DAIO Defense AI Observatory

When the Teeth Eat the Tail

A Review of Canada's Defence Artificial Intelligence

Robert C. Engen

DAIO Study 23|09

Ein Projekt im Rahmen von
dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

About the Defense AI Observatory

The Defense AI Observatory (DAIO) at the Helmut Schmidt University in Hamburg monitors and analyzes the use of artificial intelligence by armed forces. DAIO comprises three interrelated work streams:

- Culture, concept development, and organizational transformation in the context of military innovation
- Current and future conflict pictures, conflict dynamics, and operational experience, especially related to the use of emerging technologies
- Defense industrial dynamics with a particular focus on the impact of emerging technologies on the nature and character of techno-industrial ecosystems

DAIO is an integral element of GhostPlay, a capability and technology development project for concept-driven and AI-enhanced defense decision-making in support of fast-paced defense operations. GhostPlay is funded by the Center for Digital and Technology Research of the German Bundeswehr (dtec.bw).

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

When the Teeth Eat the Tail

A Review of Canada's Defence Artificial Intelligence

Robert C. Engen

DAIO Study 23|09

Ein Projekt im Rahmen von

dtec.bw

Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

About the Authors
Dr Robert C Engen is Senior Lecturer in War Studies at Deakin University, working in professional military education at the Australian War College in Canberra and convening units on contemporary trends in warfare and high-end conflict. He was previously an Assistant Professor of Defence Studies at the Canadian Forces College, and a post-doctoral fellow and faculty member in the History Department of the Royal Military College of Canada. An historian by training, he has written two monographs and an edited volume on the human dimensions of warfare, and recently co-wrote a groundbreaking graphic history with Dr Matthew Barrett: *Through Their Eyes: A Graphic History of Hill 70 and Canada's First World War*. He is actively researching the intersection of the human dimensions of war and the inhuman dimensions of artificial intelligence. His Twitter account is @RobertEngen.

Acknowledgments
Great thanks are owed to Dr Allan English (Queen's University), Charlotte Duval-Lantoine (Canadian Global Affairs Institute), Tindur Sigurdarson (Queen's University), and Major Stephen Paish (Canadian Army) for valuable comments and suggestions. Brigadier-General Dave Yarker and his father, Colonel (ret'd) Rick Yarker, gave generously of their time and knowledge. Alexandre Jouan (DRDC) also provided a draft copy of the Canadian DND *AI Strategy* that completed this analysis, and DRDC okayed the citation of this important draft document. The author is solely responsible for any errors in fact, analysis, or omission.

Design
Almasy Information Design Thinking

Imprint
When the Teeth Eat the Tail: A Review of Canada's Defence Artificial Intelligence. DAIO Study 23/09 (Hamburg: Defense AI Observatory, 2023)

Defense AI Observatory | Chair of Political Theory | Helmut Schmidt University
Holstenhofweg 85 | 22043 Hamburg | T +49 40 6541 2776
www.defenseai.eu | contact@defenseai.eu | @Defense_AIO

ISSN (online): 2749-5337
ISSN (print): 2749-5345

Content

1 Summary

Canada is in trouble when it comes to defence artificial intelligence (AI). Although the country is well-placed globally for AI research, development, and funding, its Department of National Defence/ Canadian Armed Forces (DND/CAF) are badly positioned to embrace digital transformation – including artificial intelligence systems. This is a consequence of the organization's structure, its history, and its culture rather than any technical shortcomings. The consistent privileging of operations and the "teeth" of the organization and the denigration of its "tail" support functions has meant that DND/CAF information management system has been a disaster for more than two decades. Both internal and external agencies have recently flagged critical shortcomings in information management, procurement, personnel, and professionalism in DND/CAF as major roadblocks to wide-scale implementation of defence AI.

There has been a substantial amount of theoretical work done on defence AI, and the Canadian military organization has, to greater or lesser degrees, already undertaken much of the necessary intellectual heavy lifting for how to approach AI. A comprehensive DND/CAF *Artificial Intelligence Strategy* exists in draft form. There are many Canadian initiatives related to defence AI under development, and DND/CAF has solid mechanisms for funding and nurturing AI projects in partnership with academia and industry. But most of these initiatives must be small in scale to circumvent the larger, highly dysfunctional defence procurement process in Canada. The decentralized organizational siloes mean that AI development, funding, and operation happen in isolation and without horizontal connections to the rest of the organization. There are also serious

unanswered questions about how AI will be governed within DND/CAF. Defence AI systems are finding limited operational and business application in the Canadian military establishment. However, present existential issues related to procurement and personnel are likely to throw these efforts into disarray. Short of major structural and cultural change within DND/CAF, it seems extremely unlikely that Canada will be able to make meaningful steps towards large-scale implementation of defence AI this decade.

2 Thinking About Defence AI

Canada's Department of National Defence / Canadian Armed Forces (DND/CAF) are not well-prepared for defence artificial intelligence at scale. Many of the barriers to adoption come from how the Canadian military, as an institution, thinks. Organizational and cultural trends, rather than technical limits, are likely to determine Canada's trajectory in this field.

The Department of National Defence (DND) is the civilian arm of Canada's federal public service related to defence. The Canadian Armed Forces (CAF) are the country's uniformed military services. The "Defence Team" refers to both DND and the CAF, and the two halves are integrated in some ways. However, as a recent external review of the organization conducted by Justice Louise Arbour revealed, "even as part of the Defence Team (…) the CAF remains insular, closed, self-confident, persuaded of the merit of its methodolog[ies], and rarely exposed to the broader civilian organizational culture."[1] The present system of organization within the Defence Team is referred to informally as the "Level 1" or "L1" system. The head of each of the L1s reports directly to the two "Level 0s": either the uniformed Chief of the Defence Staff (CDS), or to the civilian Deputy Minister (DM) of National Defence, and, in a few cases, to both. L1s are led either by a senior military officer or a civilian assistant deputy minister. Some of the L1s' responsibilities cut across wide areas of responsibility (such as Materiel and Real Property). However, all L1s are answerable only to the CDS or DM, and behave in self-directed manners, with authority flowing hierarchically from the top. The L1 system can charitably be characterized as "federated," and more accurately as "balkanized." In the past the CDS has exerted strong central control over the L1s, but this control has weakened in the last decade.

2.1 "Records-Keeping Bedlam": Historical and Cultural Background to Defence AI in Canada

Two historical developments heavily influenced how the DND/CAF thinks. First, the transformation from three services to one service (unification) in the 1960s had the long-term effect of creating organizational balkanization. Second, drastic budget and personnel cuts beginning in the 1990s destroyed much of the organization's collective memory and left it without a solid basis for digital information management. These two aspects, in combination with an overemphasis on mission success and a system that rewards job mobility have created an almost totally

1 Arbour, Report of the Independent External Comprehensive Review of the Department of National Defence and the Canadian Armed Forces, p. 16.

dysfunctional organizational setup that seriously undercuts the ability of Canada to exploit the potential of defence AI.

The first development, unification, was a 1960s program to transform Canada's three military services (the Royal Canadian Air Force, the Royal Canadian Navy, and the Canadian Army) into one, unified service containing different subordinate Commands. Ironically, after dispensing with the three "strong services," unification created the dozens of entrenched, semi-autonomous, highly siloed organizational entities – the "Level 1s" (L1s). Each L1 pulled decision-making authorities together at the top of their own silo to ensure control and away from both subordinate elements and from enterprise-wide organizations.[2] The way that data and information management are handled within the Department of National Defence today – that is to say, poorly – is a consequence of this history. The L1s all operate semi-autonomously and have different data requirements, separate IT systems, and independent procurement processes.[3] As of 2019, the civilian Assistant Deputy Minister (Information Management) (ADM(IM)) "provides IM direction, procedures, and enterprise tools, [but] each L1 is responsible for implementing IM plans and activities within their respective operational areas."[4] The main common ground from an IM perspective is that each L1 still must meet base requirements set by the Treasury Board, which they often do not.

The second development was the significant budget cuts and reductions in personnel costs during the 1990s. The 1994 Defence White Paper reduced the size of Canada's Regular Forces by 32 per cent, from 89,000 to 60,000 as part of the Forces Reduction Program (FRP). The FRP reduced personnel and resources assigned to headquarters and support functions by 45 per cent to maximize the "teeth" of the organization – the operational elements – at a time in the mid-1990s when the tempo of CAF operational requirements was high.[5] The cuts fell disproportionately on the "tail" of the organization: the support services and headquarters. As Canadian historians wrote over two decades ago, "In the relentless paring of military personnel in the [CAF] and civilian staff in [the Department of National Defence], inevitably many of the first positions to go have been the information handlers such as clerks, secretaries, archivists, and librarians," who the FRP deemed over-staffed and expendable in comparison to operators. These people constituted the record-keeping and information management backbone of Canada's defence establishment. The well-disciplined Cold War analog record-keeping systems disintegrated just as digital technology became widespread, and the FRP reduced personnel before IM tools were in place to support smaller staff.[6]

2 Author Correspondence with LGen R. Crabbe, December 13, 2022.
3 Department of National Defence, The Department of National Defence and Canadian Armed Forces Data Strategy, p. 29.
4 Chief Information Officer, Defence Information Management Plan, p. 8.
5 Chief Review Services, NDHQ 99. Vol 1, p. 1.
6 Chief Review Services, NDHQ 99. Vol 3.

Email and instant messaging bypassed the crumbling centralized record-keeping system and aggravated the problem, and DND/CAF left its best practices behind.[7] By 2001, observers described the situation as a state of "records-keeping bedlam."[8] As a direct result of these trends, the CAF effectively has no single centralized record-keeping system, and its inability to manage its own information has been the source of serious scandals and malpractice for three decades.[9]

These historical developments have created path dependencies, aggravated by the major features of Canada's military culture.[10] One of the basic assumptions of the Canadian Armed Forces is the idea of "operations primacy" or "mission first": that mission success should receive priority over everything else.[11] This assumption comes from a long tradition of orientation towards mission effectiveness, but the new CAF professional ethos, *Trusted to Serve* (2022), reaffirmed operations primacy as a professional expectation.[12] In the Canadian experience, this expectation has sometimes promoted a "get-it-done" mentality, privileging mission efficiency and accomplishment over personal wellbeing, and even accepting a degree of wilful disobedience so long as operational results are achieved.[13] The concept of operations primacy is important for any military to function, but in Canada there is strong cultural pressure to have *every* mission be no-fail.[14] Indeed, Justice Louise Arbour's 2022 external review of the CAF noted that, "The long-established way of doing business in the CAF is anchored in operational imperatives that are often nothing more than assumptions."[15]

The basic assumption of operations primacy has a long pedigree in Canadian history, dating back to the end of the Second World War.[16] It has sometimes been illustrated using the biological metaphor of "teeth and tail," imagining the CAF as an animal whose fighting arms are the "teeth," while the supporting functions of the organization are the "tail." The metaphor lionizes the deployable, operational fighting "teeth" of the organization, while denigrating and even vilifying the supposedly non-essential "tail." The metaphor justifies cuts to particular "tail" areas (headquarters, administration, record keeping, data analysis, etc.) and assumes that it is always preferable to cut the "tail" of the CAF instead of its "teeth." "We

7 Lizotte, Learning to Swim in a Sea of Information, p. 7.
8 English/Brown/Johnston, Are We Losing Our Memory?, p. 479.
9 Desbarats, Somalia Cover-Up, pp. 59.70; Sharpe, Executive Summary – Board of Inquiry – Croatia; Sabry, Torture of Afghan Detainees, p. 33; Berthiaume, "Head of Sexual Misconduct Response Centre Says Complaints against Military Brass Are a Sign of Progress"; Arbour, Report of the Independent External Comprehensive Review of the Department of National Defence and the Canadian Armed Forces, pp. 54–55.
10 Department of National Defence, Canadian Armed Forces Ethos: Trusted to Serve, p. 53; Schein/Schein, Organizational Culture, chapter 1.
11 Hansen, "The Canadian Armed Forces Are Heading for a Titanic Collapse."
12 Department of National Defence, Canadian Armed Forces Ethos: Trusted to Serve, p. 33; Leslie, Report on Transformation 2011.
13 Rozema-Seaton, "BOXTOP 22: The Cost of Focusing on an Operational Culture," p. 15.
14 Paquet, Culture Change: Should People First Trump Mission First?, pp. 9-10.
15 Arbour, Arbour Report, p. 9.
16 Burns, Manpower in the Canadian Army, 1939-1945.

are going to have to reduce the tail of today while investing in the teeth of tomorrow," wrote Canadian Army Commander Lieutenant-General Andrew Leslie in a much-cited 2011 report that was the capstone on one of the CAF's failed transformation efforts.[17] The logic of the teeth and tail is purely that of operations primacy. It is a faulty metaphor. No higher animal consists only of teeth and tail; biological organisms are complex systems of systems, the most important of which is the guiding intelligence in the central nervous system. As historian Allan English has asked, "Is it better for the animal to lose a tooth or two, or a significant part of its brain?"[18] In other words, as noted by Commodore Hans Jung, a former Surgeon General of the CAF, major cuts to the "tail" of the armed forces (including health services, administration, and data analysis) are actually cuts to "key strategic enablers" that allow everything else to function.[19]

Operations primacy as a basic assumption is understandable within the CAF's context and history. Unlike the United States, where the armed services all wield significant political clout and enjoy relative independence, the CAF has little independence and almost no ability to shape political decision-making or strategy.[20] The ability to complete those missions assigned to it in a superb fashion is a protective mechanism for the CAF: everyday government and public indifference to the military is so great in Canada that any mission failure might become existential as an excuse for new rounds of cuts. However understandable it is, the primacy of operational requirements has important consequences related to defence AI. These are discussed further in chapters 5.2 and 7.

Another, closely related, basic assumption underlying the CAF is the value of job mobility. The CAF suffers an organizational "addiction to mobility," and likes key people, particularly leaders, to move jobs every two to three years.[21] The CAF's rewards system is performance-based, and privileges breadth and variety in postings over the development of expertise or depth. Promotions in the CAF hinge upon achieving short-term goals rapidly and then moving on, and the system has inadvertently rewarded dysfunctional behaviour as well as desired behaviour.[22] The cultivation of technical or administrative expertise in the CAF is not part of a career path that typically leads to promotion, and those who stay "geo-locked" in locations or jobs for extended periods forfeit promotion.[23]

17 Leslie, Report on Transformation 2011.
18 English, Sex and the Soldier, pp. 202-203.
19 The Canadian Press, "Military Planned to Cut Health Services, Documents Show."
20 English, Understanding Military Culture, pp. 88-89.
21 Wakeham, Career Management Modernization; Arbour, Report of the Independent External Comprehensive Review of the Department of National Defence and the Canadian Armed Forces, p. 257.
22 English, "Corruption in the Canadian Military?," p. 37.
23 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 22; English, "Enabling Innovation in Canada's Army," p. 11.

The historical problems faced by Canada's military have, since at least the 1990s, created a culture with some toxic characteristics.[24] There are substantial barriers that the culture also creates for the adoption of defence artificial intelligence. Operations primacy means that those elements of the CAF that are immediately deployable on operations, and specifically those that fulfil direct combat functions, are the most highly privileged in the organization's cultural esteem. The system is set up to reward people and perpetuate structures that are operationally focused. The CAF is addicted to job mobility among its personnel and demands the willingness to move jobs constantly to meet short-term imperatives. Technical and administrative expertise are under-privileged, or are filled with non-permanent public servant positions.

These historical developments and cultural traits have serious implications for defence AI in Canada. Canada's DND/CAF is probably two decades behind where it needs to be on information management, which is a critical part of defence AI. DND introduced solutions that IT managers proposed for digital record-keeping in the CAF – such as an Electronic Document and Records Management System – a decade late, and did not implement it enterprise-wide.[25] Powerful digital tools are available enterprise-wide, but often user training and instructions are not, and key information managers within the L1 entities are typically double-hatted from other jobs rather than being dedicated specialists. The decentralized nature of the DND/CAF hierarchy, and the hodgepodge way IT systems developed in each silo in the 1990s, has left each L1 managing its own systems. In 2012 the ADM(IM) authorized the L1s' different Records, Documents, and Information Management Systems, the Document Management Control System, and network-shared drives all as authorized repositories for data storage and management. This disparate set of applications "limits access, collaboration, and bloats the departments' IT expenses. At the strategic level, it has led to significant challenges in applying common practices for IM that can be rolled out across the enterprise."[26] A few enterprise-wide IM systems exist for critical components of DND business, but other areas of the information ecosystem are effectively ungoverned, with networked shared drives, websites, SharePoint instances, mail servers, and document repositories holding huge volumes of disorganized content. "The result," writes one CAF IM officer, "is an information environment which is untrustworthy, inefficient, that frustrates users, and limits the value the DND/CAF can glean from its own information."[27]

24 Duval-Lantoine, The Ones We Let Down.
25 English/Brown/Johnston, "Are We Losing Our Memory?", p. 478.
26 Lizotte, Learning to Swim in a Sea of Information, p. 18.
27 Ibid., p. 2.

Because of its structure, culture, and lack of internal coherence, DND/CAF has never developed holistic ways to capture data within its institutional memory.[28] A 2022 Centre for International Governance Innovation report noted that, "Canada has no enterprise-wide architecture for managing military digitalization across DND/CAF."[29] The 2019 DND/CAF *Data Strategy* highlighted similar organizational problems: the inability to make decision about data, ineffective data management practices, unwillingness to share data between L1s, lack of trust in data, inflexible legacy systems, low data literacy, and the lack of a data culture.[30] The balkanized L1 system is particularly problematic. A DND/CAF draft AI strategy from 2022 confirms that present AI initiatives within DND/CAF are fragmented between L1s, with each element proceeding independently with its own limited plans, and with no roadmap for moving the organization towards coordinated investment or governance. These problems must be addressed with culture change, as there is no culture of "working horizontally" among L1st at DND/CAF. However, the current structure, processes, and incentives are working against the necessary changes.[31] In its 2022 digital strategy, the Canadian Army correctly described the current era in DND/CAF as an ongoing "digital winter."[32] And external reviewer Louise Arbour wrote, "Ideally, a more thoughtful approach would ensure that the sum of each organization's data represents the whole picture … with the current silo model focused on achieving individual organizational mandates, this is simply not possible."[33] There remains no holistic, end-to-end ownership of data within DND/CAF and limited grounds for digital jointness. These are, in sum, major limiting factors for the implementation of AI systems at scale in Canada's defence establishment.

To return to the "tooth-and-tail" metaphor: when confronted with the choice of what to cut, the DND/CAF "animal" has historically preferred lobotomy to dentistry, shedding brain matter rather than risk losing "teeth." This attitude presents a variety of barriers for defence artificial intelligence. The basic prerequisites for understanding, developing, and fielding AI systems at scale, by DND/CAF's own reckoning, include research and development, agile project management, software (and those who use it) as an essential capability equal to hardware, massive investment in digital infrastructure and information management, and application development across the enterprise.[34] These are all functions that will normally and derogatorily be lumped in with the "tail."

28 English/Brown/Johnston, "Are We Losing Our Memory?," p. 473.
29 Araya, Artificial Intelligence for Defence and Security, p. 9.
30 Department of National Defence, The Department of National Defence and Canadian Armed Forces Data Strategy, p. 6
31 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy.
32 Canadian Army, Modernization Vital Ground, p. 12.
33 Arbour, Report of the Independent External Comprehensive Review of the Department of National Defence and the Canadian Armed Forces, p. 52.
34 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, pp. 6-7.

In 2022, Madame Louise Arbour's external review of DND/CAF discussed the organization's approach to problem solving, emphasizing why it rarely succeeds when dealing with "wicked" complex problems:

> Every problem must have a solution. The solution must be immediate and actionable. It matters little whether it actually fixes the problem, particularly if the problem is ill-defined and poorly understood, not unlike culture change. The response is a flurry of activities usually consisting of making lists, charts, inventories, and PowerPoint presentations, as well as enacting new orders, policies, and directives on top of an already complex structure … [but] the CAF leadership seems to have been incapable of examining which aspects of its culture have been the most deficient. In none of the initiatives it has launched, is there a single reflection on whether its insular, hierarchical structures may have facilitated the [problem] … Rather, the focus has been on mapping steps, pathways, and activities.[35]

The AI problem for DND/CAF has the characteristics of a wicked problem that will resist all simple technical solutions. Making the most of AI and ethical autonomy requires major structural and cultural changes within Canada's armed forces, particularly in how service members are rewarded. As it stands, there is little real appetite for change, because the reward system encourages carrying out a flurry of activities, or "doing spectacular things of small substance."[36] The changes necessary to develop the potential of defence AI are not small.

2.2 What Canada Says It Thinks About AI

At least on paper, the Canadian defence establishment is taking the uncertainties of emerging technology seriously. This begins at the top, with Canada's 2017 defence policy, entitled *Strong, Secure, Engaged (SSE)*, which enshrines many of its formal military aspirations for the future.[37] The CAF's environmental L1s (land, air, maritime, SOF) have also put thought into the future of artificial intelligence, though the degree to which this thinking has occurred, and the degree to which it has been made public, varies considerably. An overview of the thinking about AI systems on the part of the Canadian Army, Royal Canadian Navy, Canadian Special Forces Command, and the Royal Canadian Air Force follows.

35 Arbour, Report of the Independent External Comprehensive Review of the Department of National Defence and the Canadian Armed Forces, p. 10.
36 Horn/Bentley, Forced to Change, pp. 66, 68, 71–72, 76–78.
37 Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy 2017, p. 55.

The Canadian Army has been particularly forward-thinking concerning artificial intelligence. In its 2020 *Modernization Strategy*, the Canadian Army indicated that they believed it to be their responsibility "to examine the potential of AI and machine data to transform some aspects of land operations, including exploiting data and information to produce intelligence and predictive modelling to support decision-making."[38] The Army's more recent addendum to the *Modernization Strategy*, the 2022 *Modernization Vital Ground: Digital Strategy* document, reflects recent thinking on technological drivers: "Raw data of unprecedented volumes may only be processed into tangible information via human-machine teaming," the *Vital Ground* document reads. "Automating data exploration via AI/ML [artificial intelligence / machine learning] allows commanders to process more significant amounts of information while decreasing their cognitive load." The Army also emphasizes the importance of Big Data: "This requires new procedures and processes to assure timely, reliable access to data."[39] The Army's Land Warfare Centre has written very thoughtfully on how the adoption of AI by the Army, "must proceed with caution and be informed by a realistic sense of limits … Nonetheless, if pursued and applied carefully, much of what AI offers generally aligns well with [Army] requirements."[40]

The Royal Canadian Navy's (RCN) issued its *Digital Navy* strategy in 2020. *Digital Navy* addresses a broad range of digital technologies in a general manner, including "cognitive computing capabilities like artificial intelligence and machine learning that are driving advances in automation and big data analytics." The Navy's intends to use digital capabilities to "augment and empower all members of the naval team."[41] It argues for the need to cultivate a "data-centric mindset" in the RCN, as "quality data will be a fundamental enabler of this initiative … this data-centric mindset will be key to our success going forward." The RCN stresses three categories of defence AI applications. First, Autonomous Things, which "includes a broad array of technologies including advanced robots, autonomous vehicles and intelligent agents ("bots"), which are rapidly evolving due to powerful cognitive computing capabilities." Second, Augmented Analytics, using AI to enhance the analysis of both structured and unstructured data: "The RCN has made significant progress in developing its data analytic capabilities over the past few years and will continue to do so by leveraging AI. This will be done with a view to fully exploiting our data to enable timelier and better-informed decisions." Third, AI-Driven Development, using AI in the design process for software, hardware, naval equipment, and systems: "This is an emerging application of AI that is of interest to the RCN as it has implications for naval materiel assurance,

38 Canadian Army, Advancing with Purpose, p. 51.
39 Canadian Army, Modernization Vital Ground: Digital Strategy, p. 9.
40 Priems/Gizewski, "Leverage Artificial Intelligence for Canada's Army," p. 43.
41 Royal Canadian Navy, Digital Navy, p. 6.

training provided to members of the naval team, and the tools that they use."[42] The strategy concludes with the promise to establish a Digital Navy Office "to ensure the successful execution of the RCN's digital journey … to facilitate the implementation and evolution of this initiative." Its mandate will include program alignment, communications, performance measurement, look-ahead functions, process enhancement, training, and contract vehicles.[43]

The Canadian Special Operations Forces Command (CANSOFCOM) is an independent L1 within the CAF. CANSOFCOM enjoys several privileges, which it refers to as the "3As": direct *access* to decision makers; *autonomy* as a distinct and self-reliant entity; and having the appropriate *authorities* to meet their own requirements. By leveraging the "3As" CANSOFCOM is more able than other L1s to sidestep bureaucracy. In their 2020 strategic plan, *Beyond the Horizon*, CANSOFCOM laid out its perceived relationship to technology and "innovation": "the Command will prioritize the implementation of *Gradient Ascent* – a new digitalization and data analytics initiative designed to ensure a level of competency in the digital space commensurate with what we have achieved in the kinetic space – in order to attain information dominance over adversaries on operations, while simultaneously leveraging the advantages that digital technologies provide for improving institutional efficiency and effectiveness."[44] *Gradient Ascent* is CANSOFCOM's Digital Transformation Initiative.[45] Little information is publicly available.

The last environmental command, the Royal Canadian Air Force (RCAF), has published the least on artificial intelligence. The organization's *Future Air Operating Concept* is from 2016, and recent Aerospace Warfare Centre publications offers few comments on technology and nothing specifically about artificial intelligence.[46] The *Royal Canadian Air Force Journal* published a few articles related to AI between 2019 and 2022, but most of the RCAF's work on AI is being done outside of the public eye.

In all cases where they have adopted explicit stances on AI, DND/CAF entities have maintained a commitment to keeping humans "in or on 'the loop'" when it comes to decision-making, i.e. not allowing fully autonomous offensive weapon systems that "complete the loop" and offensively engage without human oversight. Attempting to ensure that combat remains an activity featuring meaningful human involvement is one of the cornerstones of Canadian AI thinking.[47] The CAF's most-used leadership framework for the past two decades, the

42 Ibid., p. 14.
43 Ibid., p. 17.
44 Canadian Special Operations Forces Command, Beyond the Horizon, p. 31.
45 Gonthier, Accelerating the Canadian Army's Digital Transformation, p. 6.
46 Goette, Preparing the RCAF for the Future.
47 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 7.

Pigeau-McCann Model, explicitly deals with "cybernetic control" systems involving some degree of autonomy as being feedback mechanisms, fundamentally lacking the properties of command.[48] There are also the beginnings of internal military discussions on developing a professional code of ethics and policy for AI in Canada.[49] The recently-formed Directorate Gender and Intersectional Analysis has also been involved with early efforts to bring what the federal government calls a "Gender-Based Analysis Plus" (GBA+) perspective to cyber, information management, and artificial intelligence capabilities in the CAF.[50]

48 Pigeau and McCann, "Re-Conceptualizing Command and Control," p. 54.
49 Wasilow/Thorpe, Artificial Intelligence, Robotics, Ethics, and the Military: A Canadian Perspective, p. 11.
50 Department of National Defence, "Gender-Based Analysis Plus."

3 Developing Defence AI

Canada represents a potentially rich site for AI research and development, and for decades the country has been a locus of AI work. Some of the seminal work in the field (backpropagation and convoluted neural networks) came from academics at Canadian universities. A recent report from the Centre for International Governance Innovation described Canada's AI strengths: "a strong AI talent pipeline, including 47 higher education institutions offering AI-specific programs and/or courses, and world-class AI institutes serving as anchors for future development."[51] In 2017, the Government of Canada announced that the Canadian Institute for Advanced Research (CIFAR) would administer a $125-million CAD Pan-Canadian Artificial Intelligence Strategy (PCAIS) for research and talent. The PCAIS invests in creating research hubs and recruiting AI researchers globally; since 2017, 113 Canada CIFAR AI Chairs have been established at institutes in Edmonton, Toronto, and Montreal, and over 200 Master's and PhD students graduate annually from these three institutes. Canadian researchers have produced the seventh most academic research publications on artificial intelligence in the world as of 2021. However, despite its prominent place in AI research output, Canada only holds about half a per cent of the world's nearly one million AI-related patents. The rate of such patents in Canada is also dropping sharply.[52] Further, between 2018 and 2022, one-third of identified Canadian AI firms either permanently closed or were acquired by foreign firms.[53] Canada hemorrhages its AI talent to American tech firms as fast as it can develop new talent.

The main L1 within the Canadian defence community that is working on AI technologies today is Defence Research and Development Canada (DRDC). DRDC's role within Canada's Defence Team is to provide leadership and advice on issues of defence science and technology, to engage and collaborate with a network of domestic and international partners, and to exercise functional authority to "ensure coherence of defence and security science, technology and innovation investments."[54] The organization therefore serves as the bridge between Canada's AI potential and its defence applications.

DRDC defence scientists carry out research internal to the organization on behalf of or in partnership with other L1s, and commission contract research from approved third-party vendors, sometimes working in partnership with them. The organization has invested in research related to artificial intelligence and machine learning for decades, both internally and externally, and a considerable *corpus* of relevant work associated with and funded by DRDC has accrued as a result. The main elements of this work are presented in chapter 9.2.

51 Araya, Artificial Intelligence for Defence and Security, p. 5.
52 OECD AI, "Visualisations Powered by JSI Using Data from MAG."
53 Araya, "Artificial Intelligence for Defence and Security," p. 5.
54 Defence Research and Development Canada, "Mandate."

Presently, the main route for pursuing the development of Defence AI internally to DND/CAF is through DRDC's Innovation for Defence Excellence and Security (IDEaS) program, which was also announced in 2017. The intention behind IDEaS is to establish "research clusters" that will "bring together academics, industry, and other partners to form collaborative innovative networks." IDEaS is a competitive funding model intended, in part, to bypass the cumbersome and archaic elements of the CAF's traditional procurement system (see chapter 5.2) by streamlining academic and industry technical cooperation with the military. Discussion of how IDEaS is funded will take place in chapter 5.1, but according to DRDC, about 65–70 per cent of all proposals from academia and industry for IDEaS grants each year "involve AI components."[55]

Many of the IDEaS related to defence AI are through the program's Competitive Projects funding mechanism. "The Competitive Projects element funds projects fast," according to the program website. "It advances promising technology quickly through a phased approach." It begins with up to six months of funding, after which there is an option for consideration for a further twelve months of funding at a much higher rate. After this, DND also has the option of pursuing the project further using non-IDEaS funding through S&T Solution Advancement.[56] AI is either central to, or a component of, many of the technologies being developed through the Competitive Projects. IDEaS's "Spot the Hack" challenge, issued on behalf of the RCAF, studies cyber vulnerabilities in the Military Standard 1553 bus used by RCAF aircraft avionics networks; many of the bids, including those from CAE, Palitronica, and Queen's University which received first and second-round funding, included AI and machine learning agents for intrusion detection purposes.[57]

Outside of DRDC, a potentially significant development avenues for AI is a relatively new DND program called "Mobilizing Insights in Defence and Security" (MINDS). MINDS is governed by DND's office of the Assistant Deputy Minister (Policy), responsible for the development and management of defence policy-making.[58] The program is based upon the idea that "policy- and decision-making are strengthened when assumptions are challenged and diverse viewpoints are considered." MINDS provides collaboration opportunities between DND/CAF and the academic defence and security community, allowing for bespoke briefing engagements, targeted engagement grants for projects and conferences, support for emerging scholars, a "rapid response mechanism" for addressing evolving priorities, and ongoing collaboration and engagement through Collaborative

55 Directorate S&T Strategic Partnerships, "Artificial Intelligence."
56 Department of National Defence, "Competitive Projects."
57 Department of National Defence, "Spot the Hack."
58 Department of National Defence, Mobilizing Insights in Defence and Security – MINDS: Annual Report 2019-2020, p. 9.

Networks.[59] DND has established several of these Collaborative Networks since the program began in 2019.

Only one Collaborative Network, the Security-Policy Nexus of Emerging Technology (SPNET) based out of Concordia University in Montreal, has specifically focused on artificial intelligence as an emerging policy issue. SPNET researchers focus on how public policy, defence decision-makers, and technology developers can address topics such as accountability, explainability, transparency, security and safety, fairness, privacy, ethics, human dignity and rights, inequality, economic impacts, international cooperation, and governance.[60] Since receiving their first MINDS money in 2019, SPNET has produced a significant body of briefing notes on relevant topics for DND, particularly focusing on ethical AI in defence, accountability, dual use, regulation, and privacy issues.

While SPNET has produced prodigious work on a variety of vital issues related to artificial intelligence (a list is provided in chapter 9.3), their last briefing notes were issued in November 2021, presumably with the expiration of the MINDS grant. The SPNET Collaborative Network was funded in the 2019–20 cycle of competitions but has not been renewed. No other major grants have yet been given for AI research and development through the MINDS program since.

The lynchpin of Canada's defence AI ecosystem is private interests working as contractors for DND/CAF. Given the internal problems facing Canada's military (see chapter 2.1) the importance of working with trusted AI vendors is magnified and presents many opportunities. The Treasury Board of Canada Secretariat maintains a "List of interested Artificial Intelligence suppliers" who can "provide the Government of Canada with responsible and effective AI services, solutions, and products." Federal departments can use these pre-qualified suppliers to launch streamlined procurement processes for AI technologies and services, for up to $9 million CAD before taxes. As of August 2022, there were 117 companies on the Treasury Board list, ranging from very small startups to large enterprises and public companies such as Palantir Technologies, Amazon Web Services, IBM Canada, and Microsoft Canada.[61] Chapter 9.1 shows the companies that, according to Open Government data, are both on the Treasury Board's pre-approved AI list and have contracted with Canada's Department of National Defence since 2010. Most of these contracts, particularly from large firms, are not for AI products, and not all details of contracts are publicly available.

59 Department of National Defence, "Mobilizing Insights in Defence and Security (MINDS)."
60 Security-Policy Nexus of Emerging Technology, "About SPNET: Our Work."
61 Treasury Board of Canada, "List of Interested Artificial Intelligence (AI) Suppliers."

The list in chapter 9.1 is nowhere near complete. In FY 22–23 alone there were 110 different contracts issued by DND for "Informatics Professional Services" and 74 for "Automatic Data Processing Software." The pre-approved AI vendors for AI are not the only ones who can, or will, provide these products and services to the Department of National Defence. There are definitely companies outside of this list contracting AI services to DND, but it is very difficult to obtain a full picture without conducting a full audit. Chapter 9.1 is presented here to give a sense of how approved AI vendors are interacting with DND/CAF, and what sorts of projects they have contracted. This ecosystem is interrogated further in chapters 4 and 5.2.

4 Organizing Defence AI

Canada's DND/CAF has been reluctant to commit itself to external governance standards for the use of artificial intelligence systems and is equally reluctant to propose firm internal governance models. Given the department's "federated" L1 system, the lack of governance mechanisms may simply default to each Level 1 organization within DND/CAF doing as it pleases in developing artificial intelligence applications, with little accountability.

4.1 External Governance for AI

Federal entities in Canada are supposed to be bound by the government's 2019 Treasury Board Directive on Automated Decision Making, which ensures that AI systems are used responsibly by government institutions.[62] This Directive is a (supposedly) mandatory policy instrument that applies throughout federal government departments.[63] The Directive applies to the use of all systems that make, or assist in making, recommendations or decisions. "Having a person make the final decision does not remove the need to comply with the Directive," according to a Treasury Board memo. "For example, systems that provide information to officers who make the final decisions could be in scope."[64] As part of the Directive, every department must complete an Algorithmic Impact Assessment (AIA) of an AI system prior to production, and whenever system functionality changes. The AIA assesses a system's impact based upon several factors, with impact levels varying based on the system's affect on the rights, health, wellbeing, and interests of individuals or communities, as well as sustainability, reversibility, and duration.[65] Based upon responses to risk and mitigation questions, the AIA assigns an impact rating and requires publication of the AIA on an open government transparency portal, creating a registry of automated decision systems in use by the Government of Canada.[66]

The Directive on Automated Decision Making appears robust but contains escape clauses and lacks enforcement mechanisms. The Directive applies only to "external" services of government – services offered to individuals or organizations by government – and does not apply internally within departments, a "glaring oversight" in this governance regime.[67] The team presently carrying out a periodic review of the Directive recommended expanding the scope to include internal as well as external systems. However, they also note that since the focus of the Directive is administrative decision-making, "Internal enterprise services, in which the provider and recipient are

62 Treasury Board of Canada, "Directive on Automated Decision Making."
63 Beshaies/Hall, "Responsible Use of Automated Decision Systems in the Federal Government."
64 Ibid.
65 Riley et al., "Bill C-27," p. 27.
66 Beshaies/Hall, "Responsible Use of Automated Decision Systems in the Federal Government."
67 Scassa, "Comments on the Third Review of Canada's Directive on Automated Decision-Making."

federal institutions, are unlikely to become subject to the Directive except where they specifically concern the rights, interests, or privileges of individual employees."[68]

The degree to which the Directive applies to the Department of National Defence remains uncertain, but it is clear that DND/CAF does not believe the Directive applies to it. DND/CAF's (unapproved draft) Artificial Intelligence Strategy notes that any new AI systems used by Defence should be developed and implemented "in accordance with applicable laws, policies, and guidelines."[69] However, the AI Strategy also proactively warns that, "because of their application to defence and national security, many DND/CAF use cases [of artificial intelligence] will fall outside the guidance provided by the Treasury Board Secretariat, and the gap between the development of AI and other emerging technologies and legislative and policy coverage only continues to widen."[70] The AI Strategy carefully discusses how it will be "aligned with" the Directive in considering risks without actually stating that it is subject to the Directive.[71] This disconnect already exists in practice. In February 2021, media outlets reported that DND had used two AI-driven hiring services – Knockri and Plum.io – to shortlist candidates for the department's executive ranks. These companies provided hiring managers with behavioural assessments and measurements of the "personalities, cognitive abilities and social acumen" of applicants. DND did not submit an Algorithmic Impact Assessment to the Treasury Board: a DND spokesperson said that because "final decisions" were not being made by AI, the department did not feel obliged to complete the Treasury's algorithmic assessment.[72] This excuse was neither in the spirit nor the letter of the Directive on Automated Decision Making, and it suggests two things. First, DND has yet to take compliance with existing AI governance directives seriously and will likely resist having them imposed by other parts of the federal government. Second, there needs to be more appreciation within DND that a "final decision" being made by a machine is not the only problem, nor even the primary problem, that governance structures like the Algorithmic Impact Assessments are meant to mitigate.[73] Reading between the lines, the AI Strategy signals that DND/CAF intends to chart its own path in this field.

4.2 Internal Governance for AI

The draft Artificial Intelligence Strategy does not definitively state how governance of AI will function internally to DND/CAF, though there are hints. It seems

68 Bitar/Deshais/Hall, 3rd Review of the Treasury Board Directive on Automated Decision-Making, pp. 10-11.
69 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 21.
70 Ibid., pp. 19-20.
71 Ibid., p. 21.
72 Cardoso/Curry, "National Defence Skirted Federal Rules in Using Artificial Intelligence, Privacy Commissioner Says."
73 Scassa, "Comments on Third Review of Canada's Directive on Automated Decision-Making."

likely that the federated L1 entities within DND/CAF – those that answer only to the Chief of the Defence Staff or the Deputy Minister (see chapter 2.1) – will be left to govern their own uses of artificial intelligence. The AI Strategy proposes the creation of a Defence AI Centre of Excellence for Canada to "accelerate AI experimentation and scaling across the Defence enterprise," creating a hub of AI expertise; however, it does not propose to invest it with governance responsibilities.[74] Instead, the AI Strategy argues that DND/CAF must, "Vest decision authorities for AI at the *lowest appropriate level* to encourage innovation."[75] Given how Canada's military works, that lowest appropriate level will probably mean the L1s.

The office of Assistant Deputy Minister (Data, Innovation, Analytics) (ADM (DIA)) is in one silo of DND, reporting directly to the Deputy Minister of National Defence. The office of Assistant Deputy Minister (Information Management) (ADM(IM)) and Assistant Deputy Minister (Defence Research and Development Canada)) are in a different silo, reporting to both the DM and to the Chief of the Defence Staff. On 6 December 2022, the DND announced the removal of the ADM (DIA) office as an L1. ADM (DIA) has merged with the Directorate of Knowledge and Information Management (DKIM) under the ADM (IM), to stand up the Digital Transformation Office (DTO). Effective 6 December, the ADM (IM) L1 itself is now called the Chief Information Office. Although it is still too early to see what effects these changes will have, the new DTO is charged with managing both IM and data and analytics enablement "in support of initiatives like machine learning and Artificial Intelligence."[76] DND/CAF insiders suggest that ADM (DIA) did not accomplish very much since it was established in 2017, so this reorganization may correct some of the confusing divisions over IT that have plagued the organization.

Perhaps with cross-cutting, general-purpose capabilities such as artificial intelligence systems, there is realistically nobody in Canada who can lead radical change except the "Level Zeros": the Chief of the Defence Staff and the Deputy Minister of National Defence. The AI Strategy, like the *Data Strategy* and other recent documents before it, is a strategy devolved to the lowest levels of authority. The thinking within DND/CAF may be that trying to govern AI is like trying to govern electricity, and this may prove to be the correct interpretation. However, it seems equally likely that the "balkanized" character of DND/CAF's structure means that governance and regulation of AI are such difficult questions that giving them sufficient consideration becomes problematic. The question of internal governance for artificial intelligence within DND/CAF is therefore an extremely difficult one, and there appear to be few answers at present.

74 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 15.
75 Ibid., p. 17. Emphasis added.
76 Matthews, "Message from the Deputy Minister Regarding the Digital Transformation Office."

5 Funding Defence AI

5.1 PCAIS, IDEaS, and MINDS

The Government of Canada has spent a generous amount of money to develop a thriving artificial intelligence ecosystem. The Pan-Canadian Artificial Intelligence Strategy (see chapter 3) infused $125 million CAD into AI research hubs and global talent recruitment back in 2017, and this effort was renewed in 2021 with an additional $440 million CAD over ten years, including $185 million to support the commercialization of AI in Canada.[77] While the PCAIS appears to be a strong investment in AI – with some limitations – there is no direct Defence component of this funding. Nor are defence-related applications among the Canadian Institute for Advanced Research's key strategic priorities for the Pan-Canadian AI Strategy: these are instead focused on fundamental AI science, AI for health care, AI for energy, AI commercialization, societal implications of AI, and advancing AI diversity and inclusion.[78]

If the Pan-Canadian Artificial Intelligence Strategy has little to say about defence AI, another program stood up by the Government of Canada in parallel serves as a corrective. Defence Research and Development Canada (DRDC) is the long-standing primary delivery agent for DND's science and technology investments (see chapter 3).[79] The main route for pursuing the development of Defence AI internally to DND/CAF is through DRDC's Innovation for Defence Excellence and Security (IDEaS) program discussed earlier. IDEaS amounted to an investment of $85 million CAD per year for 20 years – significantly exceeding the funding given to the Pan-Canadian Artificial Intelligence Strategy. This substantial fund is managed through the office of the ADM(DRDC).[80] There are five funding mechanisms to assist Canadian "innovators" in addressing defence issues: competitive projects up to $1.2 million CAD; "Innovation Networks" of up to $1.5 million CAD; contests on approved topics; sandboxes for field testing; and test drives for high-readiness ideas.[81] A less technical field of investment comes from the Mobilizing Insights in Defence and Security (MINDS) expert outreach program discussed earlier in chapter 3. The MINDS Collaborative Networks are particularly important, with successful applicants receiving $250,000 CAD per year for three years.

The key advantages of the IDEaS and MIDNS initiatives is that they involve large numbers of modest expenditures. In Canada, the Treasury Board has a $10 million CAD threshold for its Organizational Project Management Capacity level, meaning that a project valued less than $10 million CAD "will be exempt from

77 Advisory Council on Artificial Intelligence, Annual Report 2020-21.
78 McKeown, "Food for Thought Paper for the Deputy Minister and the Chief of the Defence Staff: Threats and Challenges of Artificial Intelligence," p. 5.
79 Department of National Defence, Science and Technology in Action.
80 Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy 2017, pp. 77–78.
81 Department of National Defence, "IDEaS: Innovation for Defence Excellence and Security."

much of the oversight and rigour" of the standard procurement system and does not need to prepare a project complexity and risk assessment for Treasury Board consideration.[82]

5.2 Procurement

The IDEaS and MINDS initiatives are vital because of the procurement context that they are attempting to escape. Canada's Department of National Defence has, for well over a decade, been effectively disabled from procuring major technological systems. This is part of the wider, slow-motion disaster that is Canadian defence procurement.[83] Seventy per cent of procurement contracts for Canada are overdue or delayed. Beginning in 2008, when significant increases in capital investment occurred, major capital projects became "jammed up" and have never gotten back on track.[84] The procurement system involves achieving concord among three different government departments; it is designed to prioritize investment in the Canadian defence industry over actually building the capabilities of the armed forces.[85] This process, devised in the 1970s for major capital purchases, is competition-based, and it is extremely difficult under current federal law to enter strategic partnerships with industry the way that the American armed services have with the US-based tech giants. It is nearly impossible to procure major capital pieces of technology in a useful timeframe in Canada.

DND's Project Approval Directive (PAD), updated in 2019, outlines the process for delivering new capabilities. According to Lieutenant-Colonel Kenneth Bedley, "the PAD follows a project process that is not conductive to digital technology and is causing a capability gap within the CAF." Bedley's recent study of the "tech gap" in Canada suggests that capability delivery in Canada is based on the "water-fall" approach to project management, where a linear flow of sequential project activities occurs, and the completion of one is necessary before proceeding to the next. Because Canada's Treasury Board deems DND a fiscally risky institution, it has forced the adoption of manufacturing industry best practices and standards on the process. All projects must follow the PAD, regardless of type. This process was designed to procure large capital assets and traditional military hardware, and with each discrete phase taking approximately 1–4 years, a project can easily take ten years to deliver from start to finish. Although the PAD has a tailored process for IT-related projects, this tailored process is burdened with even greater demands for documentation and control. According to Bedley, the average length of DND

82 Bedley, Closing the Tech Gap, p. 39.
83 Nossal, Charlie Foxtrot.
84 Fetterly, Arming Canada, p. 26.
85 Schofield, Delivering on Strong Secure Engaged, p. 1.

IT-related projects that followed the PAD waterfall model between 2011 and 2015 was 9.6 years, but some IT projects had been open for over 16 years.[86] The Treasury Board threshold between "minor projects" and "major projects" (see chapter 5.1) means that any IT, software, or hardware acquisition that exceeds $10 million CAD faces a ten-year delivery time.[87]

The PAD can bypass much of its own process when DND decides there is an Urgent Operational Requirement (UOR). The UOR process streamlines procurement to address short-term operational deficiencies, normally preferring high technological readiness level solutions (military-off-the-shelf and commercial-off-the-shelf) and is meant to address evolving threats. The UOR process proved highly successful during the Afghanistan era, and cut down on vital equipment procurement times dramatically, trading project risk to expedite delivery and receive priority over standard projects.[88] However, the UOR approval requirements "demand that the project directly affect combat operations and contribute to a life-saving capability."[89] This generally makes the UOR ideal for CAF requirements (see "operations primacy" in chapter 2) and there is likely scope for rushing tactical projects with AI components through the procurement process as urgent requirements. However, there is almost no chance that the broader digital transformation needed by DND/CAF and its L1s can be sold to the Treasury Board as an urgent operational requirement. And tactical, mission-focused UORs are going to constantly be taking priority for capability development within this system.

The draft *DND/CAF AI Strategy* cites the need to "improve the procurement process to support development and acquisition of AI" as a critical element of its plan.[90] Other entities within DND/CAF are saying the same thing. "The current capability investment paradigm uses a preponderance of rigid and lengthy major capital projects," writes the Canadian Army's Digital Strategy. "It does not enable the [Canadian Army] to benefit from a sustained technological advantage over a less-constrained adversary, nor parity with allies who benefit from more agile acquisition policies."[91]

The *AI Strategy* and *Digital Strategy* also assume that AI procurement should be a defence priority. But this is not a given and will likely require a champion at the CDS or Deputy Minister level. As now-retired General Tom Lawson, a former Canadian chief of the defence staff, said in 2013 that the "Canadian Armed Forces do not procure capabilities unless they're absolutely necessary to the attainment

86 Bedley, Closing the Tech Gap, pp. 36-38.
87 Perry, "Priorities for Canada's Air Force."
88 Department of National Defence, Project Approval Directive (PAD) (2019), pp. 175-186.
89 Bedley, Closing the Tech Gap, pp. 42-43.
90 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 28.
91 Canadian Army, Modernization Vital Ground, p. 13.

of our mandate."[92] What is "absolutely necessary" for the military is, of course, completely subjective, particularly given the CAF's "operations primacy" basic assumption. Money in DND/CAF flows towards improving tactical capabilities that allow the CAF's commands to maximize their short-term fitness for operations on the near horizon, instead of more general, longer-term, or enterprise-wide capabilities.[93] Given the myriad problems facing Canadian procurement, successfully shepherding any major capital project through the system on a non-emergency basis is extraordinarily difficult.[94]

92 Brewster, "More than a Decade Ago, the Army Had a Plan to Rebuild. It Went Nowhere."
93 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 16.
94 Brewster, "More than a Decade Ago, the Army Had a Plan to Rebuild. It Went Nowhere."

6 Fielding and Operating Defence AI

At present there are not many instances available in the unclassified realm of defence AI systems being fielded and used within DND/CAF. Most projects are still being researched, under development, are being tested, or are finding limited tactical or business applications.

A few defence AI initiatives are underway, as detailed in Canada's Open Government procurement site. The Goods and Services Identification Number (GSIN – an alphanumeric code used to categorize goods and services) for Artificial Intelligence in Canada's procurement system was introduced several years ago but has been used by the Department of National Defence only a handful of times amidst its tens of thousands of tenders. The most recent ones issued under that GSIN were published in FY 2021–22 (none have been issued yet in 2022–23). These included a $1.277 million CAD contract for "artificial intelligence / inference systems (R&D)" awarded non-competitively to IMRSV Data Labs in Ottawa on 13 December 2021.[95] No tender description was available. However, IMRSV advertises their Defence Suite of products as "a modern AI-enabled platform that enables all contributors to the intelligence cycles to make confidence decisions with data they trust," and products such as their "Anvil Crucible" use machine learning to automate data analysis tasks such as establishing relationships between entities, identifying trends, and making predictions for key variables.[96] The other major recent contract specifically for AI was issued by DRDC, which put out a tender asking for bidders to help "establish a technology exploitation mechanism for DRDC and DND to draw upon applied [machine learning] engineering and scientific support services. The objective of this work is to conceive, develop, test, optimize, and implement all components of custom [machine learning] solutions."[97] The contract for this tender opportunity was ultimately awarded to two firms: MDA Systems out of Richmond, British Columbia for $1.6 million CAD, and Thales Digital Solutions out of Montréal for $1.8 million CAD.[98] None of these, to date, have completed a Treasury Board Algorithmic Impact Assessment (see chapter 4.1).

Other AI systems or components of systems are being procured by DND under other GSIN labels: particularly the "Automated Data Processing (ADP) Software" category, "Informatics," and "Algorithms." But they are not being specifically flagged as artificial intelligence or machine learning procurements. The small Plum.io contract mentioned earlier in this report (see chapter 4.1) was awarded under the "Other Research and Development" GSIN code related to "Real Time

95 Department of National Defence, "Artificial Intelligence/Inference Systems (R&D), Contract #W8487-220165/001/SC, Awarded to IMRSV Data Labs Inc."
96 IMRSV Data Labs, "Our Products: Anvil Crucible Defence Suite."
97 Department of National Defence, "Arti. Intell & Mac. L. R&D Services, Solicitation #W6399-19KH95/B."
98 Department of National Defence, "Arti. Intell & Mac. L. R&D Services, Contract #W6399-19KH95/001/SL, Awarded to Thales Digital Solutions Inc.;" Department of National Defence, "Arti. Intell & Mac. L. R&D Services, Contract #W6399-19KH95/002/SL, Awarded to MDA Systems Ltd."

Analysis," and its original tender opportunity has not been made public.[99] It is likely, given the scrutiny that "artificial intelligence" systems are coming under, that we will see more procurements of AI systems fall under banal categories such as "Informatics" and "ADP Software" in future. DND has stopped contracting services under the AI GSIN code altogether as of this writing.

Operations primacy continues to shape Canada's priorities for investment. In its recent *Modernization Strategy*, for instance, the Canadian Army decided to prioritize the modernization of their operational C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance) capabilities, while putting off the establishment of a "digital army" with data analytics and artificial intelligence until a minimum 2025–2030 timeframe. Their stated assumption is that, "modernization efforts must be undertaken concurrent to (…) force employment on operations – there will be no pause."[100] In other words, the continuance of operations takes priority, and the tactical equipment most necessary for short-term mission success must be put in place before any wider initiatives can begin. The C4ISR capabilities are likely to involve AI components, and several ISR-related projects are going through the IDEaS process now (see chapters 3 and 5.1). However, these will be narrow tactical applications of the technologies, embedded within existing organizational stovepipes and without wider integration.

There are a few other systems with AI components that we know are in service, or will be shortly, with DND/CAF today. The Royal Canadian Navy awarded a $45 million CAD contract to Kraken Robotic Systems Inc., out of Newfoundland, in late November 2022 to provide remote mine hunting and mine disposal equipment, and an additional $12 million CAD for underwater sound equipment, for a 24-month acquisition followed by an initial five-year logistics support program.[101] The acquisition includes autonomous underwater vehicles and the use of Kraken's AquaPix synthetic aperture sonar and its image processing software that allows for embedded automatic target recognition and data exfiltration.[102] Since 2016, the government has awarded large contracts to IBM to provide both the Canadian Forces Health Services Group and the Canadian Institute for Military and Veterans Health Research with the data infrastructure and cognitive computing capabilities to conduct advanced "big data" analytics related to healthcare research for service members.[103] In November 2020, DND awarded a $5.75 million CAD contract

99 Department of National Defence, "Real Time Analysis: Science and Technology Related (R&D), Contract #W3371-215029, Awarded to Plum.Io Inc"
100 Gonthier, Accelerating the Canadian Army's Digital Transformation, pp. 2-3; Canadian Army, Advancing with Purpose, p. 26.
101 Department of National Defence, "Remote Minehunting and Disposal Systems, Contract #W8472-105270/001/QF, Awarded to Kraken Robotic Systems Inc.;" Department of National Defence, "Underwater Sound Equipment, Contract #W8482-206387/001/QF, Awarded to Kraken Robotic Systems Inc."
102 Kraken Robotics Inc., "Kraken Awarded $50+ Million Navy Contract for Royal Canadian Navy Minehunting Program."
103 Bélanger/Cramm, "Canadian Military Healthcare Consortium Taps Analytics for More Comprehensive Research;" Department of National Defence, "CFHIS - Support Services, Contract #W8474-03BH01/001/XT, Awarded to IBM Canada Ltd."

to the Calian Group consulting firm for data remediation and marking of serially managed materiel, with the goal of supporting the implementation of automatic identification technology throughout the organization – a project to make more DND assets machine-readable that has been ongoing, with stops and starts, since 2016.[104]

However, one example publicized by DND/CAF as an effective use of AI is in fact an indictment of the organization's data ecosystem. The *AI Strategy* cites the example of an AI tool used by the Joint Targeting Intelligence Centre (likely the IMRSV Anvil Crucible), which maps networked relationships between target entities: "In 2021, CAF was presented with an urgent request from Immigration Refugees and Citizenship Canada (IRCC) for the names of Afghan personnel who had worked for Canada and now needed evacuation. This data existed, but as large quantities of paper files that would take dozens of people hundreds of hours to review manually. With permission from JITC and support from the vendor, the team spent a weekend scanning the documents and used the tool to extract thousands of names for IRCC."[105] While the story suggests that applying an "agile AI-based solution" was a major accomplishment, the problem it solved was entirely manufactured by the failure of basic digitization and stovepiped information within DND/CAF. It was fortunate that a tool existed that could partially salvage the situation, but DND/CAF may come to rely on AI systems rescuing it from its own poor practices.

So far there are very few "use cases" publicly identified where defence AI systems are actively being fielded and operated by DND/CAF today.

104 Department of National Defence, "Informatics Professional Services, Contract #W6381-170008/001/XG, Awarded to Calian Ltd.;" Calian Group, "Unique Identification (UID) to Improve Tracking, Remediation, and Life Cycle Management of Materiel Assets."

105 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 29.

7 Training for Defence AI

The Canadian Armed Forces are presently facing an existential threat in the form of a human resources crisis in their pool of uniformed personnel. As of December 2022, the CAF is 10,000 uniformed members short of its authorized strength, with a 10 per cent annual attrition rate that is "downright catastrophic."[106] A Chief of the Defence Staff / Deputy Minister Directive on Reconstitution was issued on 6 October 2022 that began the process of scaling back non-essential operations and activities to "recover and rebuild (reconstitute) the organization," but noted that the personnel shortfalls had already "severely impacted the organization's ability to deliver professional and collective training." "During this period of change," the Directive reads, "we will need to make difficult choices about our readiness levels, capacity for sustained operations, as well as our level of commitment to all activities, while continuing to deliver strategic effects for the [Government of Canada]."[107]

What does reconstitution mean for defence AI? The draft *DND/CAF AI Strategy* highlights the "people problems" as requiring its own line of effort, and makes these points: "We must identify and plan for our workforce needs[,] we must cultivate AI readiness among our existing people[, and] we must find new ways to bring critical skills into the enterprise – and to retain and use them." However, it will now be an uphill struggle. Recent polling has found a distinct lack of enthusiasm among young Canadians for joining the CAF, and this polling is mirrored in disastrously low recruiting and high attrition rates. As Ken Hansen has recently argued, "The Canadian Armed Forces no longer reflect the principles and values of the Canadian populace, or of a modern Canadian work force. If this is not addressed, any reform will only amount to a shuffling of the deck chairs."[108] Hansen's judgment is harsh, but the present existential crisis in recruiting suggests that he is correct about at least one thing: Canadians do not wish to join the armed forces. This creates special problems for nurturing an internal talent pool with fluency in highly specialized AI technologies. If the values and principles of DND/CAF do not appeal to prospective servicemembers with skills in AI technologies then the situation may be unsalvageable, because those skills fetch an unmatchable premium on the open market. It is also worth mentioning that while "modernization" is supposedly a key part of the Reconstitution directive, there is no mention in the order itself of information management or ADM (IM).

The draft *AI Strategy* says that it will meet the "talent and training" challenge first with a review of DND/CAF workforce needs for AI: "DND/CAF must review its AI workforce requirements to identify the skills, competencies, and personnel required to implement AI successfully. This must include not only subject matter experts in AI, but also staff whose roles support the AI lifecycle, including civilian and military

106 Hansen, "The Canadian Armed Forces Are Heading for a Titanic Collapse."
107 Eyre/Matthews "CDS/DM Directive for CAF Reconstitution."
108 Hansen, "The Canadian Armed Forces Are Heading for a Titanic Collapse."

leadership." The *Strategy* also urges DND/CAF to identify priority AI workforce needs and either develop or procure training curricula to meet them: "This review should consider training needs at all levels, and the exploration of new options for both academic and professional training to ensure a talent pipeline for future needs." Finally, it flags the urgent need to "Explore and identify processes to recruit and retain AI talent, and to utilise it where it is needed." Some of the solutions that the strategy offers are the creation of technical Reserves, short-term exchanges, and more flexible career pathways allowing for the attraction of tech-savvy talent above entry level in the CAF.[109] These are all potentially viable paths, and Canada's draft *AI Strategy* does an exemplary job of identifying problems and systemic barriers.

The barriers are many. The assumption of operations primacy has consequences for training and the CAF's posting cycle. Promotion at the mid-level ranks are disproportionately determined by success in commanding operations.[110] Personnel in non-operations career trajectories are far less likely to "have legs" in the reward system, and are unofficially barred from holding the seniormost leadership positions within the organization.[111] "While the CAF recognizes its own need for AI skills," the DND/CAF draft Artificial Intelligence Strategy writes, "it often struggles to make use of those it already has. Members have described their specialization in AI and related fields as career-limiting and speak of having to choose between remaining within their technical field and [choosing] a career path that would lead to promotion. Unsurprisingly, the frustration this produces leads members to release or transfer to the Reserves. This must change if DND/CAF is to rise to the AI challenge."[112]

It is therefore difficult to see how the Department of National Defence and the Canadian Armed Forces will be able to train a reliable AI talent pipeline internally, particularly with uniformed servicemembers. DND/CAF is already embroiled in the wicked problems of training and talent retention more generally, which does not create a promising milieu for harnessing defence AI. The special problems of talent retention in a hot tech market are aggravated by the CAF basic assumptions of operations primacy and unlimited job mobility discussed earlier. Neither hard-won technical expertise in a narrow field, nor a focus on "non-operational" specialist computer science occupations are much rewarded within the CAF. Changing that will require an overhaul of the entire rewards and promotions system, and such an overhaul will meet fierce resistance. DND/CAF may have no choice but to seek external partnerships and contracting for all their major AI needs, as the development of an internal talent pipeline will present a major problem. But as we have seen when discussing Procurement, that path also contains major obstacles.[113]

109 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 24.
110 Hansen, "The Canadian Armed Forces Are Heading for a Titanic Collapse."
111 Kelley, Correlation of Military Trade with Selection of Generals and Flag Officers.
112 Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy, p. 22.
113 Duval-Lantoine, The Ones We Let Down, pp. 1141-17.

8 Conclusion

Technologies categorized as artificial intelligence are in use in Canada's Department of National Defence and Canadian Armed Forces now, and this will continue at a modest pace in the years to come. However, the organization faces serious challenges to any kind of digital transformation or large-scale adoption of defence AI systems. These problems are almost entirely historical, cultural, and organizational, rather than technical. As a country, Canada is quite well-positioned to engage with the potentially transformational effects of artificial intelligence. Its armed forces, however, are definitively not.

Historical and cultural trends within the Canadian military have left the institution heavily decentralized, and its "Level 1" organizations (including the main force employers) are stovepiped from one another, developing capabilities in isolation. DND/CAF's enterprise-wide information management has been a disaster for more than two decades and the organization's data stewardship is a constant source of scandal and embarrassment. Progress is uneven across the organization. Governance appears to be an afterthought.

Is DND/CAF capable of transforming itself? It is not impossible. However, the necessary changes would go "against the grain" of DND/CAF military culture. The changes needed to embrace an "innovative" mindset with regards to AI will run afoul of existing values and norms related to operations primacy, service members' job mobility, rewards, and the insularity of its hierarchical structure. As Allan English has argued, "to enable innovation one must either have a long-term plan to change culture or, if one is not willing or able to do that, change should be planned to be compatible with the existing organizational culture."[114] The existing organizational culture, according to DND/CAF's own strategy documents, is not conducive to the widespread implementation of digital technologies and defence AI. And to make matters worse, DND/CAF's other culture change initiatives have, to date, been very weak. Compounding the matter is the CAF's present "existential crisis" of personnel, which has required an operational pause to focus on reconstitution.

The cultural considerations do not even include the prosaic considerations of procurement: Treasury Board rules and treatment of DND as a high-risk investment disables DND from acquiring anything valued over $10 million CAD in much than ten years. DND has organized funding mechanisms to allow for "minor projects" beneath the $10 million CAD envelope, including the IDEaS and MINDS programs, both of which have exciting possibilities for defence AI in the country. However, the scope of these projects is, even for a relatively small country, tiny. A plethora of small projects means that individual tactical defence AI capabilities

114 English, "Enabling Innovation in Canada's Army," p. 8.

(particularly mission-oriented ones) might be advanced, but the wider problem of balkanized data, IT, IM, and digital infrastructure in DND/CAF will not be addressed with dribs and drabs of "minor project" funding. The DND/CAF draft *Artificial Intelligence Strategy*, which has sadly been languishing unsigned for months, correctly identifies that much larger and more fundamental transformations are needed. A wholesale reform of how the organization handles procurement is likely necessary before any major defence AI acquisitions or partnerships can occur.

This brings us back to the "teeth-and-tail" metaphor for operations primacy. Although AI technologies are broad and cross-cutting, enabling them as strategic assets, will require heavy, even transformational investment in what is derogatorily referred to as the "tail" of the organization. In a small defence force such as Canada's, this will require trade-offs. The idea that the procurement of new combat equipment should be further delayed or cancelled in favour of enhanced back-end computing capabilities and enterprise-wide information management software is going to be a difficult sell to the L1s. But the DND/CAF "animal" of the metaphor is in deep trouble, and its teeth are falling out on their own for lack of strength in the rest of the organization. There is remarkable work being done on defence AI at the grassroots level in DND/CAF, and there are pockets of expertise throughout the organization, particularly in Defence Research and Development Canada. These allow some progress in defence AI. Coupled with low-level "minor project" funding through programs such as IDEaS, some interesting developments can still occur in Canada. However, without leadership and funding above the "minor" threshold, it seems unlikely that these initiatives will be transformational.

In short, something fundamental must change before Canada makes any serious advance towards integrative defence AI across its institution. Realistically, many fundamental things must change. And it seems unlikely that they will change in any great hurry. The fact that the *DND/CAF AI Strategy* has been completed since the middle of 2022 but still awaits "Level Zero" signatures may be suggestive of exactly what kind of priority AI can expect within a department filled with conflicting, competing demands between the L1 siloes. If the global adoption of defence AI proceeds on its present course, Canada is going to be left well behind both its adversaries and its allies, the latter of which will present the greater problem. Worse yet, there are no easy answers or straightforward prescriptions for how Canada might be able to improve its position. The list of what must be done is significant, and almost every point on it will face vitriolic opposition from some quarter. But Canada will mostly likely continue as it is, developing minor tactical AI-related capabilities while neglecting the more serious problems.

9 Annex

9.1 Contracts

Vendor	Business Type and Sector	HQ	Known, Likely, and Possible Defence AI-Related Contracts
Calian Ltd.	Consulting / General Purpose	Ottawa, Canada	■ Informatics – data remediation and labelling (2020, $5.75 million CAD) ■ Support to DRDC Human-Autonomy Interactions (2019, $6.38 million CAD) ■ Informatics – Courseware Dev for Land Command Support System (2018, $1.41 million CAD) ■ Informatics – IM/IT Engineering and Architecture (2018, $9.97 million CAD)
Ernst & Young LLP	Consulting / General Purpose	London, UK	■ None Known
Global Spatial Technology Solutions Inc. (GSTS)	Software / Geospatial Imaging	Nova Scotia, Canada	■ Radar Defence Systems (R&D) (2022, $555K CAD)
IBM Canada Ltd.	Consulting / IT Solutions	New York, USA	■ Project Management and Engineering Support Services (2019, $4.12 million CAD) ■ Canadian Forces Health Information System Support Services (2016, $6.22 million CAD) ■ Director Human Resources Information Management Professional Services (2022, $10.5 million CAD) ■ Task-Based Informatics for custom software (2018, $4.89 million CAD)
KPMG LLP	Consulting / General Purpose	Amstelveen, Netherlands	■ Director Human Resources Information Management Professional Services (2022, $11.7 million CAD) ■ Task-Based Informatics for custom software (2018, $2.84 million CAD) ■ Cyber Operator Training (2020, $1.06 million CAD)
L3 Technologies MAS Inc.	Consulting / Defence	Quebec, Canada	■ Computer-Assisted Learning (2022, $36,842 USD)
Lockheed Martin Canada Inc.	Software / AI Solutions	Washington, DC, USA	■ Radar Equipment (2022, $1.5 million CAD) ■ Underwater Sound Equipment (2022, $1.99 million USD)

Vendor	Business Type and Sector	HQ	Known, Likely, and Possible Defence AI-Related Contracts
Louis Tanguay Informatique (LTI), Ltd.	Software / IT Solutions	Quebec, Canada	■ Weapon systems analysis, modeling, and simulation for DRDC (2020, $5.75 million CAD) ■ Soutien à la recherche et au développement au niveau de l'apprentissage machine (2019, $2.30 million CAD)
MDA Corporation	Software / IT Services	British Columbia, Canada	■ Hyperspectral Target Detection (2017, $977K CAD) ■ Research & Development Support to DRDC, Joint ISR (2020, $3.2 million CAD)
Pricewaterhouse-Coopers LLP	Consulting / General Purpose	London, UK	■ Audit services of internal financial controls and IT systems (2017, $5.23 million CAD)
SAP Canada Inc.	Software / IT Solutions	Walldorf, Germany	■ Automatic data processing software (2018, $376K CAD)
Sierra Systems Group, Inc.	Consulting / IT Services	Tokyo, Japan	■ Informatics for Air Defence IT System Management (2019, $4.31 million CAD)
Thales Canada Inc.	N/A	La Défense, France	■ Command, Control and Information capability development for DRDC (2020, $10.34 million CAD) ■ R&D Embedded Systems Security (2022, $14.95 million CAD) ■ Cryptological Equipment and Components (2021, $1.13 million USD) ■ Mid-Earth Orbit Search and Rescue Satellite Ground Segment (2018, $8.60 million CAD)
Thomson Reuters Canada Ltd.	Software / Data Solutions	Ontario, Canada	■ None Known
Xtract AI Inc.	Software / AI Solutions	British Columbia, Canada	■ Science and Tech R&D Development, Formulation, Modification (2019, $157K CAD)
Ipss Inc. / Service-Now Canada Inc.	Software / IT Solutions	Ontario, Canada	■ Informatics: provision of IM/IT engineering and architecture services (2020, $10.28 million CAD)

9.2 Defence Research and Development Related to AI, 2009–2022

DRDC Report Number	Date	Title	Partners
DRDC-RDDC-2022-P359	01-Sep-22	A novel machine learning approach to analyzing geospatial vessel patterns using AIS data	Dalhousie; DRDC Halifax
DRDC-RDDC-2022-R017	01-Jan-22	Live Automated Video Analysis (LAVA): Proof of Concept	DRDC Valcartier
DRDC-RDDC-2021-R175	01-Nov-21	Question Answering Artificial Intelligence Chat-bot on Military Dress Policy	DRDC Ottawa
DRDC-RDDC-2021-R163	01-Nov-21	Machine learning literacy and applications in defence and security	DRDC Halifax
DRDC-RDDC-2021-R163	01-Nov-21	Machine learning literacy and applications in defence and security	DRDC Halifax
DRDC-RDDC-2021-R155	01-Oct-21	Validation of the ARMOUR Automated Computer Network Defence Technology Demonstrator	DRDC Ottawa
DRDC-RDDC-2021-D079	01-May-21	Artificial intelligence tools for threat assessment	DRDC Ottawa
DRDC-RDDC-2021-C082	01-Mar-21	Survey of Video-to-Text Literature	Thales Research Canada; DRDC Valcartier
DRDC-RDDC-2021-R016	01-Mar-21	Deep Learning Methods for Object Classification in Wideband Sonar Scattering Data	DRDC Halifax
DRDC-RDDC-2021-D046	01-Mar-21	Training strategies for sustaining operator attention in automated systems for Canadian Armed Forces environments	DRDC Toronto
DRDC-RDDC-2022-N258	01-Jan-21	Mission-Oriented Research for artificial intelligence (AI) and Big Data for Military Decision Making	The Netherlands Organization; DRDC Valcartier; Leonardo Societa per Azioni (Italy)
DRDC-RDDC-2020-R13	01-Dec-20	A RADARSAT-2 dataset for the application of machine learning in maritime domain awareness	DRDC Ottawa

DRDC Report Number	Date	Title	Partners
DRDC-RDDC-2020-C175	01-Nov-20	Final report for Task 2 on artificial intelligence (AI) and cognitive informatics (CI) for authority pathway for weapon engagement (APWE)	DRDC Toronto
DRDC-RDDC-2020-D111	01-Oct-20	Computational resources to address emerging artificial intelligence defence requirements: joint targeting section	DRDC Ottawa
DRDC-RDDC-2020-R086	01-Sep-20	Development of a testing architecture for characterization of deep learning algorithms	DRDC Valcartier
DRDC-RDDC-2021-C072	01-Aug-20	Final Report, AT01: Data Management, Labelling, and Automation for Machine Learning	Solana Networks; DRDC Valcartier
DRDC-RDDC-2020-P186	01-May-20	MiNet: Efficient deep learning automatic target recognition for small autonomous vehicles	DRDC Halifax
DRDC-RDDC-2019-C268	01-Nov-19	UPEI Development of an Automated Goniometer	DRDC Valcartier; University of Prince Edward Island
DRDC-RDDC-2019-C067	01-Apr-19	Machine Learning in Vulnerability Assessment	Solana Networks; DRDC Ottawa
DRDC-RDDC-2019-C082	01-Apr-19	Methodology for Evaluating the Fitness of Vulnerability Assessment Tools for Automated Computer Network Defence	DRDC Ottawa; Solana Networks
DRDC-RDDC-2022-P287	01-Mar-19	Artificial Intelligence, Robotics, Ethics, and the Military: A Canadian Perspective	DRDC Ottawa
DRDC-RDDC-2020-C064	01-Mar-19	Task Authorization 43 - doc2vec Deep Learning for Text Analytics	Thales Research Canada; DRDC Valcartier
DRDC-RDDC-2018-R249	01-Dec-18	Reduction of False Alarms in Sea Ice Covered Ocean Regions Using Machine Learning	DRDC Ottawa
DRDC-RDDC-2022-D133	01-Oct-18	A Deep Reinforcement Learning-based Trust Management Scheme for Software-defined Vehicular Networks	Carleton; DRDC Ottawa; Association for Computing Machinery (NY)

DRDC Report Number	Date	Title	Partners
DRDC-RDDC-2021-N138	01-Oct-18	Supporting technology enabled learning with artificial intelligence and cognitive modelling	DRDC Toronto; National Research Council of Canada
DRDC-RDDC-2019-N155	01-Oct-18	Internet of things and machine learning for information operations targeting	DRDC Ottawa; Communications Research Centre
DRDC-RDDC-2017-D136	01-Feb-18	Investigation to replace machine learning architecture in DRDC's aural classifier	DRDC Halifax
DRDC-RDDC-2017-P035	25-Oct-17	Automated stationary human target detector for 3-D through-wall radar imagery	DRDC Ottawa
DRDC-RDDC-2017-C169	01-Jul-17	System Concept of Operations (CONOPS) for the Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) Contract	DRDC Ottawa; General Dynamics Canada
DRDC-RDDC-2016-P144	04-May-17	ISR asset visibility and collection management optimization through knowledge models and automated reasoning	DRDC Valcartier; US Army Research Lab
DRDC-RDDC-2017-C061	01-Mar-17	Deep Learning for Human Decision Support	DRDC Ottawa; National Research Council of Canada
DRDC-RDDC-2016-C330	01-Mar-16	Automated Computer Network Defence Architectures in Coalition Environments	DRDC Ottawa; Bell Canada; Sphyrna Security
DRDC-RDDC-2015-C006	01-Jan-15	Automated Computer Network Defence Technology Demonstration Project Architectural Design Document	DRDC Ottawa; General Dynamics Canada
DRDC-RDDC-2014-P5	18-Mar-14	Automated Extraction and Characterisation of Social Network Data from Unstructured Sources	DRDC Valcartier
DRDC-OTTAWA-CR-2013-101	01-Nov-13	Automated Experimentation System - Malware Analysis System	DRDC Ottawa; AEPOS Technologies
DRDC-CSS-TN-2013-031	01-Nov-13	Overview of the All Hazards Risk Assessment (AHRA) Automated Application and Capability Assessment Management System (CAMS)	DRDC Ottawa

DRDC Report Number	Date	Title	Partners
DRDC-CORA-CR-2013-121	01-Aug-13	Machine Learning Algorithms for Multiple Autonomous Unmanned Vehicle Operations: Using Support Vector Machine	DRDC Ottawa; Nathalie Japkowicz Consulting
DRDC-CORA-CR-2013-119	01-Aug-13	Methods and Tools for Automated Data Collection and Collation of Open Source Information	DRDC Ottawa; CAE Professional Services
DRDC-CORA-CR-2013-059	01-Apr-13	Machine Learning Algorithms for Multiple Autonomous Unmanned Vehicle Operations: A Fast Detection Algorithm	DRDC Ottawa; Nathalie Japkowicz Consulting
DRDC-OTTAWA-TM-2012-084	01-Aug-12	Artificial Intelligence in Games: A Survey of the State of the Art	DRDC Ottawa
DRDC-CORA-CR-2012-154	01-Jun-12	Machine Learning Algorithms for Multiple Autonomous Unmanned Vehicle Operations: Research Proposal	DRDC Ottawa; Nathalie Japkowicz Consulting
DRDC-OTTAWA-TR-2012-060	01-May-12	Automated risk management system	DRDC Ottawa
DRDC-VAL-CARTIER-SL-2012-027	01-Jan-12	Artificial Intelligence for Networked Robotic Drones	DRDC Valcartier
DRDC-OTTAWA-TM-2010-215	01-Dec-10	Security classification using automated learning (SCALE): Optimizing statistical natural language processing techniques to assign security labels to unstructured text	DRDC Ottawa
DRDC-VAL-CARTIER-SL-2009-384	15-Sep-09	Automated Reasoning for Maritime Anomaly Detection	DRDC Valcartier

9.3 Security Policy Nexus of Emerging Technology (SPNET) Briefing Notes on AI, 2020–2021

SPNET Briefing Note Title	Authors	Date
Transparency, Accountability, and Bias in AI	Mehdi Taheri, Reza Bahrevar and Kash Khorasani	October 2020
Requirements for AI Liabilities, Accountability and Role of Explanation	Mohammadreza Nematallahy and Kash Khorasani	October 2020
Facial Recognition, Impact of AI on National Security, Adversarial Attacks and Trust in AI	Mehdi Taheri and Kash Khorasani	October 2020
Dual-Use Technology Policy for AI	Bita Afshar and Kash Khorasani	October 2020
The Rise of Industrial Cyber Defence Power in the 21st Century – Regulation and Public Partnerships	Dave McMahon	October 2020
Vulnerabilities of Technology: A Framework to Look into the Impact on Human Activity	Michael Wood and Mohsen Farhadloo	October 2020
Why Specialized Military AI Inspectors are Needed?	Reza Bahrevar and Kash Khorasani	February 2021
Privacy, Fairness, and Security: AI and Edge Computing	Reza Bahrevar and Kash Khorasani	February 2021
Dual-Use in IT Development	Bita Afshar and Kash Khorasani	February 2021
Future of Privacy and Security Issues of AI Systems Under the Branch of Fog Computing	Reza Bahrevar and Kash Khorasani	February 2021
National Defence and the Infodemic	Dave McMahon	February 2021
Data Privacy and Liability of Emerging Technologies and AI	Edward Gharibian and Kash Khorasani	February 2021
Regulation and Need for Categorization of AI-Based Systems	Reza Bahrevar and Kash Khorasani	May 2021
Dual Use Aspects of Artificial Intelligence (AI) and Autonomous Systems	Reza Bahrevar and Kash Khorasani	May 2021
Dual Use Aspects of Artificial Intelligence (AI) and Autonomous Systems	Bita Afshar and Kash Khorasani	May 2021

SPNET Briefing Note Title	Authors	Date
Requirements for Liabilities of AI Systems	Mohamadreza Nematollahi and Kash Khorasani	May 2021
Accountability and the Role of AI Explanation	Mohamadreza Nematollahi and Kash Khorasani	May 2021
Public and Defence Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity	Neshat Elhami Fard, Rastko R. Selmic and Khashayar Khorasani	May 2021
Challenges of Public Policy in Autonomous Systems	Shahram Shahkar and Kash Khorasani	May 2021
Vulnerabilities of Emerging Technologies: A Systematic Literature Review	Saman Asvadi and Mohsen Farhadloo	May 2021
Data Restriction for AI-Based Dual Use Technologies and AI Defensive Measures	Reza Bahrevar and Kash Khorasani	August 2021
Public and Defence Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity Part 2: Defence Policy Challenges of Artificial Intelligence	Neshat Elhami Fard, Rastko R. Selmic and Kash Khorasani	August 2021
Public and Defence Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity Part 3: Reinforcement Learning Algorithms for Cybersecurity and Military Defense Applications	Neshat Elhami Fard, Rastko R. Selmic and Kash Khorasani	August 2021
Public and Defence Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity Part 4: Reinforcement Learning Algorithms for Cybersecurity and Military Defense Applications	Neshat Elhami Fard, Rastko R. Selmic and Kash Khorasani	August 2021
Public and Defence Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity Part 5: Applications, Challenges, and Ethical Behaviors on Reinforcement and Deep Reinforcement Learning Algorithms	Neshat Elhami Fard, Rastko R. Selmic and Khashayar Khorasani	August 2021

SPNET Briefing Note Title	Authors	Date
CYBER DECEPTION - The Art of Camouflage, Stealth and Misdirection	Dave McMahon and Clairvoyance Cyber Corp	August 2021
Canadian Design Concepts in Autonomous Systems	Shahram Shahkar and Kash Khorasani	August 2021
Ethical and Privacy Issues in AI and IoT Devices	Mehdi Taheri and Kash Khorasani	August 2021
Ethics of Lethal Autonomous Weapons Systems	Kari Zaccharias and Ketra Schmitt	August 2021
Data Restriction for AI-based Dual Use Technologies	R. Bahrevar and K. Khorasani	November 2021
Cognitive Security Analyst and Why we Need It	R. Bahrevar and K. Khorasani	November 2021
Artificial Intelligence: Ethical Challenges of Labor Market	M. R. Nematollahi and K. Khorasani	November 2021
Artificial Intelligence: Economic System and Financial Market Security	M. R. Nematollahi and K. Khorasani	November 2021
AI, Contestability, and Legal Arguments	R. Bahrevar and K. Khorasani	November 2021
Regulation and Need for Categorization of AI-Based Products	R. Bahrevar and K. Khorasani	November 2021
Canadian Design Concepts in Autonomous Systems	S. Shahkar and K. Khorasani	November 2021
Accountability and Transparency in AI Systems: A Public Policy Perspective	R. Bahrevar and K. Khorasani	November 2021
Accountability and Transparency in AI Systems	R. Bahrevar and K. Khorasani	November 2021
Public Policy Framework for AI-Powered Facial Recognition Technologies	M. R. Nematollahi and K. Khorasani	November 2021
Public and Defense Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity Part 7: Ethical AI in Defence-	Neshat Elhami Fard, Rastko R. Selmic and Khashayar Khorasani	November 2021
Public and Defense Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity, Part 8: Ethical AI in Defence	Neshat Elhami Fard, Rastko R. Selmic and Khashayar Khorasani	November 2021

SPNET Briefing Note Title	Authors	Date
Public and Defense Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity, Part 9: Ethical AI in Defence	Neshat Elhami Fard, Rastko R. Selmic and Khashayar Khorasani	November 2021
Public and Defense Policy Challenges and Innovations on Artificial Intelligence, Autonomous Systems, and Cybersecurity, Part 10: Ethical AI in Defence	Neshat Elhami Fard, Rastko R. Selmic and Khashayar Khorasani	November 2021
How to Apply AI in the Battlefield Arena?	R. Bahrevar and K. Khorasani	November 2021
Defence Policies on Zero Trust Model for Battlefield Applications	R. Bahrevar and K. Khorasani	November 2021
Artificial Intelligence: National Security and Policy Considerations	M. R. Nematollahi and K. Khorasani	November 2021
Artificial Intelligence: International Security and Foreign Policy	M. R. Nematollahi and K. Khorasani	November 2021
Artificial Intelligence: Defense, Intelligence and National Security	M. R. Nematollahi and K. Khorasani	November 2021
Arms Race Dynamics for Artificial General Intelligence	Patrick Folinsbee	November 2021
Semiconductor Supply Chains	Vincent Zottola	November 2021

Literature

Advisory Council on Artificial Intelligence, Annual Report 2020-21 (Ontario: Innovation, Science and Economic Development Canada, 2021), https://ised-isde.canada.ca/site/advisory-council-artificial-intelligence/en/annual-report-2020-21 (last accessed January 18, 2023).

Araya, Daniel, Artificial Intelligence for Defence and Security (Waterloo: Centre for International Governance Innovation, 2022).

Arbour, Louise, Report of the Independent External Comprehensive Review of the Department of National Defence and the Canadian Armed Forces (Montreal: Bordner Ladner Gervais, 2022), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/report-of-the-independent-external-comprehensive-review.html (last accessed January 18, 2023).

Bedley, Kenneth P, Closing the Tech Gap: A CAF Start-up Model for Digital Transformation. JCSP 47 Master of Defence Studies (Ontario: Canadian Forces College, 2021), https://www.cfc.forces.gc.ca/259/290/23/286/Bedley.pdf (last accessed January 18, 2023)

Bélanger, Stéphanie and Heidi Cramm, "Canadian Military Healthcare Consortium Taps Analytics for More Comprehensive Research," IBM Blog, November 22, 2016. https://www.ibm.com/blogs/think/2016/11/canadian-military-healthcare-consortium-adopts-analytics-for-deeper-research/ ((last accessed January 18, 2023).

Berthiaume, Lee, "Head of Sexual Misconduct Response Centre Says Complaints against Military Brass Are a Sign of Progress," The Globe and Mail, March 17, 2021.

Beshaies, Benoit and Dawn Hall, "Responsible Use of Automated Decision Systems in the Federal Government," Statistics Canada, December 1, 2021. https://www.statcan.gc.ca/en/data-science/network/automated-systems (last accessed January 18, 2023).

Bitar, Omar, Benoit Deshaies, and Dawn Hall, 3rd Review of the Treasury Board Directive on Automated Decision-Making (Ontario: Treasury Board of Canada Secretariat, 2022).

Brewster, Murrray, "More than a Decade Ago, the Army Had a Plan to Rebuild. It Went Nowhere," CBC News Online, January 7, 2023. https://www.cbc.ca/news/politics/canadian-armed-forces-equipment-procurement-ukraine-latvia-1.6706444 (last accessed January 18, 2023).

Burns, E.L.M, Manpower in the Canadian Army, 1939-1945 (Toronto: Clarke Irwin, 1956).

Calian Group, "Unique Identification (UID) to Improve Tracking, Remediation, and Life Cycle Management of Materiel Assets," Calian Group Press Release, July 26, 2021. https://www.calian.com/press-releases/calian-enables-department-of-national-defence-to-track-millions-of-assets/ (last accessed January 18, 2023).

Canadian Army, Advancing with Purpose: The Canadian Army Modernization Strategy (Ottawa: HQ, Canadian Army, 2020).

Canadian Army, Modernization Vital Ground: Digital Strategy (Ottawa: HQ, Canadian Army, 2022)

Canadian Special Operations Forces Command, Beyond the Horizon: A Strategy for Canada's Special Operations Forces in an Evolving Security Environment (Ottawa: CANSOFCOM, 2020).

Cardoso, Tom and Bill Curry, "National Defence Skirted Federal Rules in Using Artificial Intelligence, Privacy Commissioner Says," The Globe and Mail, February 7, 2021. https://www.theglobeandmail.com/canada/article-national-defence-skirted-federal-rules-in-using-artificial/ (last accessed January 18, 2023).

Chief Information Officer, Defence Information Management Plan (Ottawa: Department of National Defence, 2019.)

Chief Review Services, NDHQ 99: Review of Restructuring and Re-Engineering: Volume 1 (Ontario: Chief Review Services, 2001), https://publications.gc.ca/collections/collection_2015/mdn-dnd/D58-83-2001-eng.pdf (last accessed January 18, 2023).

Chief Review Services, NDHQ 99: Review of Restructuring and Re-Engineering: Volume 3 (Ontario: Chief Review Services, 2001).

Defence Research and Development Canada, "Mandate," January 27, 2022. https://www.canada.ca/en/defence-research-development/corporate/mandate.html (last accessed January 18, 2023).

Department of National Defence, "Arti. Intell & Mac. L. R&D Services, Contract #W6399-19KH95/001/SL, Awarded to Thales Digital Solutions Inc.," CanadaBuys Award Notices, October 27, 2020. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w6399-19kh95001sl (last accessed January 18, 2023).

Department of National Defence, "Arti. Intell & Mac. L. R&D Services, Contract #W6399-19KH95/002/SL, Awarded to MDA Systems Ltd.," CanadaBuys Award Notices, November 16, 2020. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w6399-19kh95002sl (last accessed January 18, 2023).

Department of National Defence, "Arti. Intell & Mac. L. R&D Services, Solicitation #W6399-19KH95/B," CanadaBuys Tender Notices, June 23, 2020. https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-sl-014-38055 (last accessed January 18, 2023).

Department of National Defence, "Artificial Intelligence/Inference Systems (R&D), Contract #W8484-220165/001/SC, Awarded to IMRSV Data Labs Inc.," CanadaBuys Award Notices, December 13, 2021. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w8484-220165001sc (last accessed January 18, 2023).

Department of National Defence, "CFHIS - Support Services, Contract #W8474-03BH01/001/XT, Awarded to IBM Canada Ltd.," CanadaBuys Award Notices, June 14, 2016. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w8474-03bh01001xt (last accessed January 18, 2023).

Department of National Defence, "Competitive Projects." Innovation for Defence Excellence and Security (IDEaS). Accessed December 30, 2022. https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/competitive-projects.html (last accessed January 18, 2023).

Department of National Defence, "Gender-Based Analysis Plus," DND Department Results Reports, February 1, 2022. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-results-report/2020-21-index/supplementary-information-tables/gba-plus.html (last accessed January 18, 2023).

Department of National Defence, "IDEaS: Innovation for Defence Excellence and Security," Accessed November 5, 2022. https://www.canada.ca/en/department-national-defence/programs/defence-ideas.html (last accessed January 18, 2023).

Department of National Defence, "Informatics Professional Services, Contract #W6381-170008/001/XG, Awarded to Calian Ltd.," CanadaBuys Award Notices, November 27, 2020. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w6381-170008001xg (last accessed January 18, 2023).

Department of National Defence, "Mobilizing Insights in Defence and Security (MINDS)," October 26, 2022. https://www.canada.ca/en/department-national-defence/programs/minds.html (last accessed January 18, 2023).

Department of National Defence, "Real Time Analysis: Science and Technology Related (R&D), Contract #W3371-215029, Awarded to Plum.Io Inc.," CanadaBuys Award Notices, May 15, 2020. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w3371-215029001sc (last accessed January 18, 2023).

Department of National Defence, "Remote Minehunting and Disposal Systems, Contract #W8472-105270/001/QF, Awarded to Kraken Robotic Systems Inc.," CanadaBuys Award Notices, November 30, 2022. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w8472-105270001qf (last accessed January 18, 2023).

Department of National Defence, "Spot the Hack: Intrusion Detection Systems for Avionics Networks and Bus Technologies." Innovation for Defence Excellence and Security (IDEaS) Competitive Projects, April 1, 2022, https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/competitive-projects/challenges/spot-hack-intrusion-detection-avionics-networks-technologies.html (last accessed January 18, 2023).

Department of National Defence, "Underwater Sound Equipment, Contract #W8482-206387/001/QF, Awarded to Kraken Robotic Systems Inc.," CanadaBuys Award Notices, November 30, 2022. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w8482-206387001qf (last accessed January 18, 2023).

Department of National Defence, Canadian Armed Forces Ethos: Trusted to Serve (Ottawa: Canadian Defence Academy – Professional Concepts and Leader Development, 2022), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-ethos-trusted-to-serve.html (last accessed January 18, 2023).

Department of National Defence, Mobilizing Insights in Defence and Security – MINDS: Annual Report 2019-2020 (Ottawa: Department of National Defence, 2020), https://www.canada.ca/content/dam/dnd-mdn/documents/minds/minds-annual-report-2020.pdf (last accessed January 18, 2023).

Department of National Defence, Project Approval Directive (PAD) (2019).

Department of National Defence, Science and Technology in Action: Delivering Results for Canada's Defence and Security," Defence and Security S&T Strategy (Ottawa: Department of National Defence, 2013.)

Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy 2017 (Ottawa: Department of National Defence, 2017), http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf (last accessed January 18, 2023).

Department of National Defence, The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy (UNAPPROVED DRAFT) (Ottawa: Department of National Defence, 2022).

Department of National Defence, The Department of National Defence and Canadian Armed Forces Data Strategy (Ottawa: Department of National Defence, 2019).

Desbarats, Peter, Somalia Cover-Up: A Commissioner's Journal (Toronto: McClelland & Stewart, 1997.

Directorate S&T Strategic Partnerships, "Artificial Intelligence," PowerPoint Brief, Ottawa, September 2022.

Duval-Lantoine, Charlotte, The Ones We Let Down: Toxic Leadership Culture and Gender Integration in the Canadian Forces (Montreal & Kingston: McGill-Queen's University Press, 2022).

English, Allan, "Corruption in the Canadian Military? Destroying Trust in the Chain of Command," Canadian Foreign Policy Journal 23, no. 1 (2017), pp. 32–46.

English, Allan, "Enabling Innovation in Canada's Army: Cultural Transformations and Military Effectiveness." Conference Presentation, Canadian Army Historical Workshop, Kingston, 2011.

English, Allan, "Sex and the Soldier: The Effect of Competing Ethical Value Systems on the Mental Health and Well Being of Canadian Military Personnel and Veterans," in Stephanie A. H. Belanger and Daniel Lagace-Roy (eds.) Military Operations and the Mind: War Ethics and Soldiers' Well-Being (Montreal & Kingston: McGill-Queen's University Press, 2016), pp. 191–208.

English, Allan, Angus Brown, and Paul Johnston, "Are We Losing Our Memory? Decision Making in DND," in Yves Tremblay (ed.), Canadian Military History Since the 17th Century: Proceedings of the Canadian Military History Conference, Ottawa, 5-9 May 2000 (Ottawa: Directorate of History and Heritage, 2001), pp. 473-480.

English, Allen, Understanding Military Culture: A Canadian Perspective (Montreal & Kingston: McGill-Queen's University Press, 2004).

Eyre, Wayne and Bill Matthews, "CDS/DM Directive for CAF Reconstitution," Department of National Defence, October 6, 2022. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/dm-cds-directives/cds-dm-directive-caf-reconstitution.html (last accessed January 18, 2023).

Fetterly, Eglin Ross, Arming Canada: Defence Procurement for the 21st Century. PhD Thesis (Ontario: Royal Military College of Canada, 2011).

Goette, Richard, Preparing the RCAF for the Future: Defining Potential Niches for Expeditionary Operations (Astra: RCAF Aerospace Warfare Centre, 2020).

Gonthier, Nicholas, Accelerating the Canadian Army's Digital Transformation. Joint Command and Staff Program 48 Service Paper (Ontario: Canadian Forces College, 2022).

Hansen, Ken, "The Canadian Armed Forces Are Heading for a Titanic Collapse," The Globe and Mail, December 2, 2022. https://www.theglobeandmail.com/opinion/article-canada-military-shortage-crisis/?utm_source=dlvr.it&utm_medium=twitter (last accessed January 18, 2023).

Horn, Bernd, and Bill Bentley, Forced to Change: Crisis and Reform in the Canadian Armed Forces (Toronto: Dundurn Press, 2015).

IMRSV Data Labs, "Our Products: Anvil Crucible Defence Suite," IMRSV Data Labs, 2022. https://imrsv.ai/products (last accessed January 18, 2023).

Kelley, Travis, Correlation of Military Trade with Selection of Generals and Flag Officers. Master of Defence Studies (Ontario: Canadian Forces College, 2020), https://www.cfc.forces.gc.ca/259/290/22/286/kelley.pdf (last accessed January 18, 2023).

Kraken Robotics Inc., "Kraken Awarded $50+ Million Navy Contract for Royal Canadian Navy Minehunting Program," December 7, 2022, https://krakenrobotics.com/kraken-awarded-50-million-navy-contract-for-royal-canadian-navy-minehunting-program/ (last accessed January 18, 2023).

Leslie, Andrew, Report on Transformation 2011 (Ontario: Department of National Defence, 2011), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/report-on-transformation-2011.html (last accessed January 18, 2023).

Lizotte, Ryan, Learning to Swim in a Sea of Information: Improving Information Management in the Department of National Defence. Joint Command and Staff Program 45 Solo Flight (Ontario: Canadian Forces College, 2019).

Matthews, Bill, "Message from the Deputy Minister Regarding the Digital Transformation Office," The Maple Leaf, December 6, 2022. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2022/12/message-deputy-minister-digital-transformation-office.html (last accessed January 18, 2023).

McKeown, Ryder, "Food for Thought Paper for the Deputy Minister and the Chief of the Defence Staff: Threats and Challenges of Artificial Intelligence." Department of National Defence, Directorate of Policy Development, November 30, 2018.

Nossal, Kim Richard, Charlie Foxtrot: Fixing Defence Procurement in Canada (Toronto: Dundurn, 2016).

OECD AI, "Visualisations Powered by JSI Using Data from MAG," December 31, 2021 https://oecd.ai/en/data?selectedArea=ai-research&selectedVisualization=ai-publications-by-country-over-time (last accessed January 18, 2023).

Paquet, Guillaume, Culture Change: Should People First Trump Mission First?, JCSP 48 Service Paper (Ontario: Canadian Forces College, 2022) https://www.cfc.forces.gc.ca/259/290/24/192/Paquet.pdf (last accessed January 18, 2023).

Perry, Dave, "Priorities for Canada's Air Force," Defence Deconstructed, https://soundcloud.com/user-609485369/defence-deconstructed-priorities-for-canadas-air-force (last accessed January 18, 2023).

Pigeau, Ross, and Carol McCann, "Re-Conceptualizing Command and Control," Canadian Military Journal, vol. 3, no. 1 (Spring 2002), pp. 53–64.

Priems, Geoffrey, and Peter Gizewski, "Leveraging Artificial Intelligence for Canada's Army: Current Possibilities and Future Challenges," Canadian Army Journal, vol. 19, no. 2 (2021), pp. 40–51.

Riley, Alycia, Jasmine Samra, Matt Hervey, and Jocelyn Paulley, "Bill C-27: A Depper Dive into Canada's Proposed Artificial Intelligence and Data Act," Gowling WLG, October 28, 2022. https://gowlingwlg.com/en/insights-resources/articles/2022/canada-s-artificial-intelligence-and-data-act/ (last accessed January 18, 2023).

Royal Canadian Navy, Digital Navy: A Strategy to Enable Canada's Naval Team for the Digital Age (Ottawa: Royal Canadian Navy, 2020).

Rozema-Seaton, Erik, "BOXTOP 22: The Cost of Focusing on an Operational Culture," Royal Canadian Air Force Journal, vol. 8, no. 4 (Fall 2019), pp. 6–23.

Sabry, Omar, "Torture of Afghan Detainees: Canada's Alleged Complicity and the Need for a Public Inquiry (Ottawa: Canadian Centre for Policy Alternatives, 2015).

Scassa, Teresa, "Comments on the Third Review of Canada's Directive on Automated Decision-Making," May 17, 2022, https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=354:comments-on-the-third-review-of-canadas-directive-on-automated-decision-making&Itemid=80 (last accessed January 18, 2023).

Schein, Edgar H., and Peter Schein, Organizational Culture and Leadership (New York: John Wiley & Sons, 2017).

Schofield, M.E., Delivering on Strong Secure Engaged: Defence Procurement Reforms to Increase Efficiency. JCSP 45 Service Paper (Ontario: Canadian Forces College, 2019) https://www.cfc.forces.gc.ca/259/290/308/192/schofield.pdf (last accessed January 18, 2023).

Security-Policy Nexus of Emerging Technology "About SPNET: Our Work," https://www.concordia.ca/ginacody/research/spnet/about.html (last accessed January 18, 2023).

Sharpe, G.E. "Executive Summary – Board of Inquiry –Croatia," January 19, 2000. Fonds 31, Box 2, 04.37.05. PPCLI Archives.

The Canadian Press. "Military Planned to Cut Health Services, Documents Show." CBC News Online, October 3, 2012. https://www.cbc.ca/news/politics/military-planned-to-cut-health-services-documents-show-1.1164960 (last accessed January 18, 2023).

Treasury Board of Canada, "Directive on Automated Decision Making (2019)," https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 (last accessed January 18, 2023).

Treasury Board of Canada, "List of Interested Artificial Intelligence (AI) Suppliers," August 22, 2022. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/list-interested-artificial-intelligence-ai-suppliers.html#wb-auto-5 (last accessed January 18, 2023).

Wasilow, Sherry and Joelle Thorpe, Artificial Intelligence, Robotics, Ethics, and the Military: A Canadian Perspective. External Literature (P) (Ottawa: Defence Research and Development Canada, 2022).

Defense AI Observatory Studies

23|09 Robert C Engen, When the Teeth Eat the Tail: A Review of Canada's Defence Artificial Intelligence

23|08 Çağlar Kurç, Enabling Technology of Future Warfare. Defense AI in Turkey

23|07 Lauren A. Kahn, Risky Incrementalism. Defense AI in the United States

22|06 Yvonne Hofstetter, Wie KI Innere Führung lernt. Wertbasierte Technik mit IEEE7000TM-2021

22|05 Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini, Exploring the Benefits of a New Force Enabler: Defense AI in Italy

22|04 Kenneth Payne, Bright Prospects – Big Challenges. Defense AI in the United Kingdom

22|03 Heiko Borchert, Christian Brandlhuber, Armin Brandstetter, and Gary S. Schaal, Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense

22|02 Peter Layton, Evolution not Revolution. Australia's Defence AI Pathway

21|01 Heiko Borchert, Torben Schütz, Joseph Verbovszky, Beware the Hype. What Military Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War

Defense AI Observatory

www.defenseai.eu