National Defence
Défense nationale

Canadian
Forces
College

Collège
des
Forces
Canadiennes

CREATING THE FOUNDATION FOR MULTI-DOMAIN OPERATIONS

Lieutenant-Colonel Jason Caron

JCSP 49

Exercise Solo Flight

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.

PCEMI n° 49

Exercice Solo Flight

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.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Exercise Solo Flight – Exercice Solo Flight

CREATING THE FOUNDATION FOR MULTI-DOMAIN OPERATIONS

Lieutenant-Colonel Jason Caron

"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 difuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

CREATING THE FOUNDATION FOR MULTI-DOMAIN OPERATIONS

Introduction

As the future of modern battlespaces evolves with the rapid advance of technology, Western militaries have wrestled with the question, "What is after Joint" as a method to focus cross-domain operations.[1] To counter evolving threats from adversaries leveraging "grey zone" operations and Anti Access / Area Denial (A2AD) tactics, the United States of America's (USA) Army has developed the concept of Multi-Domain Operations (MDO) to counter these tactics by employing capabilities across all domains including Cyber and Space.[2] To successfully adopt the principles of MDO, the USA's Department of Defense has embarked upon a rigorous education program designed to educate its personnel in MDO, particularly enhancing familiarity with the two newest domains of Space and Cyber.[3] As other Western armed forces adopt this new methodology of integrating multiple domains' capabilities into operations, how might the Canadian Armed Forces (CAF) best position itself to adopt MDO?

MDO as a concept is critical for future CAF operations; in particular, several modern papers have been released showcasing how adversaries are developing new ideas to counter our key allies' military strength.[4] Since MDO is designed to enable allies to think and plan effects to counter both the "grey zone"[5] and A2AD[6] methods by our adversaries, the CAF must position itself to work as part of an allied force to counter them. MDO showcases itself as an extension of joint warfare through armed forces' capabilities that impact modern technology, having pan-domain cascading effects in others.[7] Thus, attaining pan-domain proficiency would be the next progressive step to integrating cyber and space environments with traditional warfighting domains.

This paper presents specific recommendations that can be adopted now by the CAF to help the integration of MDO practices in the future. Due to the relative size differences between the armed forces of the USA and Canada, conducting a similar education program to the United States Air Force (USAF) on an equivalent scale would take much work.[8] Therefore, more focused education on critical positions within the unit level would set conditions to implement MDO in detail. Once it takes root to create a center of expertise, this focused education can program an effective familiarity program and training for the greater CAF.

This paper is organized to describe what MDO is, what it is meant to do, and outline why the CAF must adopt it. It then describes some of the mixed capabilities the

[1] Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought." 61.
[2] James Black, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paillé, Fiona Quimbre, "Multi-Domain Integration in Defence," 9.
[3] Flack and Reith, "Self-Directed Learning Tools in USAF Multi-Domain Operations Education."
[4] Burke et al., "People's Liberation Army Operational Concepts," 8.
[5] Terry, "'Gray Zone' Competition - The Race for Multi-Domain Capability."
[6] Krause and Bruns, "Power-Projection vs. Anti-Access/Area-Denial (A2/AD): The Operational Concepts of the U.S. Navy (USN) and the People's Liberation Army Navy (PLAN) in the Indo-Pacific Region," 170.
[7] Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," 67.
[8] Flack and Reith, "Self-Directed Learning Tools in USAF Multi-Domain Operations Education."

CAF already possesses to generate personnel with the required technical skills. The following section describes where current CAF doctrine and organizations can be modified to embrace MDO best. Next, this paper discusses where modifications to existing education and training could be revised and expanded for CAF personnel incorporating MDO. The remaining section discusses cultural practices that must be adopted throughout the CAF to embrace the pace of technological developments supporting MDO.

MDO is Critical to Future Operations

MDO is the planning methodology integrating aspects from multiple domains to create far-ranging effects necessary to overcome adversarial capabilities.[9] MDO was developed primarily as a countermeasure to adversary use of A2AD capabilities, as no single service could contend with them alone.[10] The primary driver of the concept is that operations within multiple domains are conducted in a synergetic and simultaneous fashion to overwhelm adversaries' capabilities. Under this concept, personnel across the traditional environments of Land, Maritime, and Air require an expanded education and training to adopt familiarity with the two newest domains of Space and Cyber to plan operations together to achieve the necessary effects.

Despite the strategic analysis of the CAF primarily subscribing to "contribution warfare" when working on international operations[11], its personnel must still understand the concept when working with allies to provide capabilities and sensors for further integration effectively. By way of example, picture the CAF providing its CF-18 fighter force to the North Atlantic Treaty Organization (NATO), Baltic air policing[12], whereby it patrols Eastern Europe to counter Russian aggression. In this example, despite the air power being provided, several other domains are leveraged to support the overall mission within the NATO construct. Examples include relying on space domain assets to provide early warning, intelligence, and cyber defence capabilities to protect the deployed Air Task Force's (ATF) communications and planning networks. Expanding this example within the traditional joint construct, NATO could further support with capabilities from the maritime and land domains to extend the coverage of air defence radars and land-based air defence systems to counter Russian aggression further.

The difference between what are joint effects and where the expanded definition of MDO is more accurate is that the overall impact of the Baltic air policing mission is achieved through a pan-domain consideration whereby the mission is effectively supported while protecting each capability across multiple domains. Traditional joint effects include utilizing all assets to achieve exquisite results. Still, planners must account for the technological integration and understanding achieved with intelligence,

[9] Atkins, "Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace," 26.

[10] "The US Army's Multi-Domain-Operations Doctrine."

[11] Vance, "Tactics Without Strategy or Why the Canadian Forces Do Not Campaign.," 280.

[12] Department of National Defence, "Canada's Air Task Force – Romania Begins NATO Air Policing Mission."

surveillance reconnaissance (ISR) and communications technologies that MDO strives to achieve.[13]

Another critical threat posed by adversaries is conducting operations below the threshold of outright conflict when considering the defence of Canada. These operations do not directly involve armed forces but instead use other activities, such as coercion or subterfuge, to fulfill political goals.[14] These activities do not fall within the purview of operations involving the CAF unless it is targeting its personnel on an overseas operation. The primary institution responsible for countering these sorts of activities in Canada is the Canadian Security Intelligence Service (CSIS). To effectively counter the below-the-threshold effects of an adversary's armed forces in Canada, it would require a cross-domain response involving assistance and expertise from other government departments, such as CSIS, to achieve the overall impact. An example of below-the-threshold-type attacks against Canada would be reported adversary operations targeting Canadian democratic elections.[15] Leveraging the recent CSIS reporting on the issue, adversaries' "grey zone" tactics can be summarized along with the subversion, deception, and coercion techniques that targeted elected members, Canadian audiences, and critical members involved in the elections process within Canada.[16] The overall Canadian response to elections security would be led through the Department of Public Safety and CSIS as the leading agency to combat these threats from a foreign adversaries. In the 2019 Canadian elections, capabilities within the Department of National Defence, namely the Communications Security Establishment (CSE), were leveraged in concert with the Royal Canadian Mounted Police (RCMP) and Global Affairs Canada (GAC) through the Security and Intelligence Threats to Elections (SITE) task force.[17]

There are many recent examples of the CAF supporting other departments with its personnel to support recent domestic emergency responses such as COVID.[18] In the elections security example, the CAF may have participated through its expertise in cyber defence through the Canadian Forces Network Operations Centre (CFNOC) by providing trained personnel to help watch for network intrusion attempts.[19] The CAF could also assist with delivering Public Affairs support to reporting online disinformation[20] as it is found and confirmed through GAC and CSIS.[21] In both examples, the CAF has one advantage over its other security-related departments regarding the number of personnel. By leveraging similar skill sets, the CAF can augment the different departments by providing personnel required to counter online threats of disinformation and cyber threats.

[13] Underwood, "Preparing Leaders for Joint Multidomain Warfighting," 17.
[14] Roberts, "On the Need for a Blue Theory of Victory," 3.
[15] Canadian Security Intelligence Service, "FOREIGN INTERFERENCE THREATS TO CANADA'S DEMOCRATIC PROCESS," 7.
[16] Canadian Security Intelligence Service, "FOREIGN INTERFERENCE AND YOU," 4.
[17] Canadian Security Intelligence Service, "FOREIGN INTERFERENCE THREATS TO CANADA'S DEMOCRATIC PROCESS," 14.
[18] Government of Canada, "OP VECTOR."
[19] Stephen Fouchard, "Cyber Operations an Enjoyable Puzzle."
[20] Government of Canada, "Countering Disinformation with Facts - Russian Invasion of Ukraine."
[21] Canadian Armed Forces / Department of National Defence, "Canadian Armed Forces: Official."

The current state of MDO in the CAF

The CAF has personnel with the skills and expertise within its current organization to leverage the specialized capabilities required to move from the joint operations construct into MDO. Specifically, many of the technical functions within Space and Cyber have been recently consolidated across the CAF within newly created units and trades. Additionally, many related expertise sets within the Space and Cyber domains that reside within the Information domain, such as influence activities (IA) and electronic warfare (EW), exist within multiple CAF units. These capabilities are also crucial to MDO due to the impacts these capabilities can create within the Space and Cyber domain.

The CAF Cyber forces primarily exist under the direction of the recently assigned Joint Forces Cyber Component Commander within the Associate Deputy Minister Information Management (ADM(IM)).[22] These forces include the newly created Cyber Operator occupation, primarily employed within CFNOC, who are responsible for monitoring and defending them against external threats. The unit mainly resides within the Ottawa region, as it often works closely with CSE and the Canadian Centre for Cyber Security as part of its mandate to defend CAF networks.[23]

As of the summer of 2022, the CAF has organized all its Space Domain expertise under the Royal Canadian Air Force (RCAF) within the 3rd Canadian Space Division (3 CSD). This unit primarily resides within the Ottawa area as it has many ties within the Canadian Space Agency for its expertise and mutual support.[24]

To properly execute MDO, the CAF requires capabilities with effects across multiple domains. Personnel with the expertise and capabilities that affect the information domain and the electronic-magnetic spectrum (EMS) are critical to MDO. Many of these specialized capabilities exist within the traditional environmental organizations of the RCAF, Royal Canadian Navy (RCN) and the Canadian Army (CA). The RCAF possesses its own EW support unit with 414 EW Squadron located within Ottawa, which provides information for training and the defence of its air platforms.[25] The RCN has its own Naval Electronic Sensor Operator trade trained to operate the RCN's various ship EW capabilities.[26] The CA have specialized capabilities in Influence Activities Task Force and 21 EW Regiment and placed them within the 5th Division to keep the collective training available for the CA within one spot.[27]

Despite possessing several specialized units, the primary reason that the CAF is not yet best postured to incorporate the practices of MDO is that there is no method by which the technical expertise and education required within these units are shared across

[22] Director General Evaluation, "Evaluation of the Cyber Forces," 5.

[23] David Perry, Canadian Global Affairs Institute, "Defence Deconstructed: Developing the CAF's Cyber Force."

[24] Government of Canada, "3 Canadian Space Division."

[25] Government of Canada, "414 Electronic Warfare Support Squadron."

[26] "Naval Electronic Sensor Operator."

[27] Government of Canada, "Units and Formations - 5th Canadian Division."

every CAF officer and non-commissioned member (NCM). Unlike the Cyber Operators and Naval Electronic Sensor Operators, most of these individual units are occupied by trades that do not specifically specialize. Personnel planning MDOs require familiarity and education within the new domains to best leverage and consider the unique capabilities as needed.

What can the CAF do to best posture itself for future MDO adoption?

To adopt MDO, a culture that exceeds joint and retains the principles of mission command must be developed and adopted CAF-wide.[28] At the core of MDO integration, the CAF requires training and education within one place to provide a center to create the content and cultural changes necessary to embrace MDO best. The best unit to commence integration would be within the Canadian Joint Operations Command (CJOC) operations and planning staff, specifically the sub-units responsible for planning and conducting CAF operations.[29]

CJOC is the best unit to lead MDO integration for the CAF primarily due to its current role as the joint forces planning centre for domestic and international-based operations. The commanders of the 3 CSD and DGIMO are already assigned the roles of Joint Forces Space Component Commander (JFSCC)[30] and Joint Forces Cyber Component Commander (JFCCC), respectively, with established reporting lines directly to Commander CJOC.[31] It is also advantageous that CJOC is already located in Ottawa, where 3 CSD and the Canadian Cyber Forces reside with their partner agencies.

The CAF could be considered best postured for MDO integration right now due to the proximity of CJOC and the two newest domain organizations; however, the integration still needs to be internalized. When looking within CJOC, the best sub-units to perform the integration of MDO should be concentrated along three different sections: the J3 Operations, J5 Planning and Joint Targeting and Effects (JTE) branches. Here, the CAF could best position itself for MDO integration by beginning to structure education, training, and lexicon through planning, executing, and conducting operations with MDO-attuned personnel within these sections.

J5 Plans

With MDO, all domains of warfare in military operations require consideration to counter both below-the-threshold operations and adversary A2AD. The first key concern when planning operations would be protecting CAF forces from being imperilled by adversary attacks from their capabilities by planning the security aspects of deployed forces via the Shield concept capability of their forces.[32] The J5 Plans section is responsible for planning future deployments and creating conceptual operations to fast-track response to likely emergencies, such as domestic support to Canada in case of

[28] Smith, "Mission Command in Multi-Domain Operations."

[29] Government of Canada, "Canadian Joint Operations Command (CJOC)."

[30] Government of Canada, "Royal Canadian Air Force and Space."

[31] Director General Evaluation, "Evaluation of the Cyber Forces," 30.

[32] Canadian Forces Warfare Centre, *CFJP 3.0 Operations*, 1–5.

natural disasters like OP LENTUS.[33] The other conceptual capability would be the Sustain aspect within the J3 and J5, as integrating modern computer technology enhances supporting services, which means that the protection and deployment of these systems are paramount to operational success.

The reason for the J5 section to possess the MDO mindset and familiarity training is that these planners must know precisely when to consider all aspects of each domain regarding any future CAF operation. Suppose the operation requires additional skill sets in the various domains to participate in planning. In that case, they must be able to enlist the expertise of the different specialized units for more guidance. Another essential consideration would be to consider alliance planning activities with MDO-minded allies. CAF J5 planners must be familiar with other capability considerations pan-domain to assess the best CAF capabilities for alliance or coalition planning efforts.

The critical aspect relates to the Shield concept within the CAF planning process, whereby deploying Canadian units would be threatened by adversary capabilities across all domains. Here staff planning elements responsible for the deployment of CAF assets would be able to account for adversary threats from each domain and deploy the best security capabilities while ensuring that the appropriate countermeasures and training are implemented before the execution of the operation.

J3 and JTE

Like the planning criteria used within the J5 Planning, considering the collective capabilities across all domains to overwhelm the adversary's A2AD systems leveraging the Command, Act and Sense aspects.[34] When planning MDO to counter an adversary's A2AD capabilities, for example, the encroaching area that has been denied through political power such that there are no nearby ports or airports to deploy forces and is defended through a series of networked air defence systems. As part of an integrated plan, capabilities from Cyber and Space are included to counter the adversary's air defence networked technology by deceiving and blinding their sensors before forces are deployed.[35] To achieve the necessary integration and understanding across all domains, the J3 and JTE staff must have access to and understand the diverse technical expertise required to ensure the proper execution of these specialized capabilities. Therefore, MDO-integrated planning and expertise within the J3 Operations and JTE would be best for exercising the execution of coordinated capabilities.

CJOC requesting the localized expertise of the Space and Cyber forces residing close by in Ottawa would be enough to conduct MDO, but there is a problem. The primary issue with the staff currently is that there needs to be a common language that exists between the domains that allow different experts to coordinate effects and impacts.[36] The current CAF Joint Targeting guidance gives excellent guidance regarding using conventional munitions. Still, the Space and Cyber domains need further

[33] Canadian Forces Warfare Centre, 4–6.
[34] Canadian Forces Warfare Centre, 1–5.
[35] Langford, "Australia's Offset and the A2/AD Strategies," 95.
[36] Miller, "Cross-Domain Operations," 18.

consideration, as their unique characteristics should be mentioned.[37] There exists no advice to cross-communicate a common lexicon or consideration for effects that have impacts between the domains. This shortfall of commonality in understanding the capabilities gets further exacerbated when considering the J3 section, which has responsibilities for monitoring and reporting on the current situation in operations.

MDO integration and expertise are essential for the J3 staff to monitor events across operations and understand what it means when piecing every aspect together, whether directly supporting operations or at the operational level. From the CJOC headquarters level, it would be across multiple CAF operations. There the J3 would be the primary integrator of planning the Joint Task Force (JTF) structure on CJOC operations, and through them, they would establish the reporting norms for the JTF. However, the key MDO integration would occur at lower JTF levels. This means that the skill sets, training and reporting efforts required from the JTF would be driven through the J3 at CJOC.

The JTE section is responsible for leading the CAF Targeting process for the various CJOC operations whereby CAF capabilities are used in conflicts. The CAF Targeting doctrine has rules and procedures governing using conventional munitions and non-lethal effects, including Information operations and influence activities. The shortfall within Information operations is that the target audience is well described; however, there needs to be guidance defining the medium on which they can be conducted. For example, a broader understanding of how current technology creates and proliferates messaging is just as important as the message itself.[38] The CAF Targeting doctrine requires updates to consider further the impacts of cyber and space capabilities across numerous disciplines and how best to apply their integrated effects to achieve more significant results. Therefore, achieving MDO expertise within the JTE would require expanded education with the new domains since its governing principles need combining effects from multiple domains to achieve tactical and operational level effects.

Beyond the scope of the paper but very much needed to be considered with MDO is the investment in complex systems to fuse sensor information. The CAF has officially stated its goals with operational integration into the Digital Campaign Plan.[39] It leverages technology to enhance the Command, Sense and Act functions requiring pan-domain understanding to coordinate and display that information. Understanding how these systems function to integrate sensors and fuse data will also enhance MDO planning for targeting adversary systems while protecting deployed CAF units which will be discussed later.

It is not just about the CAF

To counter future “grey zone” operations from an adversary, the CAF must seek methods of integrating other security departments, such as CSIS or CSE, within their

[37] Joint Doctrine Branch, Canadian Forces Warfare Centre, *CFJP 3-9 - Targeting*.
[38] Mirbabaie et al., “Digital Nudging in Social Media Disaster Communication,” 1100.
[39] Canadian Armed Forces / Department of National Defence, “Canadian Armed Forces Digital Campaign Plan,” 16.

MDO planning processes. Canadian government departments must be able to work alongside each other, with consideration from the CAF that other departments have fewer personnel. It is becoming more commonplace for the CAF to be directed to assist other government departments with both personnel and its unique capabilities in responding to emergencies that are not directly linked to conflict or warfare.

To properly exercise MDO for future CAF operations, CJOC must integrate other government agencies within CAF operations planning to enhance MDO further. Organizations such as the Canadian Space Agency and CSE are already tied with similar CAF organizations to share resources and expertise in pursuing common goals for Space and Cyber. Working with other departments helps the CAF refine its MDO planning processes to include other department capabilities and specialties to achieve impacts on the battlefield outside its capacity.

Amending the Training and Education of MDO

It is paramount to discuss how the training and education to incorporate for the CAF to excel at MDO, ensuring that the selected personnel are effectively trained for employment within these CJOC sections. Considering the issues of the common lexicon between domains and collective understanding outlined previously more than attempting to group the necessary specialists within CJOC is needed to achieve MDO practices. An education with the new domains of warfare must be implemented to facilitate communications and understanding across all sections to leverage coordinated planning effectively.

The joint operational planning process (OPP) is the current method by which the CAF brings diverse expertise across the RCN, CA, and RCAF to conduct joint planning.[40] The CAF mandates training in OPP specifically to personnel before employment within the J3 and J5 sections at CJOC and some of its subordinate commands. The CA introduces the OPP process within their Army Operations Course, specifically for Army planning for their junior officers.[41] The RCAF conducts similar training for junior officers through the Air and Space Operations Course.[42] There is also the Joint Operational Planning course, typically for personnel employed at a J3 or J5 section at CJOC or one of its six regional headquarters across Canada.[43] Typically, this course is meant for staff officers but can be opened for all rank levels. The last available course that gives official OPP training is the Joint Command and Staff Programme, targeting senior CAF officers.[44]

The specific joint OPP courses would be excellent candidates to start completing MDO considerations while instructing the necessities of multi-domain concerns from

[40] Canadian Forces Warfare Centre, *CFJP 3.0 Operations*, 5–2.

[41] Canadian Army Command and Staff College, "Canadian Army Command and Staff College Army Operations Course Joining Instructions."

[42] Captain Robert MacKenzie and Major Jen Campbell, "Air and Space Power Operations Course Breaks down 'Stovepipes.'"

[43] Canadian Forces College, "Joint Staff Operations Programme."

[44] "Joint Command and Staff Programme."

adversary capabilities. For instance, lessons could be generated on how best to approach new types of training and education with cyber or space domain capabilities and how they support overall efforts for international operations. These courses could integrate a familiarity and planning portion of classes to ensure new domains are taught while covering lexicon and planning considerations between both. This would also include engaging and leveraging capabilities from these domains and resource requirements, like providing Space and Cyber domain expertise from 3 CSD and CFNOC to advise students during the exercise portions.

The other aspect of training would focus on leveraging capabilities from multiple domains to resolve complex operations and targets for future operations by expanding the Joint Targeting training. The current joint publication on Targeting for the CAF was last released in 2014 when expertise in the cyber and space domains was still in development, meaning that a refresh of the current understanding of each domain should be prioritized.[45] One of the issues with the outdated publication is that the process was tailored towards the execution of conventional military effects that assumed every capability could follow the same process. This can be readily accomplished through joint exercises and training based on potential future conflicts with adversaries requiring new methods to assess and engage targets. For example, an exercise could include an adversary attempting to exploit Western concerns to minimize civilian casualties by hiding their command centers within civilian-populated structures to avoid conventional munitions. Capabilities from the new domains may be the best method to disable those command centres while not threatening civilian lives or infrastructure. Completing such exercises would give Targeting staff confidence when approaching complex problems while providing a way to organize MDO to achieve similar effects from the new domains.

Preparing the Command and Sense aspect of MDO

To add two additional warfare domains, the CAF must prepare its information technology (IT) and sensor systems to collect information for commanders while avoiding information overload across the many domains.[46] As the commander's staff must assess sensor information and make judgment calls, they must be familiar with the systems to manage its presentation. A unique aspect of MDO is the integration of multiple sensors from various platforms providing an accurate picture of operations.[47] Intelligence staff will require the capacity and expertise with big data management tools to assess and compile the influx of information across multiple domains.[48] Part of the future education aspect required to adopt MDO quickly would be the pan-domain management of multiple sensor data to respond to changing situations on the battlefield.[49]

[45] Joint Doctrine Branch, Canadian Forces Warfare Centre, *CFJP 3-9 - Targeting*.

[46] Prunckun, "Drinking from a Fire Hydrant: Information Overload As a Cyber Weapon," 61.

[47] Daly et al., "The Future of Aerial Intelligence, Surveillance, and Reconnaissance in Support of Multi-Domain Operations," 47.

[48] Cruikshank, "The ABCs of AI-Enabled Intelligence Analysis," 4.

[49] Porche, Rand Corporation, and National Defense Research Institute (U.S.), *Data_flood: Helping the Navy Address the Rising Tide of Sensor Information*, RR-315-NAVY:20.

A vital element of this training would be augmenting the CAF's collective digital literacy and enhancing it such that all personnel can embrace the management and adoption of newer tools to manage the information. Digital literacy is the knowledge and expertise to consume, create and present information directly related to the multiple IT technologies available and in development.[50] Starting an education program earlier in the CAF would be paramount for leading its personnel in adopting new systems and tools to manage, assess and present the information from multiple domains into a coherent picture for commanders to consume and base decisions on.

To further support digital literacy integration for the CAF, its personnel will require the environment and tools to establish the capacity to practice it. This plan has already been identified within the CAF Digital Campaign Plan.[51] All that remains is the technological implementation across all the bases and wings across Canada. For example, the RCAF has implemented widespread use of its Electronic Flight Bags (EFBs) that complement flying operations procedures and allow custom software to assist with administrative functions.[52]

Media literacy, like digital literacy, is the ability to consume information, understand the technology used to create it and leverage modern and future media technology to communicate your message.[53] It is helpful for modern-day Information Operations and ensures commanders have the necessary considerations for impacts in the public information sphere while providing resilience against adversary information operations to its forces.[54] This sort of education aligns with digital literacy, whereby the effects of observing the news and assessing how one's actions can be interpreted online are helpful. This also helps with understanding how to craft the appropriate messaging by understanding the different technologies used by media platforms today. This is essential to understand how messaging can be exploited through various technologies.

Media literacy also enhances a JTF commander's ability to understand how an adversary can perceive their actions and either counter the narrative before operations or prepare and conduct deception for future operations. Media literacy, in this way, enhances the CAF's capacity to perform and familiarize themselves with information operations while at the same time recognizing an adversary's attempt to exploit and provide resilience toward these attacks.

Adopt the culture of Lifelong Learners.

To better prepare the CAF to adopt MDO, it must adopt a "continuous learning" culture to train its personnel in new technology and techniques. Embracing familiarity with new warfare domains while simultaneously expanding educational opportunities

[50] Adobe, "What Is Digital Literacy?"
[51] Canadian Armed Forces / Department of National Defence, "Canadian Armed Forces Digital Campaign Plan," 17.
[52] TAA & OAA RCAF, "Advisory on Obtaining TAC and OAC for Portable Electronic Flight Bags."
[53] Mary Kate Lonergan, "WHAT Is Media Literacy and HOW Can Simple Shifts Center It."
[54] Ventsel et al., "Building Resilience Against Hostile Information Influence Activities: How a New Media Literacy Learning Platform Was Developed for the Estonian Defense Forces."

with digital and media literacy requires much investment in the short term. Specialized college and university training usually can require up to four years before entering the workforce as a specialist within a technological domain.[55] Even technical experts in communications and cyber disciplines must constantly learn new fields of technology to maintain the operational advantage of the space to both defend and, if necessary, defeat adversaries' use of these systems.

To best adopt a culture of continuous learning regarding new technology, the CAF must outfit its personnel with the capacity to test and integrate it at the lowest level possible. Herein the CAF must allow its units to learn and incorporate changes instead of waiting for one planning unit at the national level to lead implementation efforts for everyone. For example, suppose CAF personnel are educated early in modern digital and media literacy training. In that case, this foundation allows personnel to be better equipped to test new technology independently.[56] To better adapt to the digital mindset, the culture of leveraging modern-day applications and using digital platforms to resolve administrative burdens must become the standard experience for every CAF member. There are risks with promulgating connectivity in large numbers towards the CAF due to cyber threats against its members due to misuse.[57] However, ensuring every CAF member receives a similar education and practice in using digital applications and managing data raises its' digital literacy while providing an education in modern cybersecurity practices.[58] Having all its members familiar with modern technology and information management practices will better prepare the CAF to adopt advanced MDO practices across multiple domains.

Conclusion

MDO represents a new concept by which armed forces approach warfare that combines capabilities and defence against threats from the two latest domains of war along with the traditional domains. MDO, at its basic level, appears to be the newest version of joint warfare; however, when looking deeper into the technological expertise and pan-domain considerations that both Space and Cyber require, it becomes much more complex due to how both domains' technologies interact with the traditional domains. MDO is not just a new concept for including an all-domain approach to targeting various adversary capabilities but also considers planning aspects whereby capabilities can impact multiple domains. MDO also consists of the planning aspects for the defence of friendly forces on deployment that may be susceptible to adversary capabilities seeking to exploit advantages in these new domains.

To best posture the CAF for formally integrating MDO into its planning standards, the best unit to align these efforts would be the CJOC headquarters, specifically within its J3, J5 and JTE sections, to initially implement it and then use their experiences to inform the greater CAF. The staff sections outlined above are best

[55] University of Toronto, Office of the Registrar, "Computer Science."
[56] Crittenden, Biel, and Lovely, "Embracing Digitalization: Student Learning and New Technologies."
[57] Strelicz, "Risks and Threats in Cyberspace – The Key to Success in Digitization," 4.
[58] Yuliana, "THE IMPORTANCE OF CYBERSECURITY AWARENESS FOR CHILDREN," 42.

postured to immediately execute the MDO concept and create a solid foundation of a common lexicon to fuse understanding across all domains.

Another benefit of MDO integration is that it allows the CAF another medium by which it can support operations from other government departments, specifically the cyber and space domains that already have government partnerships with them. In this aspect, if an adversary is leveraging below-the-threshold operations, the CAF could counter its operations by supporting other departments better suited to the operation with the support of CAF capabilities and personnel. The CAF exercising MDO with other departments give the Government of Canada further flexibility to respond to encroaching threats across nonmilitary aspects.

The CAF will also need to refine its training and education for its members to foster expertise in the newest domains to execute MDO. Modifying the joint OPP and joint targeting courses can integrate domain familiarity training into their curriculum to start education. Follow-on joint training exercises leveraged through the practical application at CJOC would further benefit the development and integration of MDO.

MDO requires a higher level of digital literacy to incorporate the new warfare domains better and manage multiple sensors and information. The CAF could also incorporate digital literacy pan-CAF into its necessary training by leveraging the technology across all its education and training. Digital literacy also supports the CAF Digital Campaign Plan, which leverages updating current CAF administrative processes and future sensor integration, further assisting MDO implementation.[59] Also, digital literacy helps with learning media literacy, which benefits commanders' understanding of modern-day information operations, how adversaries exploit it, and defensive measures that can be considered to counter threats.

As one of the most critical aspects of preparing itself for the integration of MDO, the CAF must adopt a culture of lifelong learning to train its personnel for the educational goals outlined in the paper. To create an environment for learning, the CAF must establish a digital environment and include this technology in every course and administrative function of the CAF, allowing its personnel to learn and exercise familiarity. Although it can be argued that this further opens the CAF to vulnerabilities from the information and cyber domains, it also educates and provides a proper learning ground to incorporate cyber security practices to guard against future threats.

[59] Canadian Armed Forces / Department of National Defence, "Canadian Armed Forces Digital Campaign Plan," 8.

BIBLIOGRAPHY

Adobe. “What Is Digital Literacy?” Information & Business. Adobe.com, 2023. https://www.adobe.com/acrobat/hub/how-to/what-is-digital-literacy.html.

Atkins, Sean A. “Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace.” *Air & Space Power Journal* 32, no. 3 (2018): 26–44.

Burke, Edmund J., Kristen Gunness, Cortez A. Cooper, and Mark Cozad. “People’s Liberation Army Operational Concepts.” *Policy File*. RAND Corporation, 2020.

Canadian Armed Forces / Department of National Defence. “Canadian Armed Forces Digital Campaign Plan.” Canadian Armed Forces, June 17, 2022. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2022/06/release-caf-digital-campaign-plan.html.

———. “Canadian Armed Forces: Official Twitter.” Social media. Twitter, December 7, 2022. https://twitter.com/CanadianForces/status/1600598001722048512?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Etweet.

Canadian Army Command and Staff College. “Canadian Army Command and Staff College Army Operations Course Joining Instructions.” CASC, June 7, 2015. https://www.canada.ca/en/army/services/line-sight/articles/hold/army-operations-course-aoc.html.

Canadian Forces College. “Joint Command and Staff Programme.” Information, April 13, 2023. https://www.cfc.forces.gc.ca/226-eng.html.

———. “Joint Staff Operations Programme.” Information. Canadian Forces College, November 8, 2021. https://www.cfc.forces.gc.ca/230-eng.html.

Canadian Forces Warfare Centre. *CFJP 3.0 - Operations*. CFJP. Ottawa: Canadian Forces Warfare Centre, 2011.

Canadian Security Intelligence Service. “FOREIGN INTERFERENCE AND YOU.” Canadian Security Intelligence Service, February 9, 2022. https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-and-you/AOSE_ForeignInterferenceHandout%20-%20Digital_ISBN_A.pdf.

———. “FOREIGN INTERFERENCE THREATS TO CANADA’S DEMOCRATIC PROCESS.” Government of Canada, July 2021. https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-threats-to-canada%27s-democratic-process.pdf.

Captain Robert MacKenzie and Major Jen Campbell. “Air and Space Power Operations Course Breaks down ‘Stovepipes.’” Information & News. The Maple Leaf, January 4, 2019. https://www.canada.ca/en/department-national-defence/maple-leaf/rcaf/2019/01/air-and-space-power-operations-course-breaks-down-stovepipes.html.

Crittenden, William F., Isabella K. Biel, and William A. Lovely. “Embracing Digitalization: Student Learning and New Technologies.” Edited by Victoria Crittenden and Robert A. Peterson. *Journal of Marketing Education* 41, no. 1 (2019): 5–14. https://doi.org/10.1177/0273475318820895.

Cruikshank, Iain. “The ABCs of AI-Enabled Intelligence Analysis.” *War on the Rocks*, February 14, 2020, 3.

Daly, Derek, Vinette Lawrence, Paul Giamalis, and James Beyer. “The Future of Aerial Intelligence, Surveillance, and Reconnaissance in Support of Multi-Domain Operations.” *Military Intelligence Professional Bulletin* 46, no. 2 (2020): 46–53.

David Perry, Canadian Global Affairs Institute. “Defence Deconstructed: Developing the CAF’s Cyber Force.” Defence Deconstructed, n.d. https://www.cgai.ca/developing_the_cafs_cyber_force.

Department of National Defence. “Canada’s Air Task Force – Romania Begins NATO Air Policing Mission.” Information. Government of Canada, August 4, 2022. https://www.canada.ca/en/department-national-defence/news/2022/08/canadas-air-task-force--romania-begins-nato-air-policing-mission.html.

Director General Evaluation. “Evaluation of the Cyber Forces.” ADM (Review Services), April 2021. https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2021/reports-pubs-audit-eval/report-1258-3-031-en.pdf.

Flack, Nathaniel, and Mark Reith. “Self-Directed Learning Tools in USAF Multi-Domain Operations Education.” In *European Conference on Cyber Warfare and Security*, 752–XIV. Reading: Academic Conferences International Limited, 2019.

forces.ca. “Naval Electronic Sensor Operator.” Information & Recruitment, April 2023. https://forces.ca/en/career/naval-electronic-sensor-operator/.

Government of Canada. “3 Canadian Space Division.” Information & News. Canada.ca, October 11, 2022. https://www.canada.ca/en/air-force/corporate/3-canadian-space-division.html.

———. “414 Electronic Warfare Support Squadron.” Information. Canada.ca, March 22, 2021. https://www.canada.ca/en/air-force/corporate/squadrons/414-squadron.html.

———. “Canadian Joint Operations Command (CJOC).” Information. Canada.ca, July 12, 2018. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/canadian-joint-operations-command.html.

———. “Countering Disinformation with Facts - Russian Invasion of Ukraine.” Information & News. Canada.ca, March 22, 2022. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng.

———. “Espionage and Foreign Interference.” Information. Canada.ca, April 12, 2021. https://www.canada.ca/en/security-intelligence-service/corporate/publications/2020-public-report/the-threat-environment.html.

———. “Op VECTOR (CAF Support to the Distribution of COVID-19 Vaccines).” Information. Canada.ca, January 19, 2020. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/secd-state-of-caf-19-april-2021/reference-material/op-vector.html.

———. “Royal Canadian Air Force and Space.” Information. Canada.ca, October 8, 2020. https://www.canada.ca/en/air-force/corporate/space/roles-leadership.html.

———. “Units and Formations - 5th Canadian Division.” Information. Canada.ca, January 27, 2022. https://www.canada.ca/en/army/corporate/5-canadian-division/units-formations.html.

James Black, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paillé, Fiona Quimbre. “Multi-Domain Integration in Defence Conceptual Approaches and Lessons from Russia, China, Iran and North Korea.” RAND Europe, 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA500/RRA528-1/RAND_RRA528-1.pdf.

Joint Doctrine Branch, Canadian Forces Warfare Centre. *CFJP 3-9 - Targeting*. 1st ed. 3-9. Ottawa: Canadian Forces Warfare Centre, 2014. DWAN only.

Krause, Joachim, and Sebastian Bruns, eds. “Power-Projection vs. Anti-Access/Area-Denial (A2/AD): The Operational Concepts of the U.S. Navy (USN) and the People’s Liberation Army Navy (PLAN) in the Indo-Pacific Region.” In *Routledge Handbook of Naval Strategy and Security*, 201–12. Routledge, n.d. https://doi.org/10.4324/9781315732572-24.

Langford, Ian. “Australia’s Offset and the A2/AD Strategies.” *Parameters (Carlisle, Pa.)* 47, no. 1 (2017): 93. https://doi.org/10.55540/0031-1723.2839.

Lieutenant-General (Ret.) Associated Professor Constantin MINCU, Ph.D. “INFORMATIONAL SYSTEMS AND TECHNOLOGIES IN CURRENT AND

FUTURE MILITARY CONFLICTS." *Annals: Series on Military Sciences* 14, no. 2 (2022): 63–82.

Mary Kate Lonergan. "WHAT Is Media Literacy and HOW Can Simple Shifts Center It." Information & News. PBS.org, October 28, 2022. https://www.pbs.org/education/blog/what-is-media-literacy-and-how-can-simple-shifts-center-it.

Miller, Stephen W. "Cross-Domain Operations." *Military Technology* 45, no. 5 (2021): 14.

Mirbabaie, Milad, Christian Ehnis, Stefan Stieglitz, Deborah Bunker, and Tanja Rose. "Digital Nudging in Social Media Disaster Communication." *Information Systems Frontiers* 23, no. 5 (2021): 1097–1113. https://doi.org/10.1007/s10796-020-10062-z.

Porche, Isaac, Rand Corporation, and National Defense Research Institute (U.S.). *Data_flood: Helping the Navy Address the Rising Tide of Sensor Information*. Vol. RR-315-NAVY. Book, Whole. Santa Monica, CA: RAND, 2014. https://doi.org/10.7249/j.ctt6wq8rr.

Prunckun, Henry. "Drinking from a Fire Hydrant: Information Overload As a Cyber Weapon." In *Cyber Weaponry*. Switzerland: Springer International Publishing AG, 2018. https://doi.org/10.1007/978-3-319-74107-9_5.

Reilly, Jeffrey M. "Multidomain Operations: A Subtle but Significant Transition in Military Thought." *Air & Space Power Journal* 30, no. 1 (2016): 61.

Roberts, Brad. "On the Need for a Blue Theory of Victory." *War on the Rocks*, September 17, 2020, 9.

Smith, David "Cam." "Mission Command in Multi-Domain Operations." *Over the Horizon, Multi-Domain Operations & Strategy*, October 30, 2017.

Stephen Fouchard. "Cyber Operations an Enjoyable Puzzle." Information & News. Canadian Army Today, October 28, 2019. https://canadianarmytoday.com/cyber-operations-an-enjoyable-puzzle/.

Strelicz, Andrea. "Risks and Threats in Cyberspace – The Key to Success in Digitization." *Journal of Physics. Conference Series* 1935, no. 1 (2021): 12009. https://doi.org/10.1088/1742-6596/1935/1/012009.

TAA & OAA RCAF. "Joint TAA-OAA Advisory on Obtaining TAC and OAC for Portable Electronic Flight Bags." Information. Canada.ca, June 6, 2018. https://www.canada.ca/en/department-national-defence/services/military-airworthiness/technical-airworthiness-authority-overview/technical-airworthiness-regulatory-documents/technical-airworthiness-authority-advisories/2012-01.html.

Terry, James. "'Gray Zone' Competition - The Race for Multi-Domain Capability." *National Defense* 107, no. 833 (2023): 14–14.

"The US Army's Multi-Domain-Operations Doctrine." *Strategic Comments* 28, no. 8 (2022): i–ii. https://doi.org/10.1080/13567888.2022.2153499.

Underwood, Kimberly. "Preparing Leaders for Joint Multidomain Warfighting." *Signal* 75, no. 5 (2021): 16–18.

University of Toronto, Office of the Registrar. "Computer Science." Information & Education. University of Toronto, 2023. https://utm.calendar.utoronto.ca/section/Computer-Science.

Vance, Col J.H. "Tactics Without Strategy or Why the Canadian Forces Do Not Campaign." The Operational Art: Canadian Perspectives Context and Concepts. Kingston, ON: Canadian Defence Academy Press, 2005.

Ventsel, Andreas, Sten Hansson, Merit Rickberg, and Mari-Liis Madisson. "Building Resilience Against Hostile Information Influence Activities: How a New Media Literacy Learning Platform Was Developed for the Estonian Defense Forces." *Armed Forces and Society*, no. Journal Article (2023). https://doi.org/10.1177/0095327X231163265.

Yuliana, Yuliana. "THE IMPORTANCE OF CYBERSECURITY AWARENESS FOR CHILDREN." *Lampung Journal of International Law* 4, no. 1 (2022): 41–48. https://doi.org/10.25041/lajil.v4i1.2526.