Security Studies*, RUSI Occasional Paper (London: October 2019): 9. For

of interoperability with the US for effective integration within any coalition C2. Before examining the C2 implications of multi-domain operations, it is essential to understand how the CAF could contribute to US-led multi-domain coalitions.

Since the end of the Second World War, Canada has maintained and contributed niche military capabilities to alliances and coalitions instead of general-purpose military forces. Canada's defence policy directs growing the Regular Force by 3500 members, notably in space, cyber, intelligence and targetting, in order to maintain "interoperability with allies and an operational advantage over potential adversaries."[71] Despite this growth, the planning and employment of novel cyber, space or information capabilities will likely remain controlled nationally, at the operational or strategic level. Indeed, the PFEC mentions that:

> tactically, this does not mean that every force element the CAF employs will have a full range of integral pandomain capabilities, but rather that they will have access to pan-domain situational understanding and both offensive and defensive pan-domain effects as required.[72]

Like the UK MDI concept, the PFEC mentions that forces provided to a coalition could request pan-domain effects through national reach-back support.[73] National strategic level forces with global reach and scope, such as cyber forces, information capabilities, or CanSpOC would support deployed forces remotely from Canada. However, Canadian tactical elements would have limited capabilities to support US multi-domain formations.

---

example, the author refers to the US Army Strategy which mentions that "the US Army will continue to train and fight with allies and partners." See: United States Army, *2019 Army Modernization Strategy: Investing in the Future* (Washington, DC: United States Army, 2019).

[71]Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa, Ont.: National Defence, 2017), 13.

[72]Department of National Defence, *Draft Pan-Domain Force Employment Concept, . . .*, 18.

[73]In general, "reach-back" is used when the resources and expertise to solve a problem are distributed into different geographical areas. Reach-back depends on the level of trust, credibility and interdependency between deployed and home personnel. Micheline Bélanger, *Command and Control Canadian Armed Forces of Tomorrow, Scoping Study Synthesis*, Scientific Report (Valcartier, Quebec: DRDC, DND, 2016)

Furthermore, integrating coalition multi-domain capabilities into Canadian elements operating at the tactical level would be limited.

For example, as part of its MDO concept, the US Army envisions integrating multi-domain capabilities at echelons higher than brigades.[74] As a medium power with limited combat forces, Canada cannot generate formations larger than brigades and does not have capabilities that could add value to US multi-domain echelons above brigade, such as long-range precision fires.[75] During major combat operations, a Canadian brigade would fight a close battle within an American divisional close area, at the range of its integral weapon systems.[76] Additionally, a Canadian brigade could not easily integrate coalition space or cyber capabilities since, under MDO, the US Army does not envision integrating multi-domain capabilities at the brigade level and below.[77] As a result, Canadian land forces operating within a US-led coalition would likely struggle to understand the multi-domain common operating picture due to a lack of shared situational awareness and understanding of higher-level effects. The requirement to share classified information with different national security caveats, and the lack of interoperability, would further exacerbate this challenge.

In contrast with the US and UK, which are developing multi-domain units and formations at the tactical level, the CAF does not envisage generating such units or

---

[74]United States Army, TRADOC *Pamphlet 525-3-8, US Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045* (Washington, DC: US Army, 2018).

[75]Watling and Roper, "European Allies in US Multi-Domain Operations . . ., 10. Long-range precision fires is the US Army top modernization priority.

[76]Department of Defense, *Field Manual 3-0 Operations* (Washington, DC: Department of the Army, 2017), 1-32. Figure 1-8 provides an example of contiguous corps, division and brigade areas of operations within which a CA brigade or unit could operate.

[77]Department of Defense, TRADOC *Pamphlet 525-3-1 . . .*, C-6. For example, the US Army Space Brigade can only provide space support elements down to divisions. See also: Department of Defense, *Field Manual 3-0 Operations* . . ., 2-21.

formations.[78] Other than the reach-back pan-domain support discussed beforehand, the CAF will likely continue to contribute traditional land, air and maritime niche capabilities to coalitions, typically integrated within each multinational component of a combined joint task force. Despite the PFEC's ambition to plan and execute some pan-domain campaigns independently from allies, the CAF does not have the resources to mount a large-scale joint task force conducting major expeditionary operations on its own. The kind of pan-domain campaigning envisaged by the PFEC would, for the most part, involve activities in the information, space or cyber domains, presumably in support of other departments or agencies. Put differently, as a medium power with limited capabilities, Canada would not be able to conduct full-spectrum pan-domain operations on its own, at least at the tactical to the operational level. Therefore, one can ask if there is value for the CAF to pursue integration beyond "jointness"?

Forces integrated from all warfighting domains into the same C2 structure instead of working stovepiped within component commands does not always bring value. Each warfighting domain is characterized by different scales and timelines, and comprises different centres of gravity and metrics for success. Also, each service has its unique knowledge base and expertise. Attempting to train and educate staff officers on multiple domains beyond "jointness" could dilute to a certain degree the depth of expertise

---

[78]Department of the Army, *Army Multi-Domain Transformation, Ready to Win in Competition and Conflict*, Chief of Staff Paper #1 Unclassified Version (Washington, DC: HQ Department of the Army, 16 March 2021), 10. https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf. The US Army is experimenting with a formation size multi-domain task force (MDTF) which includes an "intelligence, information, cyber, electronic warfare and space battalion" (I2CEWS). Similarly, the British 6 (UK) Division generates "information manoeuvre and unconventional warfare forces," which includes "intelligence, counter-intelligence, cyber, electronic warfare, information operations and unconventional warfare," for competition and warfighting, in both the virtual and physical domains. See: Ministry of Defence, The British Army, *Cutting-Edge Capabilities 6th (UK) Division*, last accessed 03 May 2021. https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/

associated with each warfighting domain.[79] In particular, given that the CAF is not resourced and does not have the requisite authorities to generate multi-domain task forces, the amount of institutional efforts required to broaden CAF officers' education and training to include the emerging warfighting domains does not appear to be much advantageous.

On the other hand, despite not contributing multi-domain task forces to alliances and coalitions, the CAF still needs to provide traditional land, air and maritime forces that interoperate sufficiently with the broader coalition, be it multi-domain or not. Effective coalition C2 requires developing multifaceted interoperability that includes more than the technical dimension. To work effectively as part of multi-domain coalitions, the CAF will need to understand allied multi-domain concepts, doctrine, and processes. More importantly, given the aspiration, or need, for closer integration with higher levels of warfare and non-military agencies, local commanders will need to understand the impacts of their local decisions on the "global enterprise" and ensure proper coordination. They will also need to understand what pan-domain effects can be requested and what information higher levels and agencies need from the tactical level. Therefore, developing multi-domain thinking and structures into the CAF would bring value for interoperability purposes, despite that the CAF would not necessarily achieve tactical gains independently by integrating beyond "jointness."

The Elusive Quest for Information Superiority

The American and British multi-domain concepts highlight their pursuit of information superiority against adversaries by leveraging an omnipresent JADC2 or

[79]Roberts, "Command and Control: By Task Or Purpose?" *Whitehall Papers . . .,* 14-15.

C4ISR architecture that connects sensors, effectors and decision-making nodes, in addition to leveraging autonomy and artificial intelligence technologies. While JADC2 focuses mainly at the tactical and operational levels, the UK has the ambition to design a C4ISTAR system of systems, common across government and allies, enabling strategic sensing, understanding, and orchestrating effects.[80] NCW was also predicated on enhancing information sharing, collaboration and shared situational awareness. It promised better quality decision-making and increased operational outputs and effectiveness. NCW even promised to "significantly reduce [the fog of war], or at the very least change the nature of the uncertainties."[81] Notwithstanding advantages provided by information technology and, potentially, artificial intelligence and automation technologies, such as increasing information distribution, collaboration and situational awareness, technology will not solve the uncertainty and friction associated with warfighting.

Several authors argued against NCW's premise that networking sensors, shooters, and decision-makers can lead to information superiority and generate more combat power. In his historical examination of how scientific and technological development affected the way Western nations have conducted warfighting, scholar Antoine Bousquet concluded that attempting to control the battlespace by applying scientific thinking and leveraging technology can lead to disastrous consequences.[82] Even

---

[80]Ministry of Defense, *Joint Concept Note 1/20, Multi-Domain Integration . . .*, 50, 68-69. Despite the UK level of C4ISTAR ambition, MDI also discusses the vulnerabilities and risks associated with complex systems, and that the envisaged C4ISTAR system will "require technical, procedural, cultural and educational leaps."

[81]Alberts, Garstka and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority . . .*, 72.

[82]Stephanie Carvin, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity, by Antoine Bousquet; and Network Centric Warfare and Coalition Operations: The New Military Operating System, by Paul T. Mitchell: Hurst/Columbia University Press, 2009, 265 Pages Routledge,*

though the character of war changes with scientific and technological advances, the nature of war as a clash of human wills endures, so does the friction and uncertainty associated with it. The recent wars in Afghanistan and Iraq provide an example where superior technology and digitization did not provide a decisive advantage against thinking and adapting enemies.

In line with this school of thought, the human aspect remains the fundamental dimension of command. In particular, commanders' cognitive abilities to deal with uncertainty and friction, focus staff on collecting information, *as well as* make good decisions based on their experience, education, training, judgement, intuition and imagination against a thinking enemy, matters more than connecting and digitizing battlefield's sensors and shooters.[83] Even though information communication technology and sensors can significantly help the commanders and staff get data on the enemy's locations and movements, technology cannot provide information on the enemy's will, mindset and intent. Also, adversaries can fool sensors with inaccurate or deceptive information.

Authors like McMaster suggested that, as "new technology reduces friction and uncertainty in some ways, friction and uncertainty reemerge in others."[84] In other words, as technology becomes more sophisticated than ever before, new sources of uncertainty emerge. The introduction of information systems in itself brings new friction and

---

2009, 170 Pages, Vol. 7 (Taylor & Francis Group, 2010), 86-88. For example, the author discusses the application of cybernetic principles during the Vietnam War, where the top-down control approach inhibited local flexibility and adaptation in the face of an unpredictable enemy.

[83]Demetrios J. Nicholson, "Seeing the Other Side of the Hill: The Art of Battle Command, Decisionmaking, Uncertainty, and the Information Superiority Complex," *Military Review* 85, no. 6 (2005): 58-61.

[84]H. R. McMaster, *Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War* (Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, 2003).

vulnerabilities. For example, the large amount of data and information available can quickly overwhelm commanders. High amounts of information add to uncertainty and friction. Commanders can delay decision-making to acquire more information in an attempt to make a risk-free decision. Similarly, too much data can hide the relevant information in the background "noise."[85] Lastly, information technology often breaks, causing friction, and is susceptible to exploitation, hacking or cyber-attacks.

The previous discussion highlighted that technology is not a panacea that will solve the security environment's complexity and uncertainty and automatically lead to the successful conduct of military or pan-domain campaigns. The pan-domain integration approach envisaged by Canada and its allies will increase complexity at all levels of warfare. The increased emphasis on inter-agency, alliance, and coalition operations in the face of sub-threshold and conventional threats means developing and maintaining multifaceted interoperability between DND/CAF, other government departments, partners, and allies will be more crucial than ever. Accordingly, DND/CAF has to adopt concepts, doctrine and processes similar to those of Canada's principal allies, and train and educate its leaders more broadly across multiple warfighting domains to enable human and social interoperability.

CONCLUSION

The draft PFEC, the UK MDI and the US MDO concepts described the security environment and threats as more complex, global, persistent and dangerous. While the US military has seen the bottom-up development of multi-domain concepts by individual services to deter and, if necessary, defeat conventional peer threats, the UK has leveraged

[85]Nicholson, "Seeing the Other Side of the Hill: The Art of Battle Command, . . . (2005).

greater integration of its military with other non-traditional and non-military capabilities, allies, partners, and across domains and levels of warfare, to gain a competitive advantage. The draft PFEC also points towards greater strategic and pan-government integration to generate effects in the emerging cyber, space and information domains, and contribute traditional land, maritime and air forces to larger multi-domain coalitions. In addition to contributing traditional forces to multi-domain coalitions, the CAF aspires to develop the ability to design and execute pan-domain campaigns to counter new threats, especially in the cyber, space and information domains, in collaboration with, or, in support of, other national security partners. DND/CAF will need to give more importance to developing interoperability internally and externally with various military and non-military entities. This requirement is especially true in the Canadian context, where other government departments hold most cyber and space authorities.

The US and UK multi-domain/joint all-domain concepts, and the draft PFEC, emphasize leveraging superior information and faster and better decision-making, aided by artificial intelligence, to gain operational advantage. Underpinning these concepts is the desire for a ubiquitous C4ISR spine, also called C4ISTAR or JADC2 network in the British and American case, respectively, to allow maximum information sharing and collaboration. As more sophisticated wireless transceivers and data links enabled Air-Land Battle in the seventies, and the introduction of information technology led to integrating components into joint task forces in the nineties, the continued advancement of technology, automation and artificial intelligence keeps changing the character of warfare. For one thing, it has the potential to enable greater synergy and integration beyond “jointness” and support decision-making. For another, it adds more complexity

and has the potential to overwhelm, disrupt and paralyze C2. The next chapter will review C2 theoretical and doctrinal concepts and discuss the various dimensions contributing to effective C2.

CHAPTER 2 – UNPACKING COMMAND AND CONTROL: DEFINITIONS, THEORIES, APPROACHES AND AGILITY

> *Far from determining the essence of command, then, communication and information processing technology merely constitutes one part of the general environment in which command operates.*
>
> - Martin van Creveld, *Command in War*, 1985

INTRODUCTION

Military practitioners often use C4ISR to refer to an assembly of information and communication technologies or a networked environment linking sensors, shooters and decision-makers. C4ISR is a broad and multidisciplinary concept that includes much more than sensors and networking technologies. At the core of C4ISR is C2, which involves planning, deciding and executing various activities to accomplish tasks and missions at different levels of warfare. To distinguish "command" from "control," some people consider "command" as an art performed by commanders and "control" as a science done by staff.[86] Others believe that cybernetics and control theory can sufficiently describe "control" and that cognitive science can describe some aspects of "command," despite never fully modelling the full range of human intangibles such as creativity or willpower.[87] In addition to cybernetics, control theory or cognitive science, the art and science of C2 encompass various social and technical disciplines such as systems engineering, complex adaptive systems, interoperability, operations research, sociology,

---

[86]David S. Alberts and Richard E. Hayes, *Power to the Edge: Command, Control in the Information Age* (Washington, DC: Office of the Assistant Secretary of Defense, Command & Control Research Program, 2004): 14.

[87]Carl H. Builder et al., *Command Concepts: A Theory Derived from the Practice of Command and Control*, MR-775-OSD (Santa Monica, Calif: RAND Corp, 1999), 135. Alberts and Hayes counter-argued that, while cybernetics and control theory were appropriate for industrial age deterministic processes, control cannot be imposed on information age complex adaptive systems: Alberts and Hayes, *Power to the Edge: Command, Control in the Information Age* . . ., 208.

management, or organizational science.[88] Before discussing how to improve C2 for pan-domain operations, it is critical to understand some of the theoretical frameworks, approaches and emerging concepts associated with C2. After reviewing the definitions and theoretical frameworks associated with "command," "control," C2, and "C2 system," the first section will suggest that human cognition and agility will remain foundational aspects of C2 despite the rapid development of artificial intelligence. The second section will examine different approaches to C2, including mission command, and discuss the importance of C2 agility for 21st-century pan-domain operations.

DEFINITIONS AND THEORETICAL FRAMEWORKS

Because command involves such diverse disciplines and practices, it has been challenging to define it adequately. Noted author Martin Van Creveld captured the diversity of practices and complexity of command in this description:

> The exercise of command in fact involves a great many things, not all of which can be clearly separated from each other. There is, in the first place, the gathering of information on the states of one's own forces – a problem that should not be underestimated – as well as on the enemy and on such external factors as the weather and terrain. The information having been gathered, means must be found to store, retrieve, filter, classify, distribute and display it. On the basis of the information thus processed, an estimate of the situation must be formed. Objectives must be laid down and alternative methods for attaining them worked out. A decision must be made. Detailed planning must be got under way. Orders must be drafted and transmitted, their arrival and proper understanding by the recipients verified. Execution must be monitored.[89]

In his description, Van Creveld primarily associates command with an executive decision-making function. As a decision-making capacity, the purpose of command is to achieve maximum operational effectiveness by synchronizing military forces and

---

[88]Guy Walker, *Command and Control: The Sociotechnical Perspective*, 1st edition (Farnham, Surrey, England; Burlington, VT: Ashgate, 2009), 172.

[89]Martin Van Creveld, *Command in War* (Cambridge, Mass: Harvard University Press, 1985), 6-7.

capabilities.[90] The commander, who holds decision-making authority and responsibility for the employment of military capabilities, plays a central role in unifying forces toward the achievement of assigned missions.

Doctrinal definitions, which emphasize commanders' authority to make decisions, appeared after World War II. Military historian and professor Allan English explained that, during the Second World War, Canadian and allied individual services opposed any form of centralization involving a single joint commander.[91] After eventually agreeing to a single joint authority to enable "unity of command," the terms "command" and "control" and the various command relationships became part of the Canadian defence lexicon.[92] In addition to being influenced by services, the adopted doctrinal definitions resulted from negotiation and compromise between NATO countries.

Command, Control and C2

NATO defines "command" as "the authority vested in an individual of the armed forces for the direction, coordination, and control of military forces."[93] The terms "C2" and "control," which came later in the 1960s, are also linked to a commander's authority.[94] The NATO standardized definition for C2 is "the authority, responsibilities and activities of military commanders in the direction and coordination of military forces

---

[90]King, *Command: The Twenty-First-Century General* (Cambridge: Cambridge University Press, 2019), 57.

[91]Allan D. English, *Command & Control of Canadian Aerospace Forces: Conceptual Foundations* (Ottawa, Canada: DND Canadian Forces Aerospace Warfare Centre, 2008), 4.

[92]*Ibid*., 5-6. Dr. Englsh explains the historical origin of operational command, operational control and tactical control. The main reason for the establishment of command relationships was cultural in that services were reluctant to having their forces under the authority of other services.

[93]North Atlantic Treaty Organization. Military Agency for Standardization, *NATO Glossary of Terms and Definitions (English and French): Glossaire OTAN Des Termes Et Définitions (Anglais Et Français)* (Brussels: NATO Standardization Agency, 2006). Canada's doctrine uses the same definition. See: Department of National Defence, CFJP 01 *Canadian Military Doctrine*, B-GJ-005-000/FP-001 (Ottawa, Canada: Canadian Forces Experimentation Centre, September 2011), GL-2.

[94]Ross Pigeau and Carol McCann, "Re-Conceptualizing Command and Control," *Canadian Military Journal* 3, no. 1 (Kingston, Canada: DND, 2002): 53. See the first footnote.

and in the implementation of orders related to the execution of operations."[95] The definition for "control" is "the authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under his command, that encompasses the responsibility for implementing orders or directives."[96] As mentioned by defence scientists Pigeau and McCann, the definitions are "circular, redundant," incomplete and unhelpful:

> The command definition makes use of the word control, the control definition uses concepts that are part of the definition of command, and the definition of C2 is merely a longer restatement of the definition of control. Add to this confusion the growing and bewildering array of C2 acronyms adopted by militaries around the world (e.g., C2I, C2IS, C4ISR, etc.), and it is no wonder that defence analyst Greg Foster has described the state of Command and Control theory as bleak, using words like "inchoate", "diffuse", "conjectural" and "seemingly random."[97]

Furthermore, Allan English pointed out that those definitions are not very applicable to "highly dynamic politico-military environment[s]" and coalition operations.[98] While military authority remains necessary during warfighting or crisis response, the C2 definitions are less relevant to those pan-domain operations envisaged by the PFEC that involve multiple non-military partners not subjected to a military commander's authority. The lack of helpful C2 definitions has led researchers like Pigeau and McCann, and Alberts and Hayes, to develop command theories that provide additional insight.

---

[95]Department of National Defence, *Canadian Military Doctrine* (Ottawa: DND, 2009).

[96]Defense Terminology Bank, *TERMIUM Plus*, Record 9, last modified 04 June 2012, https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=control&codom2nd_wet=1#resultrecs

[97]Pigeau and McCann, "Re-Conceptualizing Command and Control," . . ., 53.

[98]English, *Command & Control of Canadian Aerospace Forces* . . ., 7.

Theoretical Frameworks

Pigeau and McCann focused on the human aspect of C2. The Pigeau-McCann framework's fundamental assumption is that "only humans command" because only humans "can demonstrate the range of innovative and flexible thinking necessary to solve complicated and unexpected operational problems."[99] Pigeau and McCann define "command" as "the creative expression of human will necessary to accomplish the mission."[100] They define "control" as "structures and processes devised by command to enable it and manage risk."[101] In contrast with the NATO definition, "control" does not have to be done by the commander. Although command and control are complementary, there is an inherent tension between them. Commanders create and change control structures and processes to suit their level of risk tolerance, keeping in mind that too much control restricts freedom of action and creativity at lower levels. According to Pigeau and McCann, "command cannot be exercised without control, but control is meaningless without command," and "control should always be subordinate to command."[102] Lastly, Pigeau and McCann define C2 as "the establishment of common intent to achieve coordinated action."[103]

The entire delegation of decision-making authorities in the Pigeau-McCann framework is not realistic; commanders must strike a balance between allowing lower levels to exercise creativity on the one hand while controlling their freedom of action on the other to manage risk. Importantly, for command to be balanced and effective,

---

[99]Pigeau and McCann, "Re-Conceptualizing Command and Control," . . ., 54.
[100]*Ibid.,* 56.
[101]*Ibid.*
[102]*Ibid.,* 62.
[103]English, *Command & Control of Canadian Aerospace Forces* . . ., 14.

commanders' competency levels should match their authority and responsibility levels. While Pigeau and McCann developed their command model with military organizations in mind, Alberts and Hayes considered the broader context of coalition and inter-agency operations.

Alberts and Hayes asserted that command is not the responsibility of a single individual. Instead of linking "command" to the position and authority of a commander, the authors argued that 21st-century endeavours, involving the need to work with various military and non-military partners, require command to be more distributed and collaborative since no single individual is in charge but rather, the collective is.[104] Alberts and Hayes described "command" as establishing the initial conditions for success, developing or negotiating a shared vision or intent, and defining the mission and objectives to achieve. Besides "command," the authors conceptualized "control" as an emergent property instead of a separate parallel process imposed by higher authorities to control situations.[105] Albert and Hayes later introduced "focus" and "convergence" in place of "command" and "control" to reflect the unsuitedness of the latter terms for coalition and inter-agency operations.[106] Irrespective of terminology, Alberts and Hayes's work suggests that traditional and hierarchical approaches to C2 are not well suited for complex pan-domain operations that involve various heterogeneous actors.

---

[104]Alberts and Hayes, *Power to the Edge: Command, Control in the Information Age . . .*, 203.

[105]*Ibid.,* 205-210. Instead of "being in control," the collective or the "enterprise creates the conditions that are likely to give rise to the behaviors that are desired."

[106]David S. Alberts, *The Future of C2: Agility, Focus and Convergence* (Washington, DC: Office of the Assistant Secretary of Defense for Networks and Information Integration, 2007). Similarly, the need to evolve the C2 terminology was expressed by General McChrystal who referred to "adapt" and "collaborate," rather than "command" and "control, for complex interagency and coalition operations. According to McChrystal, "the difference between command and control on the one hand, and adapt and collaborate on the other, was the difference between success and failure" in Iraq. See: Stanley A. McChrystal et al., *Team of Teams: New Rules of Engagement for a Complex World* (New York, NY: Portfolio/Penguin, 2015).

In summary, despite the widespread use of the terms “command,” “control” and C2, there is no agreed-upon formal definition other than the NATO definitions, which, for the most part, specify the authority of commanders in directing their forces. Pigeau and McCann re-conceptualized C2, emphasizing the human dimension of command, its indissociable relation to “control” to manage risk, and the requirement to match authority and responsibility to a level commensurate with competency. Alberts and Hayes suggested that traditional C2 is not well suited for complex 21st-century coalition and interagency operations. A more collaborative approach involving information sharing and consensus-based planning might be more appropriate when no single individual is responsible but the collective.

The C2 System: Personnel, Communications, Facilities, Equipment and Procedures

Another way to gain insight into the complex topic of C2 is to consider the components of the C2 system (C2S). The C2S comprises several different variables beyond just technology and equipment, forming a complex whole. According to the US Department of Defense's original definition, the C2S consists of “personnel,” “communications,” “procedures,” and “facilities and equipment.”[107] A more recent but similar categorization of the C2S elements includes “people,” “technology,” “processes,” and “structures.”[108] In this case, “structures” can represent how the organization is structured and how authorities are distributed. This section will focus on reviewing the former categorization based on the US and NATO C2S definition.

---

[107]Joint Chiefs of Staff, *Department of Defence Dictionary of Military and Associated Terms* (Washington, DC: Joint Chiefs of Staff, 2010), 65. This definition is also consistent with NATO definition.

[108]Ministry of Defence, *Future of Command and Control, Joint Concept Note 2/17* (Swindon, Wiltshire, UK: MOD Development, Concepts and Doctrine Centre, 2017), 35. Figure 4.1 illustrates the interdepencies between people, technology, processes and structures.

"Personnel," or the human element, is the most important subset of the C2S, yet it is also the most complex. Without it, the C2S would not function. Even with the advent of artificial intelligence and automation, humans will remain "in-the-loop" or "on-the-loop" since they cannot devolve themselves from the ethical decision process to commit lethal force. Despite that recent multi-domain concepts, such as JADO, MDI or PFEC, are predicated on leveraging big data and analytics to support or automate parts of decision-making, only humans can apply judgment, based on their perceptions, intuition, experience, and other mental models, to the information and data available.

In addition to the commander and staff, "personnel" includes operators, technicians, security personnel and logisticians who operate, transport, maintain and protect the C2S and its information communications systems, facilities and equipment. In the context of pan-domain operations, "personnel" could also include any other liaison person, proxy or representatives, military or civilian partners involved with the collective endeavour, possibly with decision-making authorities beyond those vested in the military commander.

In the current information age, "communications" is the most dominant subset of the C2S, but not the most important. Without going into details, "communications" include various line-of-sight and beyond-line-of-sight means to exchange data and information. While the first half of the 20th century saw the introduction of the telegraph and wireless systems, the second half and especially the first 20 years of the 21st century saw the growth of computers and networking technology. The introduction of communication systems led to expanding C2 to command, control and communications

(C3), an acronym often used to refer to the communications subset of the C2S.[109] Communications provide a means other than face-to-face for the commander to exercise C2 of his subordinate organizations. In many cases, communication and information technology led some commanders to exercise more control over their subordinates despite the adherence of many Western militaries to mission command.

"Equipment" and "facilities" comprise all the other components that are not part of "communications" or "personnel." For example, headquarters infrastructure, furniture, vehicles, computer workstations or servers fall within that category. The introduction and evolution of computer systems led to adding another "C" to C3: command, control, communications, and computers (C4).[110] Nowadays, the line between C3 and C4, and even C4ISR, is blurrier. For example, servers could be somewhere else in the cloud, communication and sensor technologies include computers, and computers contribute to the exchange of data and information over the network. Even though artificial intelligence is not new, the exponential increase in computing power and storage capacity makes its applications more prevalent. Automated systems and non-intelligent collaborators could be considered part of this category, in addition to being part of C2 procedures.

"Procedures" govern how to conduct planning, decision-making, coordinating, and controlling forces in accomplishing assigned missions.[111] "Procedures" could take the form of standard operating procedures, rules of engagement, regulations or policies. In addition to "procedures" or processes, Pigeau and McCann describe "structures" as

---

[109]Ronald C. Bethmann, Karen A. Malloy, *Command and Control: An Introduction*, (Monterey, California: Naval Post-Graduate School, 1989), 19-21.

[110]*Ibid.,* 23.

[111]*Ibid.,* 24-25.

another mechanism to exercise control. They define "structures" as "frameworks of interrelated concepts (or physical objects) that define and classify some larger entity."[112] The headquarters staff system with numerical J-codes is an example of an organizational structure that reduces the problem space into functional areas that are more manageable.

Overall, the C2S is a complex system of people, equipment, facilities, communication technology, procedures and structures organized to support the commander and the associated C2 processes. The C2S is complex not only because it is multi-disciplinary but also because it is fundamentally imperfect; humans are imperfect by nature, and so is the technology devised by humans. Even though Western countries have often conceptualized C2 in terms of information exchange technical systems during the 20th century, 21st-century theories such as the Pigeau-McCann framework reaffirmed the human subset of the C2S as only humans can display creativity and organize themselves to solve complex problems.[113] The C2S and its technology should adapt to the commanders' needs and their associated C2 processes.

Morphology of Command: C2 Processes

C2 processes comprise three major functional areas: decision management, information management and execution management.[114] The essential element of the C2 process is decision-making, traditionally done by commanders. As part of the art of command, commanders attempt to make the best possible decisions under conditions of uncertainty and imperfect information. Information management consists of collecting,

---

[112]Pigeau and McCann, "Re-Conceptualizing Command and Control," . . ., 54.

[113]G. E. Sharpe et al., *Principles for Change in the Post-Cold War Command and Control of the Canadian Forces* (Winnipeg, MB: Canadian Forces Leadership Institute, Canadian Forces Training Materiel Production Centre, 2002), 65.

[114]Bethmann and Malloy, *Command and Control: An Introduction* . . ., 13-18.

analyzing, and managing information to support decision-making and execution management. Execution management involves the coordination and management of the execution of the mission.

In comparison with John Boyd's observe, orient, decide and act (OODA) model, decision management relates to the functions "orient" and "decide," execution management relates to "act," and information management supports all OODA functions. The collection, management and analysis of data and information play an essential role in supporting C2. The acronym intelligence, surveillance and reconnaissance (ISR) is regularly added to C4, leading to the common C4ISR acronym and other expansions such as C5ISR and C6ISR.[115] The common use of C4ISR underlines the indissociable nature of C2 and its inputs from the "sense" operational function.

Building upon Martin Van Creveld and other scholars' work, sociologist Anthony King proposed that the morphology of command comprises three intimately related functions: mission definition, mission management and mission motivation. To King, mission definition, or defining the mission statement and the commander's intent, is the ultimate function for which the commander is responsible. Command also includes two other essential executive functions: managing the mission and its designated tasks, and motivating and providing leadership to subordinates.[116] Both Van Creveld and King affirmed that, even though the human nature of command endures, the morphology of how the three command functions are practiced changes with time. In particular, King

---

[115]Daniel, Brett, *C2 vs. C4ISR vs. C5ISR vs. C6ISR: What's the Difference?*, Blogs by Trenton Systems, last modified 16 December 2020, https://www.trentonsystems.com/blog/c2-c4isr-c5isr-c6isr-differences. As technology evolves, new disciplines have been added to C4ISR. C5ISR stands for "command, control, computers, communications, *cyber-defense* (C5), intelligence, surveillance, and reconnaissance (ISR)." "C6ISR adds *combat systems* to the framework."

[116]King, *Command: The Twenty-First-Century General . . .*, 69.

made a case for a distinctive command regime in the 21st century, which he called "command collective." Before examining sociological aspects of command regimes' transformation in the next chapter, the next section will discuss the impacts of technology on the C2S.

TECHNOLOGY, C2 APPROACHES AND AGILITY

Technology and the Changing Character of C2

The character of 21st-century warfare differs significantly from warfare in the 20th century, notably because of the advent of information communication technology. The introduction of advanced digital communications enabling the exchange of a large amount of information and achieving shared situational awareness between headquarters should have facilitated C2, possibly even reduced the number of staff and the size of headquarters facilities. On the contrary, there is evidence that information technology has complexified C2 and contributed to increasing headquarters and the number of staff officers and support personnel.

A recent historical analysis of formation and unit headquarters in ground manoeuvre operations demonstrates a tenfold growth in British divisional, brigade and unit headquarters from 1900 to 2019.[117] The data shows a sharp increase in headquarters size and support personnel, notably after World War II and during Western militaries' digitization efforts of the early 2000s. Reasons for the growth of the C2S discussed in the study include increased areas of responsibility, increased complexity and diversity of units, capabilities and weapon systems, and increased blending of civil and military

[117]Paul R. Syms, Catherall John and Andrew Rawson, *Historical Analysis of Formation and Unit HQs in Ground Manoeuvre Operations* (Potsdown West, UK: Dstl Defence and Security Analysis Division, 2019), ii.

activities. Additionally, the introduction of information technology generated a requirement for additional technical support personnel to manage systems. The growth of digitized headquarters with its support system presents new vulnerabilities in the face of conventional threats due to decreased mobility and more significant electromagnetic emissions.

Another explanation for the growth of headquarters pertains to the theory of control from cybernetics. According to Ashby's law, the control system's size corresponds to the logarithm of the system's variability required to control.[118] For example, if a system's level of complexity doubles, the size of its control subsystem will also increase, although by an amount less than doubling. As more people are added to headquarters to solve complex problems, there is a point where too many staff lowers productivity and timeliness because more time and effort are required for internal management rather than producing helpful staff work.[119]

Additionally, the report describes how staff officers have become the servants of information technology, to some extent."[120] Similarly to civilian workplaces, staff officers have become consumed by emails and managing digital "information overload" instead of being attuned to other real-world situations, thinking or planning. Overall, the report concludes that information technology's benefits over the last century have proven elusive, slowing down C2 processes, encouraging micromanagement, and increasing headquarters' vulnerability.

---

[118]W. R. Ashby, "Requisite Variety and its Implications for the Control of Complex Systems," *Cybernetica* 1, no. 2 (1958): 83-99.

[119]Syms, John and Rawson, *Historical Analysis of Formation and Unit HQs . . .,* 65. The report refers to Brook's law.

[120]*Ibid.,* 45.

Like the previous study, Anthony King suggested that new communications technology has exacerbated rather than obviated the problem of C2.[121] First, information technology, including the internet, has increased the amount of information fed into headquarters. The omnipresence of military information that now blends with civil, political or cultural information can overwhelm commanders. Second, whereas commanders used to circulate daily on the battlefield to communicate face-to-face with subordinate commanders, new beyond-line-of-sight communication means have permitted the dispersion of forces over larger operations areas. In turn, more staff need to coordinate and control operations from a distance in addition to managing information entering from various means. Third, the greater interconnectivity between platforms in the land, sea and air domains has enabled more complex coordination and synchronization of effects at the joint level. The increased integration between warfighting domains has complexified military operations, placing an additional coordination burden on commanders and staff.

In response to the increased scope and complexity of 21st-century operations, theories developed by the US Command and Control Research Program, such as NCW, promised more effective operational outputs due to greater decentralization, information sharing and collaboration enabled by digital networks. Instead, in many instances, more connectivity led to more centralization, micro-management and slower decision-making. Similarly, the multi-domain operations concepts presented in the previous chapter, which promise greater collaboration, synergy and operational outputs using advanced networking technologies and artificial intelligence, have the potential to achieve

[121]King, *Command: The Twenty-First-Century General . . .*, 291.

outcomes that are opposite to what multi-domain concepts promise. Despite artificial intelligence's promises in facilitating decision-making, it could lead to more micro-management while attempting to achieve the perfect information. Just like digitization was supposed to automate manual tasks using computers and reduce headquarters' size, it increased their footprint and staffing. Any technology has flaws and errors, given that imperfect humans design it. The more complex technological systems become, the more vulnerable to technical and human errors it becomes. Additionally, the increased complexity of automation, artificial intelligence, and ubiquitous connectivity might require more humans to make sense of the information generated or validate it because of a lack of trust in non-human intelligent entities. One should remain skeptical with any promise that technology by itself would allow commanders to reduce the fog of war and uncertainty.

To Martin van Creveld, successful commanders can function effectively without complete information and get the most out of their C2S, minimizing the constraints imposed by technology:

> Far from determining the essence of command, then, communications and information processing technology merely constitute one part of the general environment in which command operates. To allow that part to dictate the structure and functioning of command systems, as is sometimes done, is not merely to become the slave of technology but also to lose sight of what command is all about. Furthermore, since any technology is by definition subject to limitations, historical advances in command have often resulted less from any technological superiority that one side had over the other than from the ability to recognize those limitations and to discover ways—improvements in training, doctrine, and organization—of going around them. Instead of confining one's actions to what available technology can do, the point of the exercise is to discover what it cannot do and then proceed to do it nonetheless.[122]

[122]Builder et al., *Command Concepts: A Theory Derived from the Practice of Command and Control*. . ., 17-18. The original quote is from: Van Creveld, *Command in War* . . ., 275.

Even with significant technological investment, it is likely that any C4ISR or JADC2 system of systems developed by the US and allies will consist of a combination of legacy and newer technology, which will never provide perfect connectivity and interoperability. Technological optimism and wishful thinking have never delivered on expectations during warfighting, in part because technology often fails when exposed to the frictions of the operational environment and a thinking adversary. Militaries that can adapt and improvise, making some aspects of digital technology work while finding workarounds for other aspects, will likely be the ones being successful.[123]

Despite the elusive advantages of digital communications, militaries' use of information technology will not change in this era where societies are becoming increasingly digital and where adversaries leverage the information domain during competition and conflict. As MDO and the PFEC dictate, the CAF will increasingly need to exchange digital information products with other government agencies and allies. The need to interoperate will continue to drive the requirement to digitize the CAF down to the tactical level. Despite the growth of technology within the C2S, the previous discussion highlighted that the human factor of command with its agility remains foundational. If humans do not understand the problems they are facing, neither will artificial intelligence.

Mission Command and Approaches to C2

Even though the terms "command" and "control" only started to appear in the military discourse since the end of the Second World War, decentralized C2 approaches such as *Auftragstaktik*, which encouraged speed, initiative and independent action by

[123]Syms, John and Rawson, *Historical Analysis of Formation and Unit HQs . . .*, 58.

local commanders, can be traced back to Frederick the Great and the Kingdom of Prussia.[124] The *Truppenfuhrung* German doctrine from the 1920s discusses mission command-type orders explicitly.[125] Inspired by German doctrines, many Western militaries have officially adopted the mission command philosophy since the 1970-80s. For example, the CAF joint doctrine, which reflects the Canadian Army approach to mission command, says:

> The CF will continue to develop and exemplify mission command leadership as the leadership philosophy of the CF. Mission command articulates the dynamic and decentralized execution of operations guided throughout by a clear articulation and understanding of the overriding commander's intent. This leadership concept demands the aggressive use of initiative at every level, a high degree of comfort in ambiguity, and a tolerance for honest failure.[126]

Despite its official adoption, the CAF rarely put mission command into practice. For one thing, there are differences in how the services practice mission command. For instance, the Royal Canadian Air Force's approach to C2 consists of centralized control and decentralized execution to ensure optimal employment and synchronization of its capabilities.[127] For another, certain situations can necessitate more central control because of a higher risk level. Therefore, two opposite kinds of C2 approaches, centralized and decentralized, deal differently with the fundamental problem of uncertainty and risk.

---

[124]Robert M. Citino, *The German Way of War*, Kansas, US: University Press of Kansas, 2005. Citino dates *Aufstragtaktik* back to the struggle between Frederick the Great and the Prussian nobility, or "Junkers." Junkers supplied the troops to Frederick's army and agreed to his command provided they could direct how their forces fulfilled those commands.

[125]*Ibid.* Citino notes that *Aufstragtaktik* basically disappeared from German C2 by 1943 given the complexity of the Eastern Front. Army *Group* commanders could not afford to permit Divisional commanders the level of freedom *Aufstragtaktik* requires.

[126]Canadian Forces Experimentation Centre, Joint Doctrine Branch, *Canadian Forces Joint Publication 01, Canadian Military Doctrine*, B-GJ-005-000/FP-001 (Ottawa: DND Canada, 2009), 4-3.

[127]English, *Command & Control of Canadian Aerospace Forces . . .*, v.

Organizations may try to minimize uncertainty and risk by implementing control processes, structures and leveraging information technology to process large amounts of information. The envisioned use of artificial intelligence applications aligns with this kind of approach, which seeks to reduce uncertainty and predict outcomes. Alternatively, decentralized organizations, which are more flexible, could be better suited to deal with uncertainty and complexity, however, at the expense of efficiency and loss of control.[128] The decentralized approach is consistent with the philosophy of mission command in the military context.

There is a range of possible C2 approaches between centralized and decentralized. For example, the NATO Research Task Group SAS-085 defines five increasingly network-enabled approaches to C2 with varying decision rights allocations, collaboration constraints and information distribution: "conflicted C2," "de-conflicted C2," "coordinated C2," "collaborative C2" and "edge C2."[129] These approaches are depicted graphically along a diagonal in the collective's "C2 approach space" in Figure 2.1.

[128]*Ibid.,* 19.

[129]NATO Science and Technology Organization, *STO Technical Report, TR-SAS-085, Command and Control (C2) Agility* (Neuilly-sur-Seine, France: NATO STO, 2014), 11. "Conflicted C2" consists of "exercising C2 only over own forces," without wide information distribution or interaction between C2 nodes. "De-conflicted C2" involves "partitioning the problem space to avoid adverse cross-organisational impacts, limited information sharing and limited interactions between C2 nodes." "Coordinated C2" involves a degree of "common intent and an agreement to link actions in plans developed by individual C2 nodes." "Collaborative C2" is "characterized by collaboratively developing a single shared plan and intent, considerable delegation of decision rights to the collective and increased shared awareness." "Edge C2" is characterized by a "networked collection of C2 nodes having easy access to information, sharing information extensively, interacting continuously and distributing decision rights broadly."

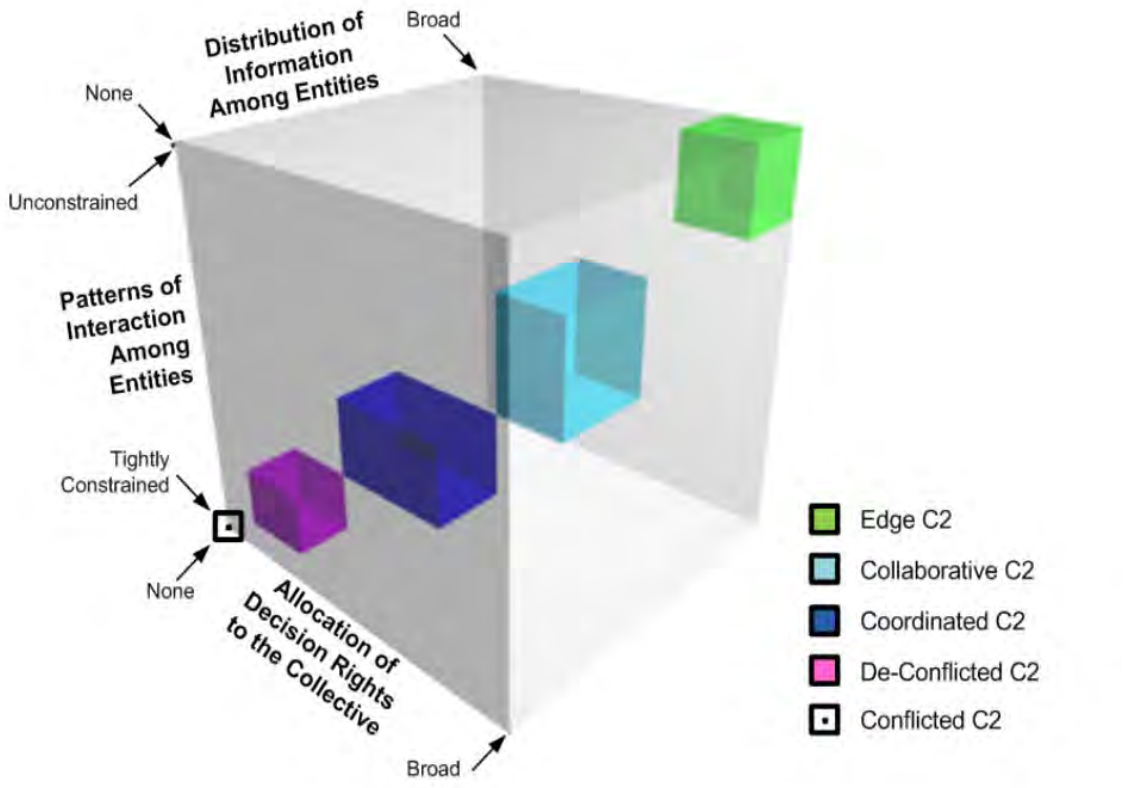

Figure 2.1 - NATO Network Enabled Capability C2 Approaches

Source: NATO STO, *TR-SAS-085, Command and Control (C2) Agility*, O-3.

"Conflicted C2" compares with traditional centralized and stove-piped military hierarchies, whereas "edge C2" consists of loosely coupled networked nodes that share information widely, collaborate extensively and distribute decision-making rights broadly. Although NCW and "power to the edge" doctrine refer to "edge C2" as the optimal approach organizations should adopt, "edge C2" is not always appropriate.[130] For example, as per the Pigeau-McCann command model, delegating decision-making authorities to actors who do not have the requisite level of competency would be risky. Also, maximizing information sharing and collaboration would not magically improve an

[130]Alberts and Hayes, *Power to the Edge: Command, Control in the Information Age . . .*, 2004.

organization's C2 effectiveness if the actors involved are not committed to a shared purpose. Therefore, there is a critical element of trust that must come with delegating decision-making authority. The level of trust an individual grants to another depends not only on competency but also on integrity and intent.[131] In other words, the individual needs to trust that the person intends to do what is right for the organization or the collective endeavour.

Nevertheless, in the context of pan-domain operations involving complex situations that cannot be controlled, or interacting with various non-military actors with their own set of authorities, then "edge C2" could be more appropriate. In the latter case, the ability to negotiate, influence, and collaborate with edge entities toward a shared purpose would be of utmost importance. The NATO C2 model acknowledges that not one C2 approach fits all situations. Instead, the model suggests that entities should "manoeuvre" in the "C2 approach space" under different missions and circumstances. This ability to transition to a more appropriate C2 approach under evolving circumstances refers to "C2 agility."

Pan-Domain Operations and the Need for C2 Agility

The previous discussion highlighted the importance of developing C2 agility as not one C2 approach is appropriate for all situations. This section discusses various situations that would warrant different approaches in the context of the PFEC. For example, there could be circumstances involving complex legal, ethical or informational dilemmas, public scrutiny or political sensitivities, leading to more centralized decision-making by the national or military-strategic level. It is also possible that other instruments

[131]Stephen M. R. Covey et al., *The Speed of Trust: The One Thing that Changes Everything*, Free Press ed. (New York: Free Press, 2018).

of power would hold decision-making authorities with DND/CAF in support; for example, Global Affairs Canada might choose to control the strategic communication narrative to de-escalate a situation during competition short of armed conflict.

Also, given the different characteristics and timelines associated with each domain, planners might need to synchronize capabilities and effects across domains to generate the synergy envisioned by pan-domain operations.[132] For example, whereas it takes months for the land component and hours to days for the air component to build up and apply combat power, the timelines associated with effects in the cyber and space domains range from seconds to days. However, in the case of cyber, it can take years to adequately plan and gain access to a target in collaboration with CSE. Synchronizing effects in multiple domains to achieve synergy might require a centralized approach similar to author Czerwinski's "command-by-plan."[133] This approach emphasizes adherence to a pre-determined plan trading flexibility for focus, like the Air Force's air tasking order process. Given that other government agencies hold most of the authorities in the space, information and cyber domains, DND/CAF will need to harmonize its planning and C2 processes, including information management and sharing, decision and execution management with those agencies involved.

In the current information age, where data and information can quickly overwhelm decision-makers, the employment of artificial intelligence, machine learning and autonomous systems has the potential to lessen the cognitive burden and support

---

[132]Mark Balboni et al., *Mission Command of Multi-Domain Operations, A US Army War College Student Integrated Research Project* (Carlisle, PA: The US Army War College Press, Strategic Studies Institute, 2020), 20.

[133]Thomas J. Czerwinski, "Command and Control at the Crossroads," *Parameters* 26, no. 3 (1996), 121. Czerwinski claimed that "command-by-plan" is useful only at the strategic and operational levels. If too much emphasis is put on adhering to the plan, this method will be unable to cope with unforeseen or rapid change.

agile decision-making.[134] Artificial intelligence and machine learning require a large amount of data to make sense out of it. Therefore, it could be tempting to adopt a centralized control or decision-making model that optimizes data input and artificial intelligence.[135] On the other hand, centralized C2 approaches can stiffen operational tempo and adaptability; therefore, they are less suited for highly complex and dynamic situations.

Despite the increased prevalence of information and artificial intelligence technologies that could support centralized C2, and the requirement to synchronize actions in time and space across all domains, the US Joint Staff reaffirmed its adherence to the tenets of mission command in the conduct of military operations, encouraging "decentralized execution based on mission-type orders."[136] Mission command requires subordinate leaders at all levels to "exercise disciplined initiative independently to accomplish the mission."[137] The 2012 US *Joint Operational Access Concept* emphasized the requirement for cross-domain synergy, including cyber and space, at increasingly lower levels than ever before "to generate the tempo necessary to exploit fleeting opportunities."[138] In the Canadian context, even though the draft PFEC does not explicitly discuss decentralizing C2 nor mention mission command as an enduring

---

[134]Sherrill Lingel et al., *Joint all-Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications* (London, UK: RAND Corporation, 2020). Leveraging artificial intelligence and data science methodologies is a fundamental element of JADC2. This report examines using artificial intelligence in support of JADC2.

[135]Bryan Clark, "JADC2 Needs to Change Course: More C2, Less Comms," *CE Think Tank Newswire,* 2020. The author examines China's centralized approach to manage the COVID-19 pandemic. The author argues against centralizing C2 through the use of networking technologies.

[136]Martin E. Dempsey, *Mission Command White Paper* (Washington, DC: Joint Chiefs of Staff, US Department of Defense, 2012). In addition to this White Paper, many US and UK multi-domain concept and doctrinal publications abide by the philosophy of mission command.

[137]*Ibid*.

[138]Department of Defense, *Joint Operational Access Concept* (Washington, DC: US Department of Defense, 2012): 16.

philosophy, it identifies the requirement for evolved, "flatter and more agile C2."[139] DND/CAF will need to retain the ability to decentralize C2 or exercise mission command when facing greater complexity, accelerated tempo or degraded communications.

Information and communication systems present vulnerabilities and risks. Given the rise of adversaries' advanced electronic warfare, cyber and space capabilities, it is likely that communications will be disrupted, degraded or denied in a contested environment. Therefore, there is a greater incentive to have the ability to decentralize decision-making authorities to the lowest level when communications are degraded or when technology fails. For this reason, despite its longtime approach of centralized control and decentralized execution, the current US Air Force JADO doctrine suggests distributing control using conditional authority matrices, enabling pre-approved delegation of authorities to lower echelons under contested and degraded conditions.[140]

DND/CAF and the broader national security enterprise could apply various approaches to C2, management or governance, depending on the context and organizational needs. Centralized and decentralized approaches could also be used simultaneously at different levels of warfare. For example, at the tactical level where the chain of command is required to manage military capabilities and where interactions with outside agencies are minimal, a centralized and directive approach could be applicable. However, at higher levels where interaction and collaboration with various non-military partners are necessary, a directive approach would be less appropriate.

---

[139]Department of National Defence, *Draft Pan-Domain Force Employment Concept . . .*, 28.

[140]Department of Defense, *USAF Role in Joint all-Domain Operations . . .*, 6. See also: David A. Deptula, "A New Era for Command and Control of Aerospace Operations," *Air & Space Power Journal* 28, no. 4 (2014), 13. In an "era of increasing threats and accelerating information velocity," Deptula suggests that the US Air Force evolves its C2 in the direction of "centralized command, distributed control, and decentralized execution" construct.

The previous discussion suggests that pan-domain operations will involve a combination of centralized and decentralized operations, depending on the situation and at different levels of warfare. More importantly, the selected C2 approach will need to harmonize with other domains, allies, government or civil agencies, and other partners. Given that DND/CAF depends heavily on cyber and space capabilities residing with other government agencies and private industries, DND/CAF will need to collaborate with civil partners in a closer fashion than ever before. As such, DND/CAF will need the agility to adopt different C2 approaches depending not only on the situation and pan-domain mission at hand but also on the entities involved. Despite that many Western militaries have officially adopted mission command and that NATO has recognized C2 agility as an essential concept for the Alliance, Western militaries rarely put decentralized C2 approaches into practice. Organizational culture, which appears to be the biggest impediment to C2 agility, will be discussed in the next chapter.

CONCLUSION

The examination of definitions, concepts and theories underlined that C2 is primarily a cognitive and organizational function and that information and communication technology, by itself, will not solve C2 challenges. Even with the development of advanced artificial intelligence applications that could support decision-making, only humans can apply judgment and intuition to understand problems and display creativity in solving them. Contrary to NCW promises, the advent of digital networks led to more prevalent micro-management and slower decision-making in many cases. Information communication technology has enabled the dispersion of forces within larger areas of operations and greater joint integration; on the other hand, it has

complexified C2 and created information overload. As commanders should remain skeptical with any promise that technology by itself would reduce the fog of war and uncertainty, over-reliance on technology as part of multi or pan-domain operations has the potential to exacerbate C2.

In the current era where societies are increasingly digital, the changing character of warfare will continue to transform how militaries execute C2 processes during competition and conflict. In the context of complex pan-domain operations involving diverse non-military actors with their own set of authorities, the ability to negotiate, influence, and collaborate with heterogeneous entities toward a shared purpose will be paramount. Pan-domain operations will involve a combination of centralized and decentralized operations, depending on the situation and at different levels of warfare. As such, DND/CAF will need the agility to adopt different C2 approaches depending not only on the situation and pan-domain mission at hand but also on the entities involved.

While nobody can predict the future, this chapter suggests that human cognition and agility rather than technology will be amongst the central determinants for successfully dealing with complex pan-domain situations. However, complete reliance on the "genius," creativity or judgement of a commander might prove to be risky as the scope and complexity of warfare continue to expand. Other critical sociological considerations such as organizational culture can either enable or impede the C2 of an organization. Despite that military culture can impede an organization from becoming more agile, the scope and complexity of warfare in the 21st century have started to transform the character of C2 into what Anthony King refers to as "collective command."

CHAPTER 3 – ADDITIONAL ORGANIZATIONAL AND SOCIOLOGICAL CONSIDERATIONS AND THE NEED FOR HUMAN INTEROPERABILITY

> *In this age, I don't care how tactically or operationally brilliant you are, if you cannot create harmony — even vicious harmony — on the battlefield based on trust across service lines, across coalition and national lines, and across civilian/military lines, you need to go home, because your leadership is obsolete. We have got to have officers who can create harmony across all those lines.*
>
> - Retired Marine General James Mattis

INTRODUCTION

This chapter reviews additional sociological and organizational considerations that can either enable or impede C2 agility and interoperability. The first section discusses that the most significant impediments to C2 agility relate to organizational culture and lack of trust, not merely technology. Despite these challenges, the new security environment has forced Western military organizations, in some cases, to delegate more authorities to highly trusted and professionalized command collectives. After reviewing the various facets of interoperability, the second section argues that pan-domain operations will require more human and social interoperability than ever before, as part of multi-domain coalitions and nationally within the whole-of-government enterprise. While sociological factors such as culture, trust, policies and politics can enable or impede interoperability, no technological solution can offset the lack of social interoperability. More importantly than any all-encompassing C4ISR network, 21st-century pan-domain operations will require developing trusting relationships and unity of efforts with various heterogeneous partners.

ORGANIZATIONAL AND SOCIOLOGICAL CONSIDERATIONS

Organizational Culture and Impediments to Agility

Despite that many Western militaries have embraced mission command and other decentralized approaches such as Alberts and Hayes' network-centric "power to the edge," C2 agility has proven challenging. Culture is a significant factor that can enable or impede organizational effectiveness or agility, as illustrated by the famous quotation "culture eats strategy for breakfast," attributed to the late business management professor and consultant Peter Drucker.[141] Organizational cultures have an enormous impact on the design, implementation and effectiveness of C2 systems. Yet, DND/CAF has often overlooked the impact of organizational culture when fielding new technologies. Authors Joe Sharpe and Allan English examined the impact of DND/CAF's organizational culture on C2 during the post-Cold War transformation period. Sharpe et al. explain that "too often in the past, change initiatives have transformed the things that could be changed – like processes and structures – while paying little attention to the so called "soft" parts of the organization, like its culture."[142] The authors further assert that:

> Most failures in C2 organizational changes can be traced to failures to modify the culture to accept the changes or by acquiring technology that is not compatible with the organization's way of doing things. An effective C2 system for the CF must recognize this uniqueness and respond to it, rather than assuming that the culture will change to accept concepts adapted from other militaries or organizations.[143]

For example, while the draft CAF *C4ISR strategic vision, goals and objectives* document underlines the importance for the CAF to transform itself into an agile and responsive

---

[141]Even though the quotation is widely attributed to Peter Drucker on the internet, no source was found to confirm the attribution.

[142]Sharpe et al., *Principles for Change in the Post-Cold War Command and Control of the Canadian Forces . . .*, 95.

[143]*Ibid*., xvi.

military force leveraging C4ISR capabilities, the document proposes 17 strategic objectives that all pertain to information communication technology.[144] Any attempt to implement an all-encompassing "C4ISR spine" to support pan-domain C2 will need to consider culture. Instead of focusing on technology, DND/CAF should consider people and culture, then work backwards to consider technology, processes and structures. DND/CAF will need to recognize the organizational culture and other sub-cultures at play, including the bureaucratic inertia that characterizes government organizations, to determine which technologies could be compatible with current or projected cultures.[145] Importantly, pan-domain operations will need a learning culture that can innovatively leverage certain aspects of technology, reject other parts, and build on human networks to interoperate better.

Another challenge to C2 agility is the discrepancy between the stated mission command philosophy and existing cultures. Despite the aspiration of Western militaries for "flatter" or "edge" approaches to C2, the notion of hierarchical chains of command not conducive to delegating authority is deeply rooted in Western military culture. As long as the culture allows micromanagement, commanders may continue to do so despite the organization's adherence to mission command. Sharpe and English characterized the Canadian and American military cultures as dysfunctional because of the prevalence of micro-management and lack of trust.[146] The military career management system, which is based on the progression of its members up the "command ladder," contributes to the

---

[144]Vice Chief of the Defence Staff, *The CAF C4ISR Strategic Vision, Goals and Objectives, Version 1.0* (Ottawa: DND Canada: Department of National Defence, 2016).

[145]Sharpe et al., *Principles for Change in the Post-Cold War . . .,* 70. The authors explain that "innovation in large organizations is usually constrained" more by culture than technology.

[146]*Ibid.,* 60.

"zero defect" and risk-averse culture.[147] Whereas mission command encourages learning from making honest mistakes, in reality, CAF leaders still see mistakes as career-damaging, even during peacetime training. On the contrary, Prussian and German armies' commanders successfully implemented mission command in the 19th and early 20th centuries because they accepted the risks inherent with exercising less control, up to a certain extent.[148]

The advent of information technology employed in relatively permissive theatres of operations has exacerbated the issue of micro-management. Once connected, higher-level commanders and their headquarters can become reluctant to relinquish control despite officially espousing mission command.[149] Information technology can contribute to a quest for ever more data, information and intelligence at the highest levels, not unlike the British MDI or fusion doctrine, which contrasts with the philosophy of mission command.[150] These approaches can encourage commanders or executives to wait for the perfect information before making decisions, which, in turn, can slow down decision-making and paralyze the organization with too much delay and analysis. In the same vein, the increased oversight and scrutiny from higher levels, combined with the pervasiveness of media reporting on tactical level operations, put additional pressure on commanders to micro-manage further.[151]

---

[147]*Ibid.*

[148]M. S. Vassiliou, David S. Alberts and Jonathan R. Agre, *C2 Re-Envisioned: The Future of the Enterprise* (Boca Raton, FL: CRC Press/Taylor & Francis Group, 2014), 246. However, the German did not always practice mission command. As mentioned before, Aufstragtaktik basically disappeared from German C2 by 1943 given the complexity of the Eastern Front. Army Group commanders could not afford to permit Divisional commanders the level of freedom Aufstragtaktik requires. See: Robert M. Citino, The German Way of War, Kansas, US: University Press of Kansas, 2005.

[149]Roberts, "Command and Control: By Task Or Purpose?" . . ., 18.

[150]*Ibid.,* 10.

[151]Vassiliou, Alberts and Agre, *C2 Re-Envisioned: The Future of the Enterprise* . . ., 122.

The previous discussion highlights that, despite the broad recognition that organizations need to adopt decentralized C2 approaches when dealing with dynamic and complex problems, such approaches are difficult to put into practice because they require a high level of trust at all levels. The existence of a network permitting the exchange of information, collaboration, and synchronization of sub-entities does not appear to be a determining factor for the successful implementation of mission command. Instead, an organizational culture, which fosters trust-building, risk-taking and the willingness to be vulnerable, is essential to mission command.

Importance of Trust

Trust plays a central role at the individual, team and organizational levels. Researchers Fulmer and Gelfan conducted a multi-level and multi-referent review of trust and identified two key dimensions that should be part of its definition:

> . . . *positive expectations of trustworthiness*, which generally refers to perceptions, beliefs, or expectations about the trustee's intention and being able to rely on the trustee, and *willingness to accept vulnerability*, which generally refers to suspension of uncertainty or an intention or a decision to take risk and to depend on the trustee.[152]

Before delegating decision-making authority to subordinates, a commander needs to be willing to accept vulnerability based on positive expectations of trustworthiness. For a commander to have positive expectations, subordinates need to demonstrate the requisite credibility, which is, according to authors Stephen Covey and Rebecca Merrill, made up of four elements: integrity, intent, capabilities and results.[153] A person of integrity is honest, congruent and interested in doing what is right for the collective,

---

[152]C. Ashley Fulmer and Michele J. Gelfand, "At what Level (and in Whom) we Trust: Trust Across Multiple Organizational Levels," *Journal of Management* 38, no. 4 (2012): 1167-1230.

[153]Covey et al., *The Speed of Trust: The One Thing that Changes Everything*, Free Press ed. (New York: Free Press, 2018).

rather than being right. Having a good intent means not trying to deceive or have hidden motives or agendas. As per the Pigeau-McCann theory, decision-making authorities should be carefully delegated only to those with the requisite level of competency or capability. Capability is about having the required knowledge, skills, and experience for the job. A person needs to earn trust by demonstrating the requisite capabilities through actions and results. Overall, trusting someone means managing risk based on perceived elements of integrity, intent, capabilities and a track record of results.

Trust applies at different levels, from individuals, teams to organizations. Although many organizations aspire to implement network-centric decentralized C2, this approach still requires high levels of trust at various levels to broadly distribute information and decision rights. Building and maintaining trust requires time and effort. People need to be adequately trained and educated to a level commensurate with the responsibility and decision-making authority delegated to them. There ought to be a culture conducive to developing trusting relationships and providing opportunities for people to demonstrate their competency. There also needs to be a common understanding of the organization's vision, goals and intent to make appropriate decisions. According to sociologist Anthony King, despite military organizations' challenges in delegating authority, the scope and complexity of 21st-century operations have forced a broader distribution of decision-making rights to highly professionalized teams that include deputies, staff, subordinates and proxies. Command in the 21st-century has evolved from being an individual effort to a collective one, at least according to the case studies examined by King.

Transformation and Emergence of Collective Command

Anthony King compares 21st-century Western command situations with those of the 20th-century, focusing on divisional command in land-based theatres such as Iraq and Afghanistan. Examining the generalship of Zinni, McChrystal, Mattis and others, King argues that a contemporary "collective command" regime has emerged in the 21st century given the increased complexity of operations, displacing the more individualistic practice of 20th-century command. King describes the emergence of "command collectives," consisting of "commanders, their deputies, subordinates and staff bound together in dense, professionalized decision-making communities," replacing the more individual and intuitive historical approach to command.[154] Instead of restricting decision-making under the sole purview of a commander, the empirical evidence gathered by King over the last 20 years of warfighting in Iraq and Afghanistan shows a distribution of operational-level decision-making to highly professionalized teams, which remain united and integrated around a common intent. He described these teams of professional decision-makers as "experts across a range of specialisms and in relation to staff procedures," empowered to make decisions in managing the mission on behalf of the commander.[155] As alluded to in the previous chapter, this period also coincides with the growth of operational-level headquarters and their associated deputies and staff, working groups, boards and structures.

King describes the emergence of a higher form of professional ethos uniting the staff despite working within dispersed and enlarged headquarters where the staff cannot

---

[154]King, *Command: The Twenty-First-Century General . . .*, 18. Anthony King's study is based on the experiences of US and UK Army and Marine divisional commanders such as Zinni, McChrystal, Petreus, Mattis and Rupert Smith.

[155]*Ibid.,* 356.

easily develop personal relationships. Without necessarily having the luxury of building strong personal relationships, the professionalization of the staff in 21st-century operational level headquarters has likely contributed to establishing the necessary level of trust for some Western general officers to distribute decision-making authority. The cases examined by King show that, following mission command, decision-makers were highly integrated and aligned toward a command intent. However, Anthony King differentiates the character of 20th-century mission command from the 21st-century approach. While "traditional mission command might be characterized as an individualistic system, giving local commanders temporary independence to make immediate tactical decisions," 21st-century mission command is highly collective; it aligns decisions across headquarters systems and command echelons.[156] The examples of 21st-century mission command studied by King involve "not the increased independence of subordinate commanders but radical interdependence."[157] Western multi-domain operations concepts also involve greater interdependence between highly specialized domain capabilities. 21st-century multi-domain endeavours will likely continue to require aligning the efforts of highly professional and expert communities toward a common intent.

"Collective command" compares to Albert and Hayes' idea that 21st-century command should be a collective endeavour enabled by network-centric processes of information sharing and collaboration. In contrast with Alberts-Hayes' view that no single commander is in charge of 21st-century endeavours, King reaffirms that there remains only one commander responsible for the mission's outcome despite the collective

[156]Anthony C. King, "Mission Command 2.0: From an Individualist to a Collectivist Model," *Parameters (Carlisle, Pa.)* 47, no. 1 (2017): 7.
[157]*Ibid.,* 19.

approach to 21st-century command. While commanders remain the only ones responsible for articulating the overall mission and intent, they have had to increasingly distribute authority in managing the mission given the scope and complexity of 21st-century operations that involve heterogeneous assets, actors and decision cycles. Highly professionalized "command boards, principal planning groups and deputies" have emerged "as an institutional response to an organizational problem" whereby the level of complexity has threatened "to overwhelm existing hierarchies and structures."[158] 21st-century collective mission command contrasts with network-centric command; it represents a human, organizational and sociological transformation, not merely a technological one.

King considered the generalship of James Mattis when commanding the 1st Marine Division during the March Up to Baghdad. General Mattis's division significantly lacked information technology.[159] Yet, using a human-centric approach, Mattis could decentralize battle management decision-making to the lowest levels while keeping his subordinates' actions aligned under a common intent.[160] General Mattis believes that war is fundamentally a human endeavour, rejecting the "net-centric warfare" notion that computers and networks "would eventually control battles' rhythm."[161] To Mattis, direct human interactions were more critical than network-centric communications. The scarcity of the 1st Marine Division's communication technology suggests that while digital

[158]King, *Command: The Twenty-First-Century General . . .*, 440.
[159]King, "Mission Command 2.0: From an Individualist to a Collectivist Model," . . ., 14.
[160]King, *Command: The Twenty-First-Century General . . .*, 262.
[161]Jim Proser, *No Better Friend, no Worse Enemy: The Life of General James Mattis,* 1st Edition (New York, NY: Broadside Books, 2018), 53.

communications may have assisted decision-making, it did not in itself transform mission command.[162]

Having one commander accountable for mission outcomes makes sense within the scope of King's analysis, which focuses on operational level command within the land domain without much consideration for the interagency and coalition aspects of operations. Mission command does not solve the need to collaborate and align the efforts of entities that do not fall within the military chain of command. Influencing and finding common interests may be the only way to align the efforts of military and non-military entities. As the PFEC will require closer inter-agency and coalition integration, more significant pressure will be put on commanders to coordinate and unify the efforts of highly professional heterogeneous actors with their own set of domain expertise and authorities.

To summarize, despite Western militaries' adherence to mission command, decentralized approaches to C2, or C2 agility in general, have proven challenging to put into practice. Organizational cultures characterized by risk aversion, "zero-defect" or careerism can impede C2 agility, especially during peacetime when higher levels of scrutiny can lead to more centralization and micro-management. Fostering the right culture could be an essential strategy to develop agility. While information communication technology can help with information sharing and collaboration, technology in itself is not sufficient to enable decentralized or edge C2. Instead, the delegation of decision-making rights requires high levels of trust between commanders and trustees.

---

[162]King, "Mission Command 2.0: From an Individualist to a Collectivist Model," . . ., 14.

Despite the challenges associated with decentralized C2, the increased complexity of the last two decades of warfighting in Afghanistan and Iraq has led, in some cases, to the emergence of a collective regime of mission command. While command remains a fundamentally human function, the sole reliance on a commander's genius and intuition is not adequate anymore in the face of complexifying operations. Instead, 21st-century operations have seen the emergence of trusted teams of professional staff, deputies and subordinates managing the mission on behalf of the commander. Nevertheless, the commander remains a focal point playing a critical role in articulating the mission, intent and unifying efforts. In the context of pan-domain operations, efforts will also need to be orchestrated and harmonized with higher strategic levels, other government agencies, and coalition partners.

PFEC AND THE NEED FOR HUMAN AND SOCIAL INTEROPERABILITY

As alluded to in the first chapter, given that pan-domain operations hinge on developing greater synergy between domains, allies, partners, and government departments, developing adequate interoperability, both internal and external to the CAF, will be foundational. Coalition operations require a high level of interoperability to exchange information, develop shared situational awareness, collaborate and synchronize effects. As Canadian units integrate with US or other coalition multi-domain formations, they will need to "plug-in" to the coalition C2 system to understand the higher level multi-domain fight. Canadian units will need to understand what higher-level effects the coalition can provide and, importantly, what information higher echelons need from the tactical level to plan and conduct MDOs.

Like the British MDI, another critical interoperability requirement for DND/CAF lies between the levels of warfare and with other government partners. As PFEC considers employing strategic capabilities owned by other government agencies and undertaking pan-domain campaigning efforts beyond the simple contribution to coalitions, synchronizing effects across different headquarters up to the strategic level will be necessary. Even as part of its contribution warfare approach, it is reasonable to expect tactical forces requesting strategic level reach-back support to generate pan-domain effects supporting national or coalition objectives, or both when they are aligned. Therefore, in addition to developing a coalition multi-domain operating picture, tactical units will also need to understand higher-level national pan-domain capabilities and effects. It will also be necessary for the national and military strategic levels to be responsive to tactical requirements and timelines.

To be ready to contribute and fight as part of a multi-domain coalition, the CAF ought to keep pace with the US military's rapid modernization and put interoperability at the forefront of its force development and thinking, primarily with the US, then with FVEY and NATO countries. Nevertheless, interoperability is a broad and complex subject that includes more dimensions than the compatibility or commonality of equipment, systems and networks.

Dimensions of Interoperability

Canadian military doctrine defines interoperability as the "ability to operate in synergy in the execution of assigned tasks."[163] In simple terms, interoperability is the

[163]Department of National Defence, *CFJP 01 Canadian Military Doctrine*, B-GJ-005-000/FP-001 (Ottawa, DND Canada: Canadian Forces Experimentation Centre, September 2011), GL-4.

ability for entities to work together. Interoperability is therefore multifaceted, complex and elusive; it requires continuous efforts to establish and maintain. In addition to the technical dimension, interoperability requires human and procedural interoperability.[164] The human and procedural interoperability dimensions comprise many areas such as concepts, doctrine, education and training, culture, readiness and authorities.[165]

When approved, PFEC will provide initial conceptual alignment with other allied militaries. However, the CAF will have to evolve many other institutional aspects, such as educating leaders on emerging warfighting domains and evolving the culture from "joint" towards "pan-domain." Pan-domain operations will require a higher level of interdependence and synergy between components and other non-military partners. Indeed, PFEC indicates that the "most immediate investment required . . . will be in areas such as planning, command and control concepts, education, and interoperability."[166] The human and procedural aspects of interoperability suggest that DND/CAF should adopt a comprehensive and institutional approach to developing interoperability. There exist other models that define the various dimensions of interoperability, including the non-technical ones.

Alberts and Hayes proposed that interoperability comprises four layers or levels: physical, information, cognitive and social.[167] First, entities need to connect to the network physically. Second, they need to be able to share information with other entities. Third, in the cognitive domain, organizations develop shared situational awareness and

---

[164]North Atlantic Treaty Organization, *AJP-01(D) Allied Joint Doctrine* (United Kingdom: NATO Standardization Agency, 2010), 3-4. NATO describes three dimensions of joint and allied interoperability: technical, procedural and human.

[165]"The Dimensions of Interoperability," *Whitehall Papers* 56, no. 1 (2003): 31.

[166]Department of National Defence, *Draft Pan-Domain Force Employment Concept, . . .,* 9.

[167]Alberts and Hayes, *Power to the Edge: Command, Control in the Information Age . . .*, 107-110.

understanding. The cognitive domain is "where perceptions, awareness, beliefs and values reside and where, as a result of sensemaking, decisions are made."[168] Fourth, entities collaborate, work with others and self-synchronize in the social domain. The social domain comprises interactions between entities. Even though the technology is necessary to provide the first level of interoperability, organizations need to evolve and harmonize their processes, structures, attitudes, and interaction patterns to achieve higher interoperability levels. Therefore, to understand what pan-domain C2 consists of, it is essential to consider how sociological factors such as culture, trust, ideology, perspectives, policies and politics could impact interoperability.

Cognitive and Social Interoperability for Inter-Agency and Coalition Operations

A comprehensive approach is required to address 21st-century security challenges. Sharing information both within the coalition and the national security enterprise will be increasingly important to develop common situational awareness. However, there are limits to the extent to which countries, militaries or government agencies are willing to trust one another and share information, thereby affecting interoperability. There are significant cultural differences between military and civil organizations. Each community has different views of the world, problems and solutions, and uses different languages. Militaries tend to see the World in a more binary or linear fashion, such as winning or losing, threats or objectives. As such, they are results-focused and decisive in their approaches.

On the other hand, government organizations tend to follow bureaucratic processes in delivering programs to the public. They see problems in a more nuanced

[168] *Ibid.,* 113.

fashion and focus on sound processes and ideas rather than quick results. Whereas the military uses terms such as C2, public and private organizations use "management" or "governance," and follow business or public administration methodologies to organize themselves and make decisions.[169] Different cultures and views can lead to skepticism toward one another; therefore, developing multi-level trusting relationships between civil and military entities is paramount.

A recent Defence Research and Development Canada report on the "C2 of CAF of tomorrow" identified the requirement to understand the JIMP context when "dealing with a diversity of actors" and to consider the "impact of different organizational objectives as well as cultural, social and organizational behaviours."[170] The report includes several recommendations for C2 agility improvements; for example, building relationships before missions, exposing CAF members to partners' organizational culture, facilitating the integration of public servants into military teams, or integrating liaison officers within the government operations centre.[171] Despite that DND and other departments can easily exchange information electronically at the unclassified level, it does not mean that collaboration, synchronization, and synergy will follow; the human element of liaison officers plays a critical role.

In addition to cultural challenges, there are other legal impediments to sharing information beyond departmental silos. Government agencies may only share a minimal amount of information. For example, despite the likemindedness of DND/CAF, the Royal

---

[169]NATO Command and Control Center of Excellence, *Webminar Review Document 2020 by NATO C2COE* (Utrecht, Netherlands: NATO C2COE, 2021) 13. Alberts differentiates between C2, "management" and "governance" as civilians working in private or public organizations do not relate to the term C2.

[170]Micheline Bélanger, *Command and Control Canadian Armed Forces of Tomorrow (C2CAF-T), Scoping Study Synthesis, . . .*, 5.

[171]*Ibid.,* 6.

Canadian Mounted Police or Canadian Security Intelligence Service as national security organizations, the misuse of shared information by another organization could expose their techniques and procedures, or compromise what they are trying to achieve. In some cases, agencies may be responsible for protecting information per the Privacy Act or other legal frameworks.[172] A similar dialectic tension between the need to share and safeguard information exists in military alliances and coalitions.

Similar to inter-agency integration, coalition interoperability cannot be reduced to the technical level only. Chiefly, compatibility of policies and concepts must be in place before integrating systems. In the context of pan-domain operations, as alluded to in the first chapter, partner nations and militaries need to have the policies and authorities to conduct operations in the electromagnetic spectrum, cyber, space and information domains during "under-the-threshold" competition, for example, in the conduct of the joint intelligence preparation of the operational environment or in undertaking defensive and offensive cyber operations.[173] Nevertheless, having similar concepts, doctrine, and policies is insufficient to permit unhindered information sharing within coalitions.

In addition to the interoperability of policies and concepts, other political aspects can impede information sharing. For example, Prime Minister Paul Martin's decision not to participate in the US ballistic missile defence in the early 2000s led to losing access to space situational awareness data for CAF members working in NORAD. Similarly, as the Canadian government delayed committing troops to Operation *Iraqi Freedom* in late

[172]Office of the Privacy Commissionner of Canada, *Summary of Privacy Laws in Canada*, last modified 31 January 2018, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

[173]Watling and Roper, "European Allies in US Multi-Domain Operations," . . ., 8, 16.

2002, the Americans gradually restricted Canada's access to coalition information.[174] Even when the government officially commits troops to a coalition, political strategy can present significant challenges to establishing trust at the operational level. Put another way, national perspectives, including any caveats to the employment of a small military contribution to a US-led coalition, directly affect trust between commanders at the operational level and, in turn, the extent to which the US will share information.[175] Canadian Forces College professor Mitchell explains that:

> . . . US commanders need to win; non-US commanders in the coalition want to make a meaningful national contribution, but they also want to minimise their casualties. Under these circumstances, can the US trust an ally or coalition partner to do what is necessary to accomplish the mission, or are these partners simply operational burden, there merely to show their national flags?[176]

Mitchell further illustrates the tension between political strategy and coalition digitization:

> At the heart of every alliance and coalition especially there is a tension between political strategy and military effectiveness. This tension is resolved only through compromises arrived at by hard negociation. The digital logic of machines cannot recognise such human arrangements.[177]

Besides Mitchell's work, a monograph from the RAND Corporation discusses how political divergence and strategic-level policy could impact operational and tactical level coalition interoperability.[178] The monograph highlights that, although coalition partners can sometimes find interoperability workarounds, such workarounds are usually

---

[174]Paul T. Mitchell, *Network Centric Warfare and Coalition Operations: The New Military Operating System*, EBSCO ebook (New York, NY: Routledge, 2009): 60.

[175]*Ibid.,* 69.

[176]*Ibid.*

[177]*Ibid.,* 72.

[178]Myron Hura, *Interoperability: A Continuing Challenge in Coalition Air Operations*, MR-1235 (Santa Monica, CA: RAND Corporation and Project Air Force, 2000), 18-19.

temporary and incomplete. No technological solution can offset an interoperability problem originating at the strategic level.

Ultimately, the ability of a contributing nation to connect with the coalition network depends on trust. Trust in an organization at the organizational level is defined as "a shared psychological state among organizational members comprising willingness to accept vulnerability based on positive expectations of an organization."[179] Even in the absence of significant political impediments, a coalition partner needs to build trust through actions to the point where the trusting nation will trade risk with the expectation of positive outcomes resulting from information sharing. Until significant trust between nations permits the digital exchange of coalition information, the information needs to be carefully safeguarded from disclosure, compromise or exploitation.

The level of ambition of JADC2/JADO and MDI C4ISTAR multi-caveated system of systems linking all coalitions' sensors, headquarters and shooters is unprecedented. The potential advantages of enabling the free passage of digital information between coalition partners and other government agencies come at a cost: it must be controlled and protected, especially in the current era of growing cyber threats. The issue of trust comes back again. Before sharing information, nations need to be convinced that the information will be adequately protected against any compromise to national and coalition security. Building reassurance and trust take time. Coalition networking is, above all, a social networking endeavour.

NATO has made significant interoperability progress since creating the International Security Alliance Forces' Afghan Mission Network (AMN) because the

[179]Fulmer and Gelfand, "At what Level (and in Whom) we Trust . . ., 1174.

Alliance realized that technical interoperability is primarily a social activity based on trust, willingness and commitment.[180] The name evolved from AMN to *Federated Mission Networking* (FMN) to reflect that FMN is a social networking activity requiring continuous collaboration. FMN provides a social framework where member nations can pre-negotiate and agree on the security arrangements and standards to comply with for future instantiation of federated mission networks. It has required many years of relationship-building for the CAF to develop and federate the Canadian Mission Network into FMN; it will continue to require ongoing social engagement, negotiation and collaboration.

Pan-Domain/Multi-Domain C2 and Harmonization

Recognizing that MDOs and the increased reliance on C4ISR and artificial intelligence technologies will change Western militaries' C2 practices, NATO STO SAS-143 is developing the *Multi-Domain C2-Harmonization* (MDC2-H) framework, as an extension of the C2 agility theory, intending to recommend how to achieve harmonization between operations in multiple domains with a variety of human and non-human partners.[181] David Alberts and NATO STO SAS-143 propose that 21st-century "complex endeavours" require the ability to conduct simultaneous and integrated operations in multiple domains grouped under the following categories: physical, virtual

[180]North Atlantic Treaty Organization, *COI Cooperation Portal, Federated Mission Networking*, last accessed 30th April 2021, https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx

[181]The NATO STO SAS-143 report was not published at the time of writing. NATO, Command and Control Center of Excellence, Operational Assessment Branch, *NATO STO SAS-143 Agile Multi-Domain C2*, accessed 01 May 2021, https://c2coe.org/wp-content/uploads/Library%20Documents/QRL/2020/QRL_C2COE%202020%20NATO%20STO%20SAS-143%20Agile%20Multi%20Domain%20C2.pdf. "Harmonization" refers to "finding an appropriate set of arrangements that govern the behaviors of the entities involved and their interactions such that operations are collectively as effective, efficient, and agile as is appropriate, given the situation." Alberts, *Operations in Multiple Domains: What's New, what's Not, . . .*, 2-3.

and social.[182] According to Alberts et al., the physical domain includes land, sea, air, and space; the virtual domain includes, but is not limited to, cyberspace and information; and the social domain includes, but is not limited to, the political, economic, and legal spheres.[183] Alberts differentiates 21st-century "complex endeavours" from past operations in four ways: "the identity of domains involved," the "set of entities participating in the enterprise," the "employment of technology," and the "rules of the game."[184] Alberts describes the prevalence of a more significant number and diverse set of interdependent entities with their C2 approach, objectives, and perceptions of situations. To Alberts, multi-domain C2 "seeks to avoid conflicts and enable synergies within, between, and among entities conducting operations in multiple domains," where nobody is in charge of the "collective."[185] Overall, Alberts' description highlights the more prevalent JIMP nature of 21st-century multi-domain operations.

As discussed in chapter two, Canadian pan-domain operations will require different C2 approaches. The selected C2 approach will need to harmonize with other allies, government or civil agencies, and other partners' approaches. Given that DND/CAF depends heavily on cyber and space capabilities residing with other government agencies and private industries, DND/CAF will need to collaborate with civil partners in a far closer fashion than ever before. Similarly, the CAF cannot compete, deter and defeat adversaries other than as part of alliances and coalitions. There will be more pressure on commanders to develop synergy with external partners by pursuing shared interests and cultivating personal relationships and trust.

---

[182]Alberts, *Operations in Multiple Domains: What's New, what's Not, . . .*, 2-3.
[183]*Ibid.,* 3.
[184]*Ibid.,* 5.
[185]*Ibid.*

Coalition or inter-agency mission partners may come from a different culture in which decision-making is highly centralized or, conversely, highly delegated. Other mission partners may not have the same degree of situational awareness, may use different communication means that cannot interoperate, or they may require increased support.[186] In particular, CAF elements may require significant support from coalition partners, likely including from the Americans, to interoperate adequately. Commanders must recognize these differences, and the possible repercussions from political divergences, as they build relationships and trust. The requirement to build trust means that commanders may increasingly have to rely on "command collectives" of staff, deputies and subordinates to control, coordinate and manage the mission, *while commanders* focus on developing relationships.

Another important implication is that individual entities, be they military or civil, may "need to adopt a C2 approach that they would not choose to employ if they were acting alone."[187] Both military and civilian organizations will have "to pay a lot more attention to the implications of working with others" than was done in the past.[188] In other words, given the possible lack of independence between domain operations, entities may need to choose a C2, management or governance approach that makes sense for the *endeavour as a whole*, not just for one domain. The selected approach of a given entity needs to consider the nature of the endeavour, domain characteristics, and entities' capabilities.[189] The NATO MDC2-H framework involves the harmonization

---

[186]Gary Luck, *Mission Command and Cross-Domain Synergy* (Suffolk VA, US: Deployable Training Division, Deputy Director Joint Staff J7, 2013), 3.

[187]Alberts, *Operations in Multiple Domains: What's New, what's Not, . . .*, 6.

[188]NATO Command and Control Center of Excellence, *Webminar Review Document 2020 . . .*, 18.

[189]Alberts, *Operations in Multiple Domains: What's New, what's Not, . . .*, 6.

arrangements governing behaviours and actions between entities. Alberts et al. depict the MDC2-H arrangements as a matrix of "C2 approach space" squares, as shown in Figure 3.1.

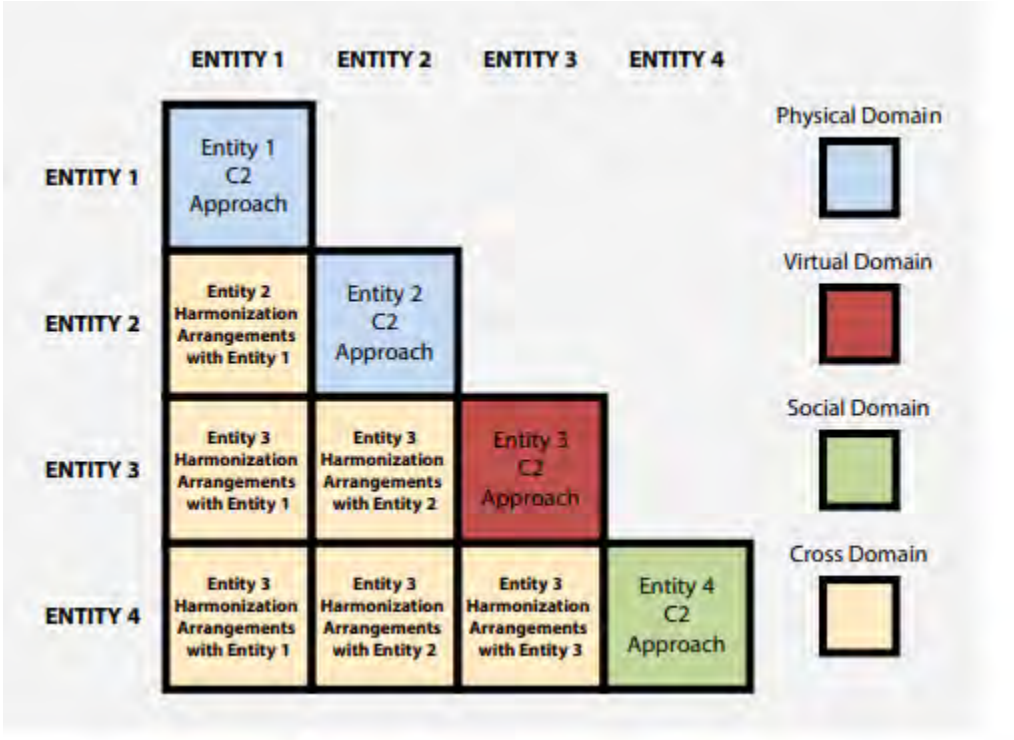

Figure 3.1 – Multi-Domain C2-Harmonization Arrangement Space.

Source: Alberts, NATO C2COE, Webminar Review Document 2020 . . .14.

The matrix diagonal in Figure 3.1 represents the C2 approach made by the individual entities. Off-diagonal squares are C2/management/governance harmonization options from which entities can choose depending on how they will work with others.

NATO STO SAS-143 characterizes the complexity of the "MDO endeavour space" using three dimensions: dynamics, interdependences and linearity.[190] According to SAS-143, the more dynamic, interdependent and non-linear MDOs become, the operation

[190]NATO Command and Control Center of Excellence, *Webminar Review Document 2020 . . .*, 14-15.

becomes more difficult to manage. The appropriateness of the harmonization arrangements will depend on those mission characteristics. Figure 3.2 illustrates the overall conceptual framework proposed by SAS-143. While Alberts's C2 agility theory asserts that more challenging missions require network-enabled C2 approaches for increased agility, SAS-143 does not make such a claim with MDOs. Indeed, Alberts and SAS-143 wrote that "although it is not certain that by their very nature MDO[s] will require network[-]centric C2 arrangements, it is likely that individual entities need to tailor the arrangements they adopt for mission partners."[191] Additionally, although SAS-143 identified the requirement to leverage autonomous and artificially intelligent systems, they carefully affirm that MDC2-H endeavours need to avoid information technologies pitfalls.[192] These assertions reinforce the idea that human interoperability is more important than technical connectivity for the successful conduct of multi-domain operations.

[191]*Ibid.,* 9.
[192]*Ibid*., 14.

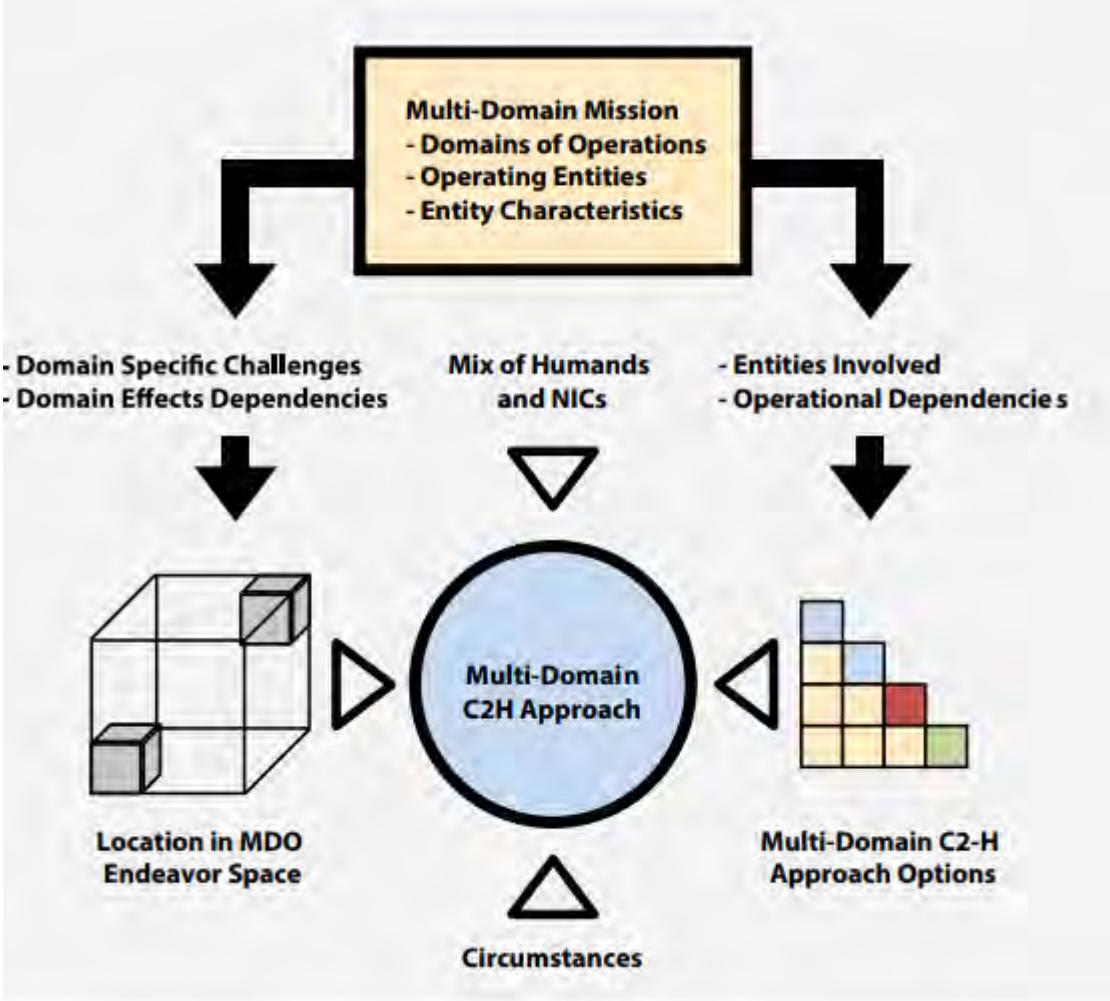

Figure 3.2: MDO / Multi-Domain C2-Harmonization Conceptual Framework.

Source: Alberts, NATO C2COE, Webminar Review Document 2020 . . .15.

In summary, 21st-century pan-domain operations will require greater human and social interoperability within MDO coalitions, across the levels of warfare, and within the whole-of-government national enterprise. Sociological factors such as culture, trust, ideology, policies and politics can either enable or impede interoperability. However, no technological solution can offset the lack of social interoperability. Therefore, sociological factors must be considered when selecting the most appropriate C2 approach and harmonizing C2 processes with other entities. Above all, developing trusting

relationships, synergies and coherence with various heterogeneous partners as part of a "collective endeavour" might become the most crucial activity of commanders.

CONCLUSION

This chapter emphasizes the preponderant role of organizational culture and trust in developing C2 agility. Fostering the right culture and levels of trust could be the most critical strategy in developing an adequate "C4ISR spine" for pan-domain operations. While information communication technology can help with information sharing and collaboration, technology does not build trust. Whereas 20th-century operations relied on the cognitive abilities of individual military commanders, 21st-century command has involved greater interdependence of highly professional teams managing complex missions.

In addition to collaborating with civil partners in a closer fashion than ever before, DND/CAF will need the agility to harmonize their C2 approaches with higher strategic levels, other government agencies, and coalition partners. As the nature of 21st-century mission involves more specialized domain capabilities, command will increasingly require aligning and harmonizing the efforts of professional and expert communities, both inside and outside DND/CAF, as part of "collective endeavours" where no single individual is really in charge. The C4ISR network envisaged by PFEC, JADC2/JADO and MDI should primarily be considered a social network.

CONCLUSION AND RECOMMENDATIONS FOR FUTURE WORK

The return of great power competition and the proliferation of connectivity, computer processing power, automatization and artificial intelligence are changing the character of conflict. For one thing, adversaries leverage information and the emerging space and cyber domains to continuously compete under the threshold of armed conflicts while, at the same time, modernizing their conventional capabilities. For another, Western-allied militaries are rapidly evolving their warfighting concepts from "jointness" toward "multi-domain," intending to leverage a ubiquitous and multi-caveated "C4ISR spine" connecting all sensors, shooters, headquarters, allies, and national inter-agency entities. In essence, western multi-domain integration endeavours, including the aspirational Canadian pan-domain concept, constitute an evolution from network-centric warfare, which sought information and decision superiority through broader digital connectivity and information sharing.

Notwithstanding the requirement to leverage information technology where it makes sense to enable the passage of data and information between services, departments and coalition partners, one must remain aware of the potential pitfalls of favouring technology over human agility and social interoperability. Rather than solely relying on technical solutions, it is crucial to understand other intangible organizational and sociological factors that can either enable or impede any C4ISR system, especially within a future marked by inter-agency and coalition pan-domain operations. This paper reviews the American and British multi-domain concepts, the draft Canadian pan-domain concept, C2 definitions, theories, including network-centric warfare, and compares centralized versus decentralized approaches to C2. It then examines how organizational

culture and trust can affect C2 agility and reviews the dimensions of interoperability. This paper argues that DND/CAF should view C4ISR as an evolving socio-technical network that will require relationship and trust-building with various heterogeneous partners, social interoperability before technical compatibility, and the honest intent to embrace human and organizational agility, including the practice of mission command when necessary.

Similarly to the UK, PFEC envisions greater domain, inter-agency and coalition integration. Since Canada cannot realistically conduct full-spectrum pan-domain operations on its own, Canada will continue to contribute land, air, and maritime forces to multinational coalitions while being supported with national cyber, space and information capabilities, partly or wholly controlled by other government agencies. Tactical commanders will need to develop multidimensional interoperability beyond technical for effective coalition C2, as well as closer integration with strategic level headquarters and other non-military agencies.

As Canada's principal allies are striving for information and decision superiority in a manner reminiscent of the network-centric warfare doctrine, the first chapter shows that technology, including artificial intelligence, is not a panacea that will lift the fog of war and generate more combat power. While technology can sometimes enable greater integration and support decision-making, it also has the potential to overwhelm, disrupt and paralyze C2.

The second chapter discusses how digital communications have changed the character of warfare by increasing the amount of information and the size of headquarters and staff, dispersing forces over larger areas of operation, and complexifying the

coordination and synchronization of effects. In addition to placing an additional coordination burden on commanders, more connectivity led to more centralization, micro-management, and slower decision-making in many instances. Similarly, the processing of a large quantity of information that could be equally altered or deceived by adversaries, as well as the increased complexity of artificial intelligence and ubiquitous connectivity, have the potential to achieve opposite outcomes than what allied multi-domain concepts promise.

Despite the greater scope and complexity of 21st-century pan-domain operations, over-reliance on technology, including artificial intelligence, could exacerbate C2 rather than enable it. Chapter two argues that human cognition and organizational agility, including the flexibility and creativity to overcome complex situations, and leveraging some aspects of information technology where it enables, will remain foundational to effective C2. DND/CAF will need to develop the agility to adopt different C2 approaches from centralized to decentralized, including mission command, depending on the situation and entities involved.

Notwithstanding the importance of individual commanders' agility and creativity, the increased scope and complexity of 21st-century warfare has changed the character of C2, forcing Western militaries, in some cases, to delegate more authorities to highly trusted and professionalized command collectives consisting of deputies, staff and subordinates. Western multi-domain operations concepts, which also involve greater interdependence between highly specialized capabilities, will likely require aligning the efforts of expert communities toward a common intent.

Other critical sociological considerations such as organizational culture and trust can either enable or impede C2 agility and interoperability. While information communication technology can enable information sharing and collaboration, technology in itself is not sufficient to enable decentralized or edge C2, contrary to what network-centric warfare promised. Instead, the third chapter argues that fostering the right culture and building multi-level trust will be necessary to support pan-domain operations and reap the benefits of an all-encompassing "C4ISR spine."

While sociological factors such as culture, trust, policies and politics can enable or impede interoperability, no technological solution can offset the lack of social interoperability. More importantly than any all-encompassing C4ISR network, 21st-century pan-domain operations will require developing trusting relationships with various interdependent and heterogeneous partners as part of multi-domain coalitions, and whole-of-government endeavours, for which no single individual is in charge. The need to work with other interdependent entities means that commanders will have to harmonize their approach or processes to support the collective endeavour.

In addition to procuring technologies, other important institutional implications could warrant future examination. Any attempt to optimize DND/CAF's C4ISR system for pan-domain operations should consider the various human, organizational, sociological and political aspects underlined in this paper; for example, recruitment, education and training of CAF personnel, civil-military relationships, operational research and experimentation, or governance. Given that any C2 system is a complex socio-technical enterprise involving people, processes, technology, and structures, DND/CAF should treat C2 as a pan-government capability necessitating continuous

governance and holistic optimization using methodologies such as PRICIE+G.[193] This directed research project could provide a basis for future PRICIE+G analysis of CAF pan-domain C2.

[193]PRICIE (+G) is a Canadian capability development framework that includes the following factors: Personnel, including leadership and individual training; Research; Infrastructure and organization; Concepts, doctrine and collective training; Information; Equipment (and Generate). See: Government of Canada, "TERMIUM Plus," Record 1, last modified 25 September 2006, https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&index=frr&srchtxt=PRICIE

BIBLIOGRAPHY

"The Dimensions of Interoperability." *Whitehall Papers* 56, no. 1 (2003): 29-33.

Alberts, David S. *Operations in Multiple Domains: What's New, what's Not, and the Implications for Command and Control*. NATO C2COE Seminar 2020 Multi-Domain Operations, Seminar Read Ahead. Utrecht, The Netherlands: NATO Command and Control Centre of Excellence, 2020.

Alberts, David S., John Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2nd (Rev.) ed. Washington, DC: National Defense University Press, 2000.

——. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2nd (Rev.) ed. Washington, DC: National Defense University Press, 2000.

——. *The Future of C2: Agility, Focus and Convergence*. Washington, DC: Office of the Assistant Secretary of Defense for Networks and Information Integration, 2007.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command, Control in the Information Age*. CCRP Publication Series. Washington, DC: Office of the Assistant Secretary of Defense, Command & Control Research Program (CCRP), 2004.

Ashby, W. R. "Requisite Variety and its Implications for the Control of Complex Systems." *Cybernetica* 1, no. 2 (1958): 83-99.

Balboni, Mark, John Bonin, Robert Mundell, Doug Orsi, Craig Bondra, Antwan Dunmyer, Lafran Marks, and Daniel Miller. *Mission Command of Multi-Domain Operations, A US Army War College Student Integrated Research Project*. Carlisle, PA: The US Army War College Press, Strategic Studies Institute, 2020.

Bélanger, Micheline. *Command and Control Canadian Armed Forces of Tomorrow (C2CAF-T), Scoping Study Synthesis, Scientific Report, DRDC-RDDC-2016-R144*. Valcartier Research Centre, Quebec: Canada, Defence Research and Development Canada, Department of National Defence, 2016.

Bethmann, Ronald C., and Karen A. Malloy. *Command and Control: An Introduction*. Monterey, California: Naval Postgraduate School, 1989.

Builder, Carl H., Steven C. Bankes, and Richard Nordin, *Command Concepts: A Theory Derived from the Practice of Command and Control*. MR-775-OSD. Santa Monica, California: RAND Corporation, Department of Defense, Office of the Secretary of Defense, and National Defense Research Institute, 1999.

Burr, Lieutenant-General Rick. "Army in Motion, Accelerated Warfare Statement." The Australian Army, 22 October 2020. https://www.army.gov.au/our-work/army-motion/accelerated-warfare

Canada. Canadian Space Agency. "RADARSAT Constellation Mission." Last modified 12 June 2020. https://www.asc-csa.gc.ca/eng/satellites/radarsat/default.asp

———. Department of National Defence. Canadian Forces Experimentation Centre, Joint Doctrine Branch. *B-GJ-005-000/FP-001, Canadian Forces Joint Publication 01, Canadian Military Doctrine*. Ottawa: DND Canada, 2009, 2011.

———. Department of National Defence. *CFJP 01 Canadian Military Doctrine, B-GJ-005-000/FP-001* Ottawa: DND Canada, 2009.

———. Department of National Defence. *Draft Pan-Domain Force Employment Concept, Prevailing in an Uncertain World*. Ottawa: DND Canada, 2020.

———. Department of National Defence. Royal Canadian Air Force, Space. "Partnerships." Last modified 08 October 2020. http://www.rcaf-arc.forces.gc.ca/en/space/partnerships.page#:~:text=Combined%20Space%20Operations&text=CSpO%20provides%20opportunities%20to%20enhance,optimize%20resources%20across%20participating%20nations

———. Department of National Defence. *Royal Canadian Doctrine Note 17/01, Space Power*. Ottawa: DND Canada, Canadian Forces Aerospace Centre. 2017.

———. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy*. Ottawa: DND Canada, 2017.

———. Department of National Defence. Vice Chief of the Defence Staff. *The CAF C4ISR Strategic Vision, Goals and Objectives, Version 1.0*. Ottawa: DND Canada, 2016.

———. Department of National Defence. Vice Chief of the Defence Staff. *VCD2020-0015391 VCDS/DMA Planning Guidance Data and Digitization*. 2020.

———. Government of Canada. Defense Terminology Bank. "TERMIUM Plus." Record 9. Last modified 04 June 2012. https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=control&codom2nd_wet=1#resultrecs

———. Government of Canada. "TERMIUM Plus." Record 1. Last modified 25 September 2006. https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&index=frr&srchtxt=PRICIE

———. Office of the Privacy Commissioner of Canada. "Summary of Privacy Laws in Canada." Last Modified 31 January 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

——. Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. Ottawa: Privy Council Office, 2004.

——. Public Safety Canada. "Government Operations Center." Last modified 14 July 2016. https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/gvrnmnt-prtns-cntr-en.aspx

Carvin, Stephanie. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity, by Antoine Bousquet; and Network Centric Warfare and Coalition Operations: The New Military Operating System, by Paul T. Mitchell: Hurst/Columbia University Press, 2009, 265 Pages Routledge, 2009, 170 Pages*. Vol. 7 Taylor & Francis Group. 2010.

Center for Strategic & International Studies (CSIS). "Competing in the Grey Zone." Last accessed 19 March 2021. https://www.csis.org/features/competing-gray-zone.

Citino, Robert M. *The German Way of War*. Kansas, US: University Press of Kansas, 2005.

Clark, Bryan. "JADC2 Needs to Change Course: More C2, Less Comms." *CE Think Tank Newswire*. 2020.

Clark, Bryan, and Dan Patt. "JADC2 May be Built to Fight the Wrong War." *Breaking Defense*. Last modified 14 January 2021. https://breakingdefense.com/2021/01/jadc2-may-be-built-to-fight-the-wrong-war/.

Covey, Stephen M. R., and Rebecca R. Merrill. *The Speed of Trust: The One Thing that Changes Everything*. Free Press Edition. New York: Free Press, OverDrive ebook, 2018.

Czerwinski, Thomas J. "Command and Control at the Crossroads." *Parameters* (Carlisle, Pa.) 26, no. 3 (1996)

Dempsey, Martin E. *Mission Command White Paper*. Washington, DC: Joint Chiefs of Staff, US Department of Defense, 2012.

Deptula, David A. "A New Era for Command and Control of Aerospace Operations," *Air & Space Power Journal* 28, no. 4 (2014): 5-16

English, Allan D., *Command & Control of Canadian Aerospace Forces: Conceptual Foundations*. Department of National Defence, Canadian Forces Aerospace Warfare Centre, 2008.

Fox, Amos C. *Hybrid Warfare: The 21st Century Russian Way of Warfare*. Fort Leavenworth, Kansas: School of Advanced Military Studies, United States Army Command and General Staff College, 2017.

Fulmer, C. Ashley and Michele J. Gelfand. "At what Level (and in Whom) we Trust: Trust Across Multiple Organizational Levels." *Journal of Management* 38, no. 4 (2012): 1167-1230.

Gerasimov, General Valery. "The Value of Science in Prediction." *Military-Industrial Kurier*, 27 February 2013.

Goldstein, Dave. *Enhancing Multi-Domain Command and Control…Tying it All Together*. Washington, DC: Chief of Staff United States Air Force. https://www.af.mil/Portals/1/documents/csaf/letter3/Enhancing_Multi-domain_CommandControl.pdf

Greenert, Jonathan. "Navy Perspective on Joint Force Interdependence." *Joint Force Quarterly*. National Defense University Press 76, 1st Quarter, January 2015. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-76/Article/577581/navy-perspective-on-joint-force-interdependence/

Hassibi, Navid. "Canada Needs a Better National Security Policy," *Policy Options* 15 March 2021. https://policyoptions.irpp.org/magazines/march-2021/canada-needs-a-better-national-security-policy/.

Hura, Myron, *Interoperability: A Continuing Challenge in Coalition Air Operations*. MR-1235. Santa Monica, CA: RAND Corporation and Project Air Force, 2000.

Karber, Philip A. *Lessons Learned from the Russo-Ukrainian War, Personal Observations*. John Hopkins Applied Physics Lab & US Army Capabilities Center (ARCIC), 8 July 2015.

Kelly, Terrence K., David C. Gompert, Duncan Long, *Smarter Power, Stronger Partners, Volume 1: Exploiting U.S. Advantages to Prevent Aggression*. Santa Monica, United States: RAND Arroyo Center, 2016.

King, Anthony. *Command: The Twenty-First-Century General*. Cambridge: Cambridge University Press, 2019.

——. "Mission Command 2.0: From an Individualist to a Collectivist Model." *Parameters (Carlisle, Pa.)* 47, no. 1 (2017)

Lingel, Sherrill, Jeff Hagen, Eric Hastings, Mary Lee Matthew Sargent, Matthew Walsh, Li Ang Zhang, and David Blancett. *Joint all-Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications*. London, UK: RAND Corporation, 2020.

Luck, Gary. *Mission Command and Cross-Domain Synergy*. Suffolk VA, US: Deployable Training Division, Deputy Director Joint Staff J7, 2013.

McChrystal, Stanley A., Tantum Collins, David Silverman, Chris Fussell, *Team of Teams: New Rules of Engagement for a Complex World*. New York, NY: Portfolio/Penguin, OverDrive ebook, 2015.

McMaster, H. R. *Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War*. Carlisle Barracks, Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, 2003.

Mitchell, Paul T. *Network Centric Warfare and Coalition Operations: The New Military Operating System*. New York, NY: Routledge, 2009.

NATO. *AJP-01(D) Allied Joint Doctrine.* United Kingdom: NATO Standardization Agency, 2010.

——. *AJP-03/05 Allied Joint Doctrine.* United Kingdom: NATO Standardization Agency, 2019.

——. "COI Cooperation Portal, Federated Mission Networking," Last accessed 30th April 2021. https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx

——. Command and Control Center of Excellence, Operational Assessment Branch, *NATO STO SAS-143 Agile Multi-Domain C2*, Accessed 01 May 2021. https://c2coe.org/wp-content/uploads/Library%20Documents/QRL/2020/QRL_C2COE%202020%20NATO%20STO%20SAS-143%20Agile%20Multi%20Domain%20C2.pdf

——. Command and Control Center of Excellence. *Webminar Review Document 2020 by NATO C2COE*. 2020 Webminar: Multi-Domain Operations: Keys to Master Complexity. Utrecht, Netherlands: NATO C2COE, 2021.

——. Military Agency for Standardization. *NATO Glossary of Terms and Definitions (English and French): Glossaire OTAN Des Termes Et Définitions (Anglais Et Français)*. Brussels: NATO Standardization Agency, 2006.

——. Science and Technology Organization. *STO Technical Report, TR-SAS-085, Command and Control (C2) Agility* Neuilly-sur-Seine, France: North Atlantic Treaty Organization, Science and Technology Organization, 2014.

Nicholson, Demetrios J. "Seeing the Other Side of the Hill: The Art of Battle Command, Decisionmaking, Uncertainty, and the Information Superiority Complex." *Military Review* 85, no. 6 (2005)

Paparone, Christopher R. "What is Joint Interdependence Anyway?" *Military Review*. Fort Leavenworth, KS, US: US Army Combined Arms Center, August 2004.

Perkins, David G. and James M. Holmes. "Multidomain Battle: Converging Concepts Toward a Joint Solution." *Joint Force Quarterly : JFQ*, no. 88 (2018)

Pigeau, R., and C. McCann. "Re-conceptualizing command and control." *Canadian Military Journal* 3, no. 1 (2002)

Proser, Jim. *No Better Friend, no Worse Enemy: The Life of General James Mattis,* 1st Edition. New York, NY: Broadside Books, 2018.

Reilly, Jeffrey M. "Multidomain Operations: A Subtle but Significant Transition in Military Thought." *Air & Space Power Journal* 30, no. 1 (2016)

Roberts, Peter. "Command and Control: By Task Or Purpose?" *Whitehall Papers* 96, no. 1 (2019)

Scott, Kyle D. *Joint-all Domain Operations is Missing all-Domain Command & Control*. Newport, RI, US: Naval War College, 2020.

Seip, Mark. "Bad Idea: All Sensors, All Shooters, All the Time – a Joint All-Domain Command and Control System That Prioritizes Centralization." *Defense 360.* Center for Strategic and International Studies, 15 December 2020. https://defense360.csis.org/bad-idea-all-sensors-all-shooters-all-the-time-a-joint-all-domain-command-and-control-system-that-prioritizes-centralization/.

Sharpe, G. E., and Allan D. English. *Principles for Change in the Post-Cold War Command and Control of the Canadian Forces*. Winnipeg, MB: Published for the Canadian Forces Leadership Institute and the Deputy Chief of the Defence Staff Group by the Canadian Forces Training Material Production Centre, 2002.

Skinner, Douglas W. *Airland Battle Doctrine.* Professional Paper 463, Strike and Amphibious Warfare Research Department, Center for Naval Analyses (Alexandria, Virginia: September 1988). https://apps.dtic.mil/sti/pdfs/ADA202888.pdf

Smagh, Nishawn S. *Joint all-Domain Command and Control (JADC2).* Washington, DC: Congressional Research Service, 2020.

Syms, Paul R., Catherall John, and Andrew Rawson. *Historical Analysis of Formation and Unit HQs in Ground Manoeuvre Operations*. Potsdown West, UK: Dstl Defence and Security Analysis Division, 2019.

The Strategy Bridge. "The Integrated Joint Force: A Lethal Solution for Ensuring Military Preeminence." Last accessed 2 March 2021. https://thestrategybridge.org/the-bridge/2018/3/2/the-integrated-joint-force-a-lethal-solution-for-ensuring-military-preeminence

Thompson, James D. *Organizations in Action: Social Science Bases of Administrative Theory* (New York: McGraw-Hill, 1967): 45-55.

Tian, Nan, Alexandra Kuimova, Diego Lopes Da Silva, Pieter D. Wezeman and Siemon T. Wezeman. "Trends in World Military Expenditure." 2019 SIPRI Fact Sheet. Stockholm International Peace Research Institute, April 2020. https://www.sipri.org/sites/default/files/2020-04/fs_2020_04_milex_0.pdf.

Townsend, Stephen. "Accelerating Multi-Domain Operations Evolution of an Idea." *Army University Press.* Fort Leavenworth, Kansas, US: Military Review Special Edition (2018). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2018/Townsend-Multi-Domain-Operations/

United Kingdom. *Future of Command and Control, Joint Concept Note 2/17*. Swindon, Wiltshire, UK: Ministry of Defence Shrivenham, Development, Concepts and Doctrine Centre, 2017.

——. "Headquarters 6 (UK) Division," The British Army, Ministry of Defence, last accessed 31 March 2021. https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/

——. *Introducing the Integrated Operating Concept*. Bristol, UK: Ministry of Defence, 2020.

——. *Joint Concept Note 2/18, Information Advantage*. Shrivenham, Swindon, Wilshire: United Kingdom: Ministry of Defence, 2018.

——. *Joint Concept Note 1/20, Multi-Domain Integration.* UK: Ministry of Defence, Director Development, Concepts and Doctrine Centre, 2020.

——. *National Security Capability Review, Including the Second Annual Report on Implementation of the National Security Strategy and Strategic Defence and Security Review 2015*. UK: HM Government, Cabinet Office, 2018.

United States. *2019 Army Modernization Strategy: Investing in the future*. Washington, DC: United States Army, 2019.

——. *Army Multi-Domain Transformation, Ready to Win in Competition and Conflict*. Chief of Staff Paper #1 Unclassified Version. Headquarters, Department of the Army, 16 March 2021. https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf.

——. *Command and Control MCDP 6*. U.S. Marine Corps. Washington, DC: Department of the Navy, 1996.

——. *Department of Defence Dictionary of Military and Associated Terms*. Washington, D.C: Joint Chiefs of Staff, 2010.

——. *Joint Operational Access Concept*. Washington, DC, US: US Department of Defense, 2012.

——. *TRADOC Pamphlet 525-3-1, the U.S. Army in Multi-Domain Operations 2028.* Washington, DC: United States Army, Department of Defense, 2018.

——. *TRADOC Pamphlet 525-3-8, US Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045*. Washington, DC: United States Army, Department of Defense, 2018.

——. *USAF Role in Joint all-Domain Operations.* Washington, DC: United States Air Force, 2020.

Van Creveld, Martin. *Command in War*. Cambridge, Mass: Harvard University Press, 1985.

Vassiliou, M. S., David S. Alberts, and Jonathan R. Agre. *C2 Re-Envisioned: The Future of the Enterprise*. Boca Raton, FL: CRC Press/Taylor & Francis Group, 2014.

Walker, Guy. *Command and Control: The Sociotechnical Perspective*, edited by Guy H. Walker, Neville A. Stanton, Paul M. Salmon and Daniel P. Jenkins. 1st ed. Farnham, Surrey, England; Burlington, VT: Ashgate, 2009.

Watling, Jack and Daniel Roper. "European Allies in US Multi-Domain Operations." *Royal United Services Institute for Defence and Security Studies.* (RUSI Occasional Paper, 2019)

Wilson, Heather, David L. Goldfein, and Kaleth O. Wright. *Memorandum for all Commanders and HAF Staff, Multi-Domain Command and Control (MDC2) Implementation Plan*. Washington, DC: The Secretary of the Air Force, Chief of Staff, United States Air Force, 2018.