

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Canada and the Interoperability Challenge

by Alexander Salt

October 2024



TRIPLE HELIX

POLICY PERSPECTIVE

CANADA AND THE INTEROPERABILITY CHALLENGE

by Alexander Salt

October 2024

A joint publication with:

TRIPLE HELIX

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
Suite 2720, 700 – 9th Avenue SW., Calgary, AB T2P 3V4
www.cgai.ca

©2024 Canadian Global Affairs Institute
ISBN: 978-1-77397-318-0

Western militaries have been actively developing the emerging concept of pan-domain operations (also sometimes referred to as multi-domain operations). This concept originated with the United States and was popularized around 2018, as it responded to shifts in the international security environment such as the reemergence of great-power competition as well as various advances in technology. Pan-domain operations enable militaries to operate across all domains and environments by employing combined arms and joint capabilities alongside other governmental assets. Canada has joined the U.S. and other allies in having identified a need to evolve military thinking beyond the traditional geographic operational domains of land, sea and air to include new areas such as the information domain, cyberspace and outer-space.[1] In order to properly respond to the challenge of pan-domain operations, Canada, along with its closest allies will be required to operate simultaneously across several different domains during future conflicts as identified in Canada's defence policy, *Strong, Secure, Engaged*[2] and the most recent Defence Policy Update, *Our North, Strong and Free*.[3] Future strategic and operational demands will require the different services of the Canadian Armed Forces (CAF) to better coordinate cross-domains and will also require the CAF to have the capabilities to fight alongside its closest allies or else risk being left behind by allies and adversaries alike. The sheer scale of this challenge significantly increases the need to enhance interoperability among allies to more effectively share resources and intelligence, enhance lethality, and allow for wider options to respond to threats.

Emerging and advanced technologies are crucial to pan-domain operations as they enable seamless military coordination across various domains. The complexity of modern operations has increased significantly, making these technologies essential for providing timely and effective solutions to new challenges. They allow militaries to operate across contested environments where traditional approaches may no longer be relevant. Advanced technologies also heighten the importance of achieving military interoperability as modern warfare increasingly relies on the integration of diverse systems and platforms. As new advanced technologies are integrated into the CAF and allied militaries, achieving highly functional interoperability becomes increasingly critical to meet the challenges of pan-domain operations and ensure the success of collaborative efforts. Military interoperability involves the near-seamless collaboration among diverse military forces, spanning different countries and service branches, to achieve shared objectives. Interoperability is key to enhancing coordination and effectiveness during joint operations, ranging from continental defence, peace-support deployments, and coalition warfare. This can involve aligning tactical approaches with the newest generation of emerging technologies. Indeed, while interoperability has always been important, current advanced technologies makes it all the more critical.

[1] "Multi-Domain Operations in NATO-Explained," *NATO Allied Command Transformation* (5 Oct 2023), https://www.act.nato.int/article/mdo-in-nato-explained/
[2] Canada, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa, ON: Department of National Defence, 2017), https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html
[3] Department of National Defence (DND), 2024. "Our North, Strong and Free: A Renewed Vision for Canada's Defence." https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html

The next generation of defence technologies have transformed the landscape of interoperability, focusing heavily on digital networking and cloud computing. Newer technologies such as Artificial Intelligence (AI), quantum computing, and advanced sensors are being rapidly integrated into this process. To enhance connectivity, Canada and its closest allies must transform their militaries from older, analogue structures into modern, fully digitized forces, that have the capacity for data accumulation, processing and storage as well as allowing for command and control (C2) to unfold at rapid speeds. These various new systems need to be able to interact and work with one another as well. This article sketches an outline of military interoperability, then explores the Canadian context of recent efforts, and concludes with suggestions to help Canada mitigate future challenges in this area.

What is Interoperability?

Interoperability is a very salient topic in military affairs. Allies fighting alongside one another has been a central characteristic of how states have waged war across history. However, modern advanced technologies, such as digital networks and new generations of sensors have radically increased the complexity of this process in the contemporary period to an unprecedented level. Further adding to this quandary is there are different definitions and understandings of the term "interoperability" among various military organizations and countries. For example, some definitions focus on specific technical dimensions of interoperability, such as the ability to have harmonized functionality of digitized information networks between militaries. There is even divergence among these technical understandings of interoperability, with some emphasizing systems, while others focus on enabler capabilities.[4] Other definitions take a broader perspective that include operational elements beyond just technical compatibility issues: NATO for example defines interoperability as, "the ability for Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives."[5] Ultimately, the commonality between most definitions is that interoperability allows allies to share and coordinate capabilities to meet multinational military objectives, such as defeating adversaries or securing other types of objectives.

Other terminology is often used alongside "interoperability" in strategic documents and doctrine. For example, "jointness" appears frequently, and generally refers to operations in which two or more different service branches of a military harmonize planning and combine their capabilities towards a common objective. An example of jointness occurs when an air force supports an army asset during a major combat engagement by providing airstrikes in support of advancing infantry and tanks.[6] Another term that is often associated with interoperability is "interconnectedness" or "interconnectivity", which describes the process in which data is shared among different sensors

[4] Chistopher G. Pernin et al, *Targeted Interoperability: A New Imperative for Multinational Operations* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2075.html, p. 13-17
[5] "Interoperability: connecting forces," *NATO* (11 Apr 2023), https://www.nato.int/cps/en/natohq/topics_84112.htm
[6] Department of National Defence, *CFJP 3.0, Operations* (Ottawa: Joint Doctrine Branch, Canadian Forces Warfare Center, 2010): 1-1, https://publications.gc.ca/collections/collection_2011/dn-nd/D2-252-300-2010-eng.pdf

and platforms within a singular network. Interconnectivity is seen as a core part of pan domain operations, and by extension the idea of Joint All-Domain Command and Control (JADC2), and the connected battlespace, which intends to allow militaries to functionally gather, process and distribute this data.[7] The newest term to be used alongside interoperability is "interchangeability", which refers to the growing preference by Western militaries to possess systems and munitions that can be used by their allies during operations. Interchangeability allows for one military to transpose a piece of equipment from another ally and integrate into their own capability relatively seamlessly.[8]

The character of interoperability will be shaped by a variety of different factors in a given period. The main threats across the international security environment play a major role in this; for example, great power competition and rivalry leads to different technological and doctrinal demands than combating transnational terrorism. The budgetary situation of allies will impact their ability to continue to upgrade their military equipment, and periods of financial austerity and budget shrinkages will place major constraints on their ability to keep up with modernized technology, which in turn leads to the growing risk of capabilities gaps between alliance leaders and junior members. The structure and mechanisms within alliances that allow for co-development of new capabilities and technologies also will have an impact on the ability for states to remain interoperable with one another. Normative factors, such as ethical beliefs can also affect interoperability by informing divergent legal regimes among allies, thus potentially acting as a constraining factor on technological connectivity. In particular, norms and ethics are very much at the centre of allied uses of AI in military affairs, as normative divergences among different allies have the potential to disrupt and constraint collaborative efforts on AI defence projects.

The current generation of emerging technologies has also reshaped how we understand the technical dimensions of interoperability, as there is now a substantial emphasis on digital networking and cloud computing in the interoperability process. During this contemporary period of information age interoperability, Canada, the U.S. and other allies are working towards integrating different sensors, effectors, data sharing and computerized command and control systems into an integrated network that would then allow near real-time coordination among allies with the wider goal of shaping the battlespace across the different domains.[9] Newer technologies such as Artificial Intelligence, quantum computing and a variety of advanced Intelligence, Surveillance and Reconnaissance (ISR) capabilities, including low orbit satellites, are continuously being integrated into this interoperability network framework.[10] There is a need for states looking to enhance interoperability to shift their mindset away from older, analog orientated processes towards building new digital architectures to allow for the sharing,

[7] "Joint All-Domain Command and Control: Background and Issues for Congress," *Congressional Research Service* (18 Mar 2021), https://crsreports.congress.gov/product/pdf/R/R46725/2#:~:text=Joint%20All%2DDomain%20Command%20and%20Control%20(JADC2)%20is%20DOD's,Force%E2%80%94into%20a%20single%20network.
[8] John A. Tirpak, "US and Partners Now Moving Toward Interchangeable – Not just Interoperable," *Air and Space Force Magazine* (30 Sep 2022), https://www.airandspaceforces.com/us-and-partners-now-moving-toward-interchangeable-not-just-interoperable-weapons/
[9] Dave Perry interview with Lt. Gen Mike Rouleau, "Lieutenant-General Mike Rouleau," *Defence Deconstructed Podcast,* podcast audio (6 Aug 2021), https://www.cgai.ca/lieutenant_general_mike_rouleau
[10] Kevin Budning, Alex Wilner and Guillaume Cote, "A view form above: Space and the Canadian Armed Forces," *International Journal* Vol. 76, Iss. 4 (2022), https://journals.sagepub.com/doi/full/10.1177/00207020211067944

processing, and storage of data as well as allowing ISR gathering, and command and control decision making, to unfold at a more rapid pace.

There are many unique challenges to building interoperability among allies that can either outright block the process from unfolding, or at minimum slow or constrain its effectiveness. At the highest level, alliance leaders such as the U.S. may become reluctant to grant access to their most secure digital networks to even their closest allies. For example, the leading state may wish to prioritize unilateral operations under certain circumstances or lack the necessary motivation to overcome related political hurdles to sharing sensitive systems. Alliance members who are more aggressive with force transformation and defence spending may undergo constant changes in their militaries' force structure and capabilities which in turn may cause difficulties with the strategic planning of others trying to keep pace with their efforts. At the tactical level, potential gaps in operational performance abilities can undercut the coordination required for streamlined interoperability. Further, technological capabilities gaps may be among the largest challenges, especially for networking; for example the U.S. was unable to securely communicate with some coalition partners during the Gulf War (1991) and Kosovo War (1999), where the U.S. found that the communication systems of these allies were unable to connect to more advanced networks, and as a result personnel had to resort to using antiquated methods of unsecured communications such as talking in codes over the radio.[11] NATO's intervention into Libya (2011) as part of Operation Unified Protector demonstrated several interoperability concerns, such as the ability of coalition members to engage in sensitive data sharing, as well as issues caused by low stockpiles of precision guided munitions.[12]

Overall, interoperability has been identified as a primary concern for most Western militaries. There is a desire to ensure that the appropriate military structures and capabilities are ready in case they are eventually needed during future operations. The reemergence of great power adversaries like Russia and China who already possess their own advanced military capabilities has added considerable motivating influences on this process, as has the war in Ukraine.[13] However, to a degree, there remains a divergence in how individual allies have interpreted the purpose and goal of interoperability, which in turn influences their preparation efforts. For example, the U.S. develops military technology first and foremost with its own military and defence in mind, so its interoperability efforts are focused on whether allied partners can physically fight alongside U.S. forces, thus their interoperability efforts are motivated by operational effectiveness.[14] While other states such as Australia may be driven by wider political objectives while approaching interoperability, such as a desire to maintain closer and deeper relations with certain allies.[15] Finland and Sweden recently joined NATO due to Russian

[11] Pernin et al, *Targeted Interoperability*.
[12] Karl P. Mueller ed., *Precision and Purpose: Airpower in the Libyan Civil War* (Santa Monica, CA: RAND, 2015), 100. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR676/RAND_RR676.pdf
[13] Mari Yamaguchi and Haruka Nuga, "NATO chief wants more 'friends' as Russia, China move closer," *Associated Press* (1 Feb 2023), https://apnews.com/article/russia-ukraine-nato-politics-jens-stoltenberg-china-aeb7fdc3ff76413aab3a84c8afa22288
[14] Myron Hura, et al, *Interoperability: A Continuing Challenge in Coalition Air Operations* (Santa Monica, CA: RAND Corporation, 2000), 7-10. https://www.rand.org/pubs/monograph_reports/MR1235.html
[15] Marcus Schultz, "US land power in the Indo-Pacific: opportunities for the Australian Army," *ASPI* (Oct 2023), https://www.aspi.org.au/report/us-land-power-indo-pacific-opportunities-australian-army

aggression in Ukraine and Europe, but have also sought to build closer integrative defence ties with the U.S.[16]

The Canadian Context

Strong, Secure, Engaged (*SSE*), released in 2017, outlines that interoperability with primary allies such as the U.S., as well as Five Eyes (FVEY) and NATO is a key focus for Canadian defence, and identifies that ISR and command and control related technologies are very important to achieving interoperability goals.[17] The CAF's *Digital Campaign Plan*, released in 2023, further states that Canada must not lag behind NATO and FVEY allies that are undergoing rapid digitization efforts, in order to maintain its relevancy on defence matters. The *Digital Campaign Plan* acknowledges that Canada's approaches to interoperability in the past have unfolded in a fairly ad hoc manner, but in future the idea is that the CAF will have transformed with the necessary force design and internal structures and systems to be better positioned to meet interoperability goals.[18]

The Trudeau government's release of *Our North, Strong and Free* in 2024 situates interoperability under the context of emerging technologies. The document notes that, "[k]eeping pace with technological change will protect Canada from international threats and ensure our interoperability with the allies and partners with whom we work to protect our collective interests."[19] The new defence policy reaffirms interoperability's importance as one of the drivers of acquiring new platforms and systems for the CAF. Further, *Our North, Strong and Free* also links the digital transformation of the CAF to interoperability, stating that wider digitization efforts, including the acquisition of new technologies such as AI, big data management systems, and secure cloud computing will help keep the CAF interoperable with its closest allies.

There has been an acknowledgement from CAF leadership that interoperability needs to be focused first and foremost on digital networking, data sharing and other information technologies. A recent study on Canadian defence and emerging technologies since the release of *SSE* has found mixed results overall, highlighting the need for Canada to accelerate its acquisition and integration process of advanced technology.[20] This trend of slower technological acquisition is further demonstrated in comparison to other FVEY allies, particularly the U.S., Australia and U.K., all of whom are quicker at adapting new technologies for defence purposes.[21] The perception is also that the CAF has needed to be better at articulating strategic plans for meeting technology related goals, though this is starting to change with recent efforts such as NORAD modernization.

---

[16] "Sweden and Finland Have Negotiated Bilateral Defense Agreements With the USA," *High North News* (Nov 2023), https://www.highnorthnews.com/en/sweden-and-finland-have-negotiated-bilateral-defense-agreements-usa
[17] *Strong Secure Engaged*, 72.
[18] Canada. *Canadian Armed Forces Digital Campaign Plan*, (Ottawa, ON: The Department of National Defence and Canadian Armed Forces, 2023)
11, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-digital-campaign-plan.html
[19] *Our North, Strong and Free*, p. 10.
[20] Alexander Salt and Alex Wilner, "Emerging Technology and Canadian Defence: From *Strong, Secure, Engaged* to Present," Canadian Global Affairs Institute, (2024, https://www.cgai.ca/emerging_technology_and_canadian_defence_from_strong_secure_engaged_to_present
[21] Alexander Salt and Alex Wilner, "Emerging Technology and Five Eyes: Implications for Canadian Defence," *Canadian Global Affairs Institute*, (2024), https://www.cgai.ca/emerging_technology_and_five_eyes_implications_for_canadian_defence#Canada

Canada may need to search out alternative strategies when procuring technologies for interoperability, such as partnering closer with industry to leverage existing systems.[22]

Canada faces several technical challenges as it enhances its interoperability capabilities.

Issues with the quality of data as well as data governance within the CAF have been longer term challenges. For example, a recent Assistant Deputy Minister Review Services report noted that, "A lack of data quality control impacts the availability of reliable information to support effective project management and senior management decision making."[23] New generations of sensors means that there is now massive amount of data points that need to be gathered from a wide range of sources. This data needs to be effectively gathered, processed and then analyzed. To ensure this unfolds in a secure and rapid enough manner, Canada will need access to cloud based digital architecture, which will likely mean partnering with the U.S. to collaborate to potentially leverage their existing systems as well as helping to avoid any unnecessary duplication of efforts. The main innovators among cloud technology are in the private sector, which provides opportunities for Canada to partner with industry to tap into already operational architectures, thus negating any need to build a new system from the ground up. Canada can also turn to lessons learned from the digital networks and integrative systems that allies are building in the Indo-Pacific, including what the U.S. is doing with regards to its sensors and missile defence systems around Guam.[24]

Canada also faces political challenges to its interoperability efforts. Canada has historically approached interoperability with a somewhat opportunistic mindset as a means of gaining access to allied technologies and have not taken into account the political implications of alliance politics. For example, many of Canada's closest NATO allies have expressed growing dissatisfaction with Canada's military contributions to the alliance.[25] Under this mindset, Canada seeks to join an alliance or partnership without first articulating what it has to offer. In recent years, allies have essentially rebuked Canada for this practice, as Canada was initially excluded from participating in the AUKUS agreement by the U.S., Australia and United Kingdom. The primary reason for such a decision is the perceived lack of commitment to defence spending by Canada.[26] To alter this perception, and to avoid being shut out of future interoperability opportunities with traditional allies, Canada will need to articulate in much firmer ways what it can offer military partnerships in way of unique capabilities.

---

[22] Dave Perry interview with Lt. Gen. Mike Rouleau et al, "Procuring for Interoperability," *Defence Deconstructed Podcast*, podcast audio (21 May 2021), https://www.cgai.ca/procuring_for_interoperability

[23] Office of the Auditor General of Canada. "ADM (RS) Audit of Information Management," (July 2022). https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2022/reports-pubs-audit-eval/report-1259-3-0067-en.pdf.

[24] Dave Perry and Julia Scouten, interview with Kate Todd et al., "Connectivity, Interoperability, and Pan-Domain Command and Control," *Defence Deconstructed Podcast*, podcast audio (10 Nov 2023), https://www.cgai.ca/connectivity_interoperability_and_pan_domain_command_and_control

[25] Paul Mcleary, "NATO is losing patience with one of its own members – and it's not who you think," *Politico* (8 Jul 2024), https://www.politico.com/news/2024/07/08/nato-summit-canada-commitment-00166648

[26] Stephanie Carvin and Thomas Juneau, "Why AUKUS and not CAUKUS? It's a Potluck, not a Party," *International Journal* Vol 78, No. 3 (2023): 359-374, https://journals.sagepub.com/doi/10.1177/00207020231195109

Canada and Interchangeability

Underpinning the development of interoperability capabilities for the CAF is the connected issue of interchangeability. Having a commonality of systems for the CAF and its closest operational partners, particularly the U.S., will have considerable effects on its ability to enhance and maintain interoperability. Interchangeability has received growing attention among NATO militaries, as members explore attempts for multi-member procurement projects.[27] Interchangeability efforts are attractive to Canada for many reasons, it allows for sharing of equipment and systems while requiring minimal modification or adaption, which is key for joint strategic planning, reducing logistical burdens and improving operational effectiveness.

However, this growing emphasis on interchangeability may pose its own set of challenges for Canada's procurement system as well as the CAF's digitization efforts. Historically, Canadian defence procurement has maintained a preference for the Canadianization of new technologies by mandating that acquisitions have certain Canada-specific requirements in order for a contract to be signed.[28] This Canadianization preference is essentially antithetical to interchangeability efforts as it prevents the rapid acquisition of equipment that is already in use by allies.

Further, the prioritization of interchangeability with allies tacitly implies that Canada will likely only be able to buy new equipment and systems from a smaller circle of suppliers, and in turn, those suppliers are highly likely to mostly be based in the U.S. This also applies to situations where FVEY, NATO, or NORAD considerations are a driver of interchangeability given the leadership role of the U.S. in each alliance. Following this path, Canada may find itself in a situation where it is only able to procure certain new pieces of equipment or systems from U.S. based firms which has the potential to clash with preexisting Canadian government policy.

Defence procurement in Canada is shaped by a number of governmental concerns and priorities that go beyond just military effectiveness of the equipment in question. Technological procurement in Canada is partly guided by the Industrial and Technological Benefits Policy (ITB) and its value proposition guide. The ITB outlines several broader considerations to ensure that defence procurement decisions yield economic benefits for Canada. Other ITB considerations include the impact on Indigenous communities, carbon reduction, and the incorporation of a gender-based analysis plus (GBA+) assessment, among other things. If Canada aggressively pursue interchangeability efforts that leads to relying on U.S.-only producers, it may find it difficult to meet some ITB objectives, particularly if cooperative acquisition models like the Joint Strike Fighter Partnership are used. This may have considerable implications for Canadian industry, as the government will need to account for what to do with Canadian firms that may lack U.S. connections on certain procurement projects. Overall, preexisting government policy and procedures are seemingly at odds with efforts to enhance military interchangeability, suggesting further reforms may be required to adjust to these new complexities. Interoperability needs to be a central concern of any defence industrial strategy as it provides focus for investments and

[27] John A. Tripak, "US and Partners Now Moving Towards Interchangeable – Not Just Interoperable – Weapons," *Air & Space Forces Magazine* (30 Sep 20222), https://www.airandspaceforces.com/us-and-partners-now-moving-toward-interchangeable-not-just-interoperable-weapons/
[28] Kim Richard Nossal, *Charlie Foxtrot: Fixing Defence Procurement in Canada* (Toronto: Dundurn, 2016), 93.

related activities. This can ensure that allies have more effective standardization of related equipment and technology while narrowing capacity and capability gaps.

Looking Ahead

To be successful at achieving effective military interoperability and interchangeability, the Canadian government must make several key decisions. Firstly, Canada must decide where and with who it wants to focus its interoperability efforts. While the U.S. will always remain Canada's most important partner, shifting focus to the Indo-Pacific may require placing greater emphasis on newer allies like Japan and South Korea. Canada lacks an extensive history of working with these partners, making it necessary to expedite efforts in aligning deeper cooperative relations. Building interoperability will always face challenges, particularly with partners with whom Canada has limited operational experience, as well as limited working-relations on defence technological development. Anything with the U.S. will require information technologies as the primary focus for new investments. This is evident with recent NORAD Modernization efforts, which have included the acquisition of new Cloud Based Command and Control (CBC2) systems. Regardless of where and how Canada decides to prioritize its investments, it will likely still be doing so as a junior partner and must understand that it needs to convince the other members that it has accepted its fair share of the burden, which will involve a mix of government messaging as well as tangible defence investments. This convincing means that Canada will need to demonstrate that its own interests and capabilities have aligned with its partners for a common purpose. The federal government also likely will need to communicate more directly with the Canadian public at the domestic level to explain the importance of these investments, and potentially strengthen the ability to shift further resources to national defence which can then help expediate the overall process.

Too often, defence goals outpace technological acquisitions and wider organizational transformation, and thus must be avoided to keep on track with building interoperability capabilities. As the CAF and Department of National Defence (DND) update existing strategies and plans that will guide its various technological modernization efforts, they must include clearly defined top-down strategic guidance to keep interoperability related changes focused on achievable goals that also outlines various success benchmarks for the different stages of the process.

The DND and CAF will need to continue to work with its allied counterparts in harmonizing requirements for technological investments, while also collaborating on co-research, development and procurement efforts. This coordination can take the form of conferences for senior officers; conferences for relevant industry stakeholders to interact with defence officials; as well as formal agreements on interoperability related matters. Increased dialogue between Canada and its partners can help to more clearly and accurately identify where interests algin, and how complimentary and niche capabilities can be developed and prioritized. Further, constant dialogue can ensure that data relevant systems and architecture are constructed in a way

that can be accessed and utilized by multiple partners, thus avoiding constraining issues with security access and compatibility. Overall, Canada's allies are a potential key resource to learn more about best practices which can lead to considerable savings in time and resources by preventing Canada from repeating the errors of others.

Canada may also need to change the way it approaches technological upgrades to achieve interoperability with the U.S. and its closest allies. As current interoperability efforts are often centred on digital technologies, Canada can no longer afford to approach modernization efforts via a periodic and ad hoc manner. Canadian defence will need to update its systems and kit consistently in tandem with its allies to avoid losing connectivity and by extension interoperability. For example, if the U.S. decides to update its digital networks and Canada fails to follow, Canada may find itself on the outside looking in, and have many existing defence efforts such as NORAD modernization significantly disrupted. This new approach will need to be built into the early planning stages of any major procurement and accounted for in the contracting of those systems.

Interoperability is rapidly changing as digital technology advances, which means flexibility and comfort with digitization will be a core necessity. A CAF that is digitally inclined will be better suited to respond to the inevitable challenges that are encountered from the organization's information technology driven interoperability efforts. Senior leaders will need to embrace the recruitment and promotion of personnel suited to this digital challenge, meaning that a future CAF officer corps will likely need to further diversify to fulfill the multiple technological challenges that the CAF will face in the years to come. CAF doctrine, educational institutions, and training material will need to be continuously updated to reflect the shift towards digitization. Further, the CAF and DND may need to offer greater financial incentives or other benefits in order to attract technologically inclined potential recruits and avoid losing them to the private sector.

Canada also needs to better communicate with industry to help those in the private sector better understand the strategic challenges that the CAF is trying to overcome. By forming new partnerships and working closer with industry, the government can potentially leverage the private sector to solve many of the technical problems that will be encountered as interoperability efforts are developed further. There will be certain constraining factors that will need to be addressed for the information technology industry in Canada to participate more deeply in national defence, which includes ensuring that appropriate security requirements are in place to meet the military's standards. Industry will also need to be encouraged to prioritize the development of digital open interfaces and architectures that can be adjusted as new strategic requirements emerge, and to move away from prioritizing proprietary offerings. Smaller firms, which are common in the Canadian information technology sector, should be given more opportunities to participate with defence contracts. In general, interoperability is a challenge that cannot be overcome by only the government, industry will need to play a key role in allowing the CAF to gain the capabilities it needs to partner with allies abroad.

Recommendations

- Continue to prioritize interoperability efforts with the U.S., focusing on digital and information technologies.
- Newer partners in the Indo-Pacific should also be prioritized when developing interoperability efforts.
- Implement clear top-down strategic guidance in DND and CAF modernization plans, including defined success benchmarks for interoperability.
- Collaborate closely with allied counterparts on harmonizing technological requirements, co-research, development, and procurement efforts, as well as shared lessons-learned related to interoperability.
- Ensure consistent and planned technological upgrades in tandem with allies to maintain connectivity and interoperability; this includes integrating these needs into early procurement planning.
- Promote and recruit personnel with strong digital and technological skills; while updating CAF doctrine, education, and training to reflect the shift towards digitization.
- DND/CAF must foster partnerships with the private sector, encouraging the development of digital open interfaces while ensuring appropriate security measures are in place.
- Enhance communication with the Canadian public to explain the importance of defence investments and potentially increase funding for national defence.

About the Author

*Dr. **Alexander Salt** has a PhD from the University of Calgary's Centre for Military, Security and Strategic Studies and an MA in Political Studies from the University of Manitoba. His dissertation explores to what extent has the battlefield experience of the U.S. military influenced post-war organizational innovation. His research has been awarded the Social Sciences and Humanities Research Council of Canada's Joseph-Armand Bombardier Doctoral Award, as well as a General Lemuel C. Shepherd, Jr. Memorial Dissertation Fellowship. He has published research relating to international security and defence policy with Strategic Studies Quarterly, Journal of Military and Strategic Studies, Canadian Foreign Policy Journal, and The Canadian Network for Research on Terrorism, Security, and Society. Previously, he was a Visiting Political Science Instructor with Macalester College and has also held positions with the Centre for Defence and Security Studies, as well as the Consulate General of Canada in Dallas, Texas, and the Consulate General of Canada in Minneapolis, Minnesota.*

Canadian Global Affairs Institute

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

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

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