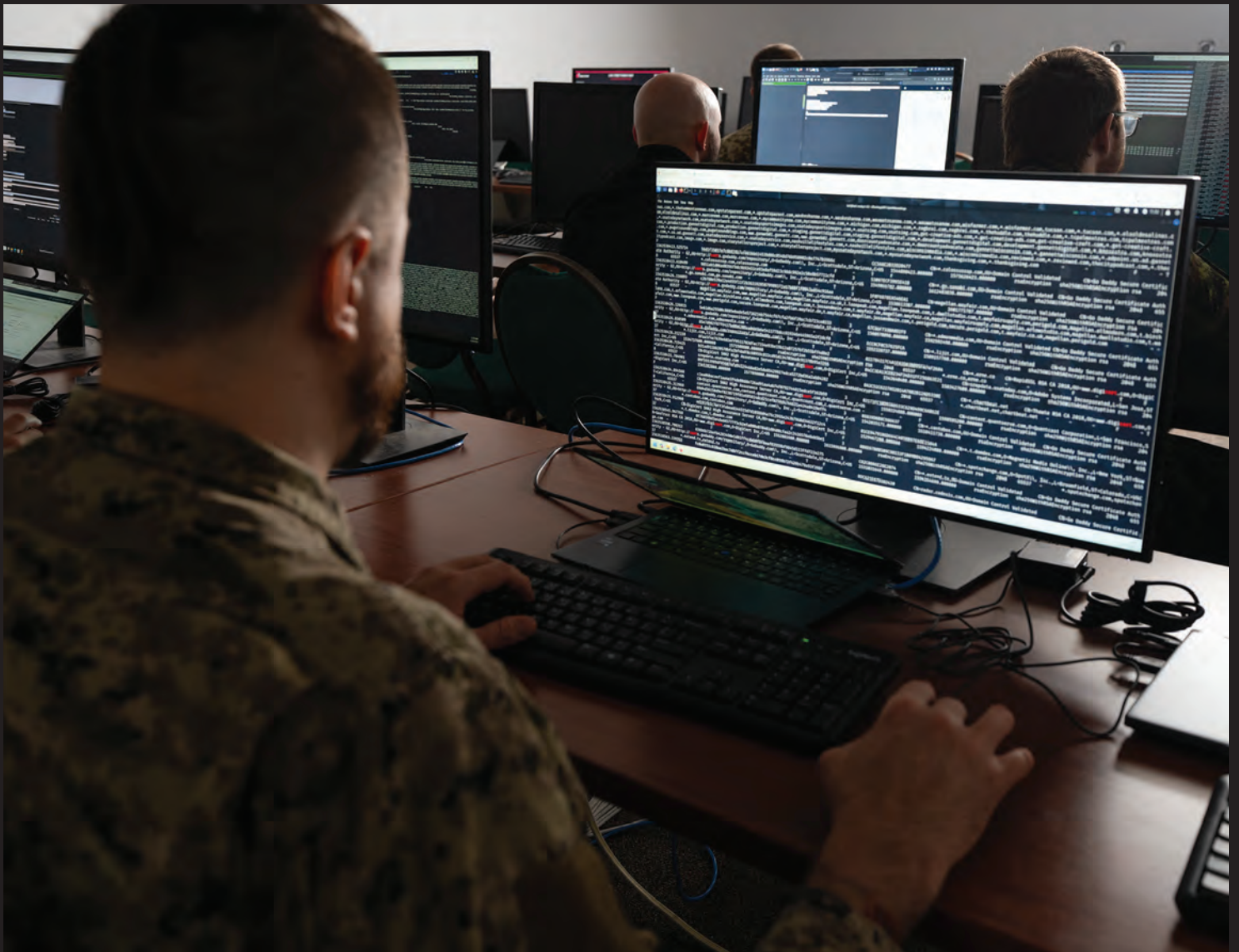


CANADIAN MILITARY JOURNAL



Guidelines for the Submission of Manuscripts

The Canadian Military Journal is the independent flagship quarterly publication of the Profession of Arms in Canada. The Journal publishes professional and scholarly articles, commentaries, opinion pieces, book review essays, and book reviews, as well as select Letters to the Editor.

It welcomes submission of manuscripts on topics of broad relevance to Canadian defence and the Defence Team, including, but not limited to, the profession of arms, security and defence policy, strategy, doctrine, operations, force generation, force employment and force structure, technology, procurement, military history, leadership, training and military ethics, institutional culture, recruitment, diversity, etc. Forward-looking pieces that present original concepts or ideas, new approaches to old problems and fresh interpretation are especially welcome.

The Journal welcomes submissions from members across all uniformed ranks. The Deputy Minister and Chief of the Defence Staff have delegated authority to approve manuscripts for publication in the Canadian Military Journal to the Journal's Editor-in-Chief, acting on recommendations of the Editorial Board. Serving members of the Canadian Armed Forces and civilian employees of the Department of National Defence need not and should not obtain prior clearance from their superior when submitting a manuscript.

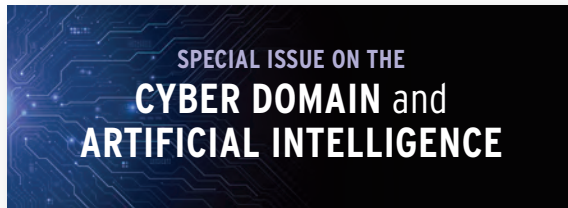
In return, the Journal follows a rigorous double-blind peer review processes that draws on both uniformed and civilian expertise to ascertain suitability of submissions. Manuscripts will be assessed on originality and quality of the argument or discussion, relevance and timeliness of the topic, and quality of the writing style. Unless otherwise agreed upon, the Canadian Military Journal insists upon right of first publication of any given submission. Submissions should not be under review by any other publication while under consideration by the Journal.

Submission Guidelines:

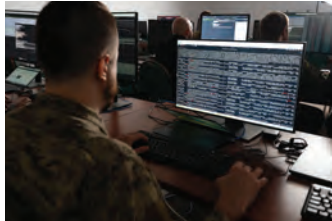
- Authors should submit two copies of their manuscript:
 - The first copy: A complete manuscript with a title, author name, author bio, author contact information, abstract, etc. Named and submitted as "Manuscript X Title-Author Name-Anonymized"
 - The second copy: An anonymized version with the author's name, contact information, and bio removed. Named and submitted as "Manuscript X Title-Anonymized"
- Manuscripts may be submitted in either of Canada's official languages;
- As a general rule, manuscripts should not exceed 5,000 words in length (but may be shorter), including endnotes.
- Manuscripts must be submitted in Word format (.docx or .doc) by email at cmj.rmc@forces.gc.ca;
- Since the Journal is a bilingual publication, manuscripts accompanied by graphics, tables, figures, charts, or maps which support the context of the article must be sent to us separately in a modifiable format to translate them in either official language. Acceptable formats include Word (.docx or .doc), PowerPoint (.pptx or .ppt), Excel (.xls or .xlsx), Vector file (.ai, .eps, .pdf) and any other format that allows the text to be modified. Any supporting photos must be provided in high resolution (minimum 300dpi) in .jpg or .tiff format for print quality and be followed with their appropriate caption and source.
- Manuscripts should conform to standard academic style, using Oxford English or Petit Robert spelling, with endnotes rather than footnotes.
- Endnotes should be embedded and not attached. Full bibliographic references are to be contained in the endnotes. Consult recent editions for examples of appropriate formatting.
- Acronyms and military abbreviations should be used sparingly, but, if unavoidable, they may be used in the body of the text provided that the term is written out in full the first time it is used, followed by the abbreviated form in brackets. Military jargon and slang terms should be avoided: all manuscripts should be readily intelligible to a general informed public readership.

Retraction Policy

The Canadian Military Journal is committed to integrity in publication. In consultation with the Editorial and Advisory boards, the Editor reserves the right to correct the record by publishing a subsequent correction or retraction. Retraction is based on the Committee on Publication Ethics (COPE) guidelines. That is, for an article to meet consideration for retraction, the article must have: unreliable findings (due to major error or falsification), plagiarism, copyright infringement, cases of redundant publication without full disclosure, failure to disclose competing or conflicting interests, substantiated reports of unethical research, or at the Editor's discretion should it turn out that content violates the Journal's ethical, professional, scholarly and other expectations.



CANADIAN MILITARY JOURNAL



A senior instructor at the Cyber Training Unit preparing a simulation exercise.

Photo: Major Charles Paquin, Public Affairs, CAFCYBERCOM



Photo details on page 39



Photo details on page 72

EDITOR'S CORNER

- 4 Foreword
Major-General Dave Yarker
- 6 Note from the Guest Editor
Matthew Kellett

COMMENTARIES

- 9 Canada as a Responsible Technology Power in the 21st Century
Christina Marcotte
- 13 Introduction to Government of Canada Cyber Basics: A Primer
Alexandra Green and Matthew Kellett
- 21 The SIGINT-Cyber Nexus in the Canadian Armed Forces
Lieutenant-Colonel L.J. Rediger
- 26 Forging the Future: An Integrated Canadian Defence AI Ecosystem
Lidia Korczynska
- 30 Artificial Intelligence and the Sino-American Techno-Competition: Implications for Canadian and Allied Defence
Jennifer Gearey and Major Tyler Currie

THE CANADIAN ARMED FORCES MODERNIZATION

- 39 Allied Interoperability Under Pressure: AI, Procurement, and the Future of Defence Cohesion
Samuel Paquette and Major Tyler Currie
- 48 Navigation by Sextant & Astrocompass: A CAF Approach for AI Adoption
Colonel Adam Moore and Matthew da Mota
- 56 Authenticity as a Weapon: The Canadian Armed Forces' Advantage in AI-Enabled Information Warfare
Ali Manouchehri and Major Tyler Currie

THE HUMAN ELEMENT

- 64 Cybersecurity and Air Power: Keeping Humans in the Loop
Kristen Csenkey and Alexis Rapin
- 72 Autonomous Weapons and Cognitive Extension
Major Andrew G. Holt

Canadian Military Journal
PO Box 17000, Station Forces
Kingston, Ontario
CANADA K7K 7B4
E-mail: cmj.rmc@forces.gc.ca



www.Canada.ca/canadian-military-journal

Director and Editor-in-Chief

Professor
Christian Leuprecht

Special Issue Guest Editor

Matthew Kellett, Ph.D.

Editors-in-Chief Emeritus

Professor
Michael A. Hennessy

Lieutenant-Colonel (retired)
John K. Martenson†

Lieutenant-Colonel (retired)
David L. Bashow

Publication Manager

Deesha Kodai

Acting Editor-in-Chief

Alex Green

**Partnerships, Communication
and Special Issue Team Lead**

Katia Dalpé-Charron

Associate Editors

Bruno Charbonneau, Ph.D.

Matthew Kellett, Ph.D.

Paul T. Mitchell, Ph.D.

Editorial Board

Co-chairs

Major-General (retired)
Craig Aitchison
Major (retired) Michael Boire
James Boutillier, Ph.D.
H. Christian Breede, Ph.D.
Vanessa Brown, Ph.D.
Stéphanie Chouinard, Ph.D.
Lieutenant-Colonel (retired)
W.G. (Bill) Cummings
Karen D. Davis, Ph.D.
Barbara J. Falk, Ph.D.
Robert Fonberg
Major-General (retired)
David Fraser
Lieutenant-Colonel
Andrew Godfrey, Ph.D.
Major-General (retired)
Daniel Gosselin
Major Tanya Grodzinski, Ph.D.
Michael Hennessy, Ph.D.
Lieutenant-General (retired)
Michael Hood
Colonel (retired)
Bernd Horn, Ph.D.
Hamish Ion, Ph.D.
Rebecca Jensen, Ph.D.
Matthew Kellett, Ph.D.

Philippe Lagassé, Ph.D.
David Last, Ph.D.
Lieutenant-Commander
Brent Lemon
Adam P. MacDonald, Ph.D.
Vice-Admiral (retired)
Paul A. Maddison
Craig Mantle, Ph.D.
Chris Madsen, Ph.D.
Lieutenant-General (retired)
Al Meinzingher
Paul T. Mitchell, Ph.D.
Mulry Mondélice, Ph.D.
Kerri-Lynn Nankivell, Ph.D.
Alan Okros, Ph.D.
Huw Osborne, Ph.D.
Gaëlle Rivard Piché, Ph.D.
Lieutenant Colonel (retired)
Anne Reiffenstein
Michael A. Rostek, Ph.D.
Grazia (Grace) Scoppio, Ph.D.
Margaret BK Shepherd
André Simonyi, Ph.D.
Elinor Sloan, Ph.D.
Colonel Max Talbot, MD,
FRCS
Colonel (retired) Randall
Wakelam, Ph.D.

Advisory Board

Chair

Major-General
Jeannot Boucher,
Commander, Canadian
Defence Academy (CDA)

Members

Colonel Marty Cournoyer,
representing Chief of the
Air Staff (CAS)
Jill Scott, Ph.D., Principal,
Royal Military College (RMC)
Captain (N) J. Jeffrey
Hutchinson, representing
Chief of the Naval Staff
(CNS)
Brigadier-General Pascal
Godbout, Commandant Royal
Military College (RMC)
Major Chris Young,
representing Chief of Staff
Army Strategy
Lieutenant-Colonel Eric J.
Weaver, Director Canadian
Forces Military Law Centre
(CFMLC), Canadian Defence
Academy (CDA)
Ms. Hanya Soliman,
representing Chief of the
Defence Intelligence (CDI)

NOTE TO READERS

As a bilingual journal, where
citations are translated from
their original language, the
abbreviation [T00] at the end
of the note, which stands for
“translation of original quote,”
indicates to the readers that
the original citation can be
found in the published version
of the Journal in the other
official language.

Subject: Action Required - Confirm Your Subscription to the *Canadian Military Journal*

Dear Subscriber,

In order to update our mailing list, we ask that you confirm your subscriber information and update your contact information. To receive a free print copy of the *Canadian Military Journal*, **please update your subscription preferences** by following the QR code or by clicking the hyperlink below. **If you do not complete this form, your subscription will automatically expire on March 31, 2027.**

To confirm your subscription, please follow these simple steps for one of the two options below:

Access via QR Code

- 1 Connect to WiFi or data.
Open the camera application on your smartphone.
Aim the camera at the QR code.
Tap the notification that appears to open the hyperlink.



2 Access via hyperlink

Download the following hyperlink: <https://forms.office.com/r/RqPPEHKHnS>.

Whichever option you choose, you will be directed to our Microsoft form, where you can **1) confirm your subscription, 2) provide your new mailing address if applicable, and 3) sign up to receive our newsletter**. If you have any **questions or comments**, please don't hesitate to communicate with the *Canadian Military Journal* team by email at cmj.rmc@forces.gc.ca.

Please know that your engagement and readership are vital to us. We look forward to continuing to provide you with the latest research, insights and analysis on the profession of arms in Canada.

Warm regards,

Professor Christian Leuprecht, Ph.D.

Editor-in-Chief

Canadian Military Journal



Attorney Odessa Rossil Magisa, Officer-in-Charge of the Office for DND Information Security, listens to Major-General Dave Yarker, Commander of Canadian Armed Forces Cyber Command (CAFCYBERCOM), during a bilateral Working Group with counterparts from the Armed Forces of the Philippines Cyber Command, held on 10 July 2025 at Camp Aguinaldo, Philippines. The meeting provided an opportunity to exchange operational insights and explore cyber defence cooperation, further advancing Canada's Indo-Pacific Strategy.

Photo: Maj Christopher Daniel, CAFCYBERCOM

Foreword

MAJOR-GENERAL DAVE YARKER

In 2024 Major General (MGen) Dave Yarker was appointed as the first Commander of the newly formed Canadian Armed Forces Cyber Command. Prior to this appointment he filled multiple roles in the Canadian Armed Forces cyber community, including command at unit and formation level and liaison positions with both United States Cyber Command and Canada's Communications Security Establishment. His earlier career included employment within the tactical signals community and joint communications roles. He holds undergraduate degrees in Engineering Physics and History, along with master's degrees in Engineering Physics, Defence Studies, and Public Administration.

It is an honour and a pleasure to be given the opportunity to provide a foreword to this important special issue of the Canadian Military Journal dedicated to cyber and artificial intelligence concerns. With the recent stand-up of the Canadian Armed Forces Cyber Command and the establishment of a formal Defence AI Centre, our warfighting institution has taken some significant steps towards recognizing the importance of these two areas.

Both artificial intelligence and cyber operations are grounded in modern technology and its pervasive impact on warfighting. That impact is simultaneously deep and broad. We have placed modern technology at the heart of our way of war, driving precision in intent, location, and time in the application of violence. However, these technologies are fundamentally vulnerable, opening new avenues of attack and therefore defence, which leads to

“ The question is no longer whether AI and cyber operations will impact the western way of war, but whether we will react to the ways they already have.”

the characterization of cyberspace as a domain of warfare. For its part, AI introduces a radically different scale and speed to many technologies at the heart of warfighting, expanding the influence of technology on our thinking in some cases and entirely replacing the need for humans in others. These are heady topics that any serious professional should be grappling with. Indeed, the very range of the articles in this special issue speaks to the complexity of integrating these key technologies into the profession of arms.

That said, it is impressive to see the talent wrestling with these challenges. On the cyber side, we go from the theoretical underpinnings of policy and foreign affairs in Christina Marcotte's article through the basic definitional grounding provided by Alex Green and Matthew Kellett to the practical reminders of a practitioner in this domain. It is a treat to see these ideas captured in professional writing. On AI, articles in this issue underline the growing influence of the Defence AI Centre, spanning a broad range of

topics and offering practical advice on the implementation of this key technology. The issue also provides an outside view that independently aligns with that vision and its risks.

The topics this special issue challenges us to consider are timely and top of mind. As I write this foreword, I need think back no further than this morning to come up with specific operational examples and recent headlines touching on either AI or cyber security concerns with direct impact on national security and warfighting. Of course, I could have written that statement at almost any time in the past few years, but recent developments have sharpened and accelerated its relevance. We have even seen AI and cyber converge, with models such as Mythos automating the discovery of vulnerabilities in software and contributing to a significant reshaping of the cyber domain.

Therein lies the real reason to engage robustly with the thinking presented in this special issue. We are living through massive shifts in capability brought about by technological advances and witnessing some shockingly rapid shifts in the character of war—even as Ukraine continues to demonstrate its enduring nature as a violent clash of wills. That violence reinforces a central point: the question is no longer whether AI and cyber operations will impact the western way of war, but whether we will react to the ways they already have. This special issue includes a timely and diverse set of perspectives to expand our understanding.

Enjoy.



A G15 Sentinel drone owned by the Advanced Naval Capabilities Unit based in Victoria, British Columbia is parked by the control tent bearing the Canadian Naval Ensign Flag. This drone is used to test interoperability in arctic conditions as part of Operation NANOOK-NUNALIVUT in Inuvik, Northwest Territories on February 27, 2025.

Photo: Master Corporal Alana Morin, Joint Task Force - North, Yellowknife



A member of HMCS MARGARET BROOKE takes a photo of Christ the Redeemer as the ship transits into Rio de Janeiro, Brazil during Operation PROJECTION 25-01 on February 1, 2025.

Photo: Corporal Connor Bennett, Canadian Armed Forces Photo

Note from the Guest Editor

MATTHEW KELLETT

Dr. Matthew Kellett is Special Advisor, Canadian Armed Forces Cyber Command and Associate Editor for Cyber for the Canadian Military Journal. He started his career as a commercial software programmer. He worked as scientific support and then as a defence scientist for 15 years with Defence Research and Development Canada, researching cyber security. Since 2017, he has advised the CAF's operational cyber commanders on the operationalization of the cyber domain with a focus in recent years on concepts, doctrine, and terminology. He has bachelor's degrees in computer science and English literature and a doctorate in theoretical computer science, all from the University of Ottawa.

Welcome to this special issue of the *Canadian Military Journal* dedicated to cyber and artificial intelligence. Cyberspace is everywhere in our lives. From doomscrolling on our phones to endless emails at work, it seems like the most familiar thing in the world. At the same time, we hear about companies being compromised and critical infrastructure being attacked. It can be hard to understand how these two worlds relate.

The truth is that the part of cyberspace we interact with—the interfaces of our iPhones and Windows computers—is a thin skin over a vast infrastructure, and that thin skin makes it seem like everything works transparently as if by magic. There is no magic. There is just a complex system of systems that requires a deep technical skillset to understand.

NATO, Canada, and many of our allies recognize cyberspace as a domain of warfare. In practice, this designation is a recognition that failure to field a specialized military capability in the cyber domain risks losing our ability to operate in all the other domains: sea, land, air, and space. It is for this reason that the Canadian Armed Forces Cyber Command (CAFCYBERCOM) was

stood up on 26 September 2024 as a two-star command under Major-General Dave Yarker and reporting directly to the Chief of the Defence Staff.

CAFCYBERCOM has the Canadian Armed Forces mandate to conduct cyber operations, signals intelligence, and joint electronic warfare. These areas share similar skillsets and, in some cases, are mutually reinforcing. These capabilities are not new. They existed and were operationally effective before the command stood up. The creation of the command simplified the military reporting structure and made these capabilities easier to integrate into military operations.

In this special issue, we look at cyberspace from a few different perspectives. We start with where Canada fits into the world with our expectations about how nation-states should act in cyberspace. *Commentary: Canada as a Responsible Technology Power in the 21st Century* by Christina Marcotte examines the Government of Canada's actions in this space, including how we adapt to new technologies like artificial intelligence and how we govern our actions and link that governance to the rules-based international system.

As I noted above, most people think about phones and computers when they think about cyberspace, what we would collectively call information technology (IT), but cyberspace can be far more than that. In our *Introduction to Government of Canada*

Cyber Basics: A Primer by Alexandra Green and Dr. Matthew Kellett (me), we try to draw a more complete picture of cyberspace in simple terms. Among other things, we talk about areas of cyberspace that users rarely think about, such as industrial control systems, military platforms, and smart lightbulbs; we discuss the difference between cyber security and cyber defence; and we discuss the reason why you rarely hear the term cyber attack in official contexts.

Finally, for the cyber part of this issue, I really wanted to expose this audience to the significance of signals intelligence to military cyber operations. *Commentary: The SIGINT-Cyber Nexus in the Canadian Armed Forces* by Lieutenant-Colonel Leslie Rediger does just that. It shows how these two disciplines, while distinct, share similar characteristics and are mutually reinforcing, which is why they have been grouped together within CAFCYBERCOM.

Artificial intelligence (AI) has been a promise and buzzword for decades. Recent advancements in generative AI, starting with ChatGPT's release in 2022, have changed that conversation. While many technological trends, like 5G, have been touted as the next industrial revolution only to deliver seemingly moderate, incremental improvements, AI has all the appearances and momentum of being revolutionary. Whether you are an AI skeptic or an AI advocate, and I, for the most part, have fallen on the skeptical side of that divide, there is no denying that AI is a collection of



Participants of a Counter-Uncrewed Aircraft Systems course tour a SA-8 air defence vehicle, in Poland, on December 11, 2024.

Photo: Canadian Armed Forces Imagery Technician

emerging technologies that cannot be ignored. We must grapple with it and its implications, and failing to do so may leave us, as a nation-state, at a severe technological disadvantage.

DND/CAF recognized this threat and in May 2024 issued the DND/CAF AI Strategy. The strategy is important in that it applies equally to both DND and the CAF and must satisfy both departmental/corporate requirements and military/operational requirements, which is not an easy task. The strategy has a strong emphasis on the responsible use of AI.

One of the major pieces of the strategy was the establishment of the Defence AI Centre. In *Commentary: Forging the Future: An Integrated Canadian Defence AI Ecosystem* by Lydia Korczynska, we get a first-hand view of the strategy and its implementation in the department from the director of the Defence AI Centre. The strategy sets an ambitious target of DND/CAF being AI-enabled by 2030, and the Defence AI Centre is charged with enabling that goal.

The next two articles come from the Defence AI Centre. *Artificial Intelligence and the Sino-American Techno-Competition: Implications for Canadian and Allied Defence* by Jennifer Gearey and Major Tyler Currie uses the lens of technological competition between China and the United States to discuss how AI is reshaping the defence landscape. It outlines the need for Canada to take decisive action in four key areas: data, compute, institutions, and talent.

Allied Interoperability Under Pressure: AI, Procurement, and the Future of Defence Cohesion by Samuel Paquette and Major Tyler Currie looks at interoperability with our allies, especially NATO, and the challenges that we face. It looks at critical barriers: volatile supply chains, slow procurement systems, and diverging governance models.

The next article, *Navigation by Sextant & Astrocompass: A CAF Approach for AI Adoption* by Colonel Adam Moore and Dr. Matthew da Mota, is notable because it does not come from the Defence AI Centre, but independently raises many of the same concerns. It looks at AI's ability to disrupt military decision-making processes and what that means for how AI is implemented and used in a military context. Simply put, a commander cannot simply blame the AI if something goes terribly wrong, and that reality means that AI will necessarily be used differently in defence than in other areas.

The final article comes again from the Defence AI Centre. *Authenticity as a Weapon: The Canadian Armed Forces' Advantage in AI-Enabled Information Warfare* by Ali Manouchehri and Major Tyler Currie looks specifically at AI-enabled disinformation, which is probably the current most publicly well-known and difficult-to-solve problem from the malicious use of AI. The article offers approaches to countering such disinformation. Interestingly, the solutions are not solely technological.

“ People are a force multiplier in the cyber domain in a way that is unheard of in other domains.”

If I can leave you with one last thought before you dive into the commentaries and articles in this special issue, it is this: in this domain, people are much more important than technology. People are a force multiplier in the cyber domain in a way that is unheard of in other domains. A trained operator or specialist can be magnitudes more effective than someone who has simply been trained to use a tool. While technology can make their work easier or allow them to do more advanced things, technology alone is not sufficient to operate effectively in the cyber domain. AI may change the pace and type of problems presented by the domain, but it is unlikely to supplant people as the major force in the domain for purely practical reasons: the things we care most about in the domain, like a nation-state adversary compromising a computer network, are vanishingly rare compared to the totality of the data available. It is our people's domain expertise and honed intuition that give us the edge. AI may eventually change that equation, but it is unlikely to be soon.

I want to thank all the authors and peer reviewers for making this special issue possible. I am indebted to the Defence AI Centre for their support and significant contributions to this special issue. I am indebted to CAFCYBERCOM for their support of my role as guest editor. I want to thank the members of the command who worked on commentaries and articles for this special issue that ultimately did not make it, mostly due to conflicting operational demands. I hope to bring you some of those pieces in future issues of this journal. A big thank you to the staff at CMJ for managing this issue so professionally. Finally, I want to thank Alexandra Green who expertly guided me through every step of the editing process.

Manuscripts solicited for this issue were written in 2025 and final versions were submitted in March 2026. The necessarily long lead time between writing, final submission, and publication may impact the currency and relevancy of the information presented, especially for quickly evolving topics like artificial intelligence.



The Deck Officer of HMCS MARGARET BROOKE, operates on the bridge as the ship transits to Rothera Research Station, Adelaide Island, Antarctica, during Operation PROJECTION 25-01 on March 15, 2025.

Photo: Corporal Connor Bennett, Canadian Armed Forces Photo

Canada as a Responsible Technology Power in the 21st Century

CHRISTINA MARCOTTE

Christina Marcotte is a deputy director in the International Security Branch at Global Affairs Canada. She spends too much time reading about history and still thinks Vespasian is the most underrated Roman Emperor. The views expressed are her own.

As Canada heads further into the 21st century, I am drawn to the words of 19th century British Prime Minister Lord Palmerston: “We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow.”¹

This commentary will describe actions by the Government of Canada (GC) to protect and advance Canadian security interests in an era of technological power. It will focus on cyberspace and cyber tools, including Artificial Intelligence (AI) (for the purposes of this commentary, I will leave aside the presumed

transformative benefits of AI and other technology on business processes). Within this scope, I will focus on the adoption of technology by the state and the governance of its use, both in a responsible way. Responsibility in this context means actions reinforce the international cooperation that has benefitted

Canada and respect Canadian democratic principles. Doing so in these two ways reinforces the governance systems that have allowed Canada and Canadians to prosper.

On the first point, security in the 21st century requires a state to adapt to changing technologies. Without the adaptation, it leaves Canadians exposed to threats to their personal and financial information and leaves Canada at a disadvantage when facing threats from adversary state and non-state actors. Foreign militaries, espionage agencies, criminals, online activists and other malicious actors operate in cyberspace.

With the vast number of threats facing citizens in cyberspace, it would be a violation of the social contract by Canada towards its citizens not to develop and use tools to counter those threats. The social contract includes the agreement that the government will use the money citizens provide to protect them. The capability to act in cyberspace to disrupt and degrade malicious cyber actors, including criminals and the cyber infrastructure criminals use, is part of that protection.²

On the second point, on governance, this is linked to the Rules Based International System (RBIS). The RBIS is the international context that has evolved since WWII and features multilateralism and its institutions such as the United Nations (UN), international law, treaties, and norms.

Canada's economic prosperity is a result of the RBIS providing stable, predictable rules for global trade and economic interactions. At the same time, the RBIS provides Canada with a stable security situation by providing a system to cooperate on international challenges and to develop mutually agreed-to codes of conduct and behaviour. As one of 193 UN member states, and a middle power in a world of increasing numbers of middle powers along with several superpowers, Canada cannot shape the world to its views. Working with like-minded countries is in Canada's interests. The RBIS provides a known and reliable framework for cooperation. It is not perfect, but its underlying values of equality and predictability are far better for Canada than a system where strength alone determines who wins.

In the context of the RBIS, a core pillar of Canada's principles and processes is responsibility. There are two aspects of responsibility. The first is the responsibility to act; the second, to act responsibly. First, those states that can act, should. It is the act of a responsible state to take action when it can. To contest the space where malicious actors operate. To leave the space uncontested leaves citizens vulnerable and at risk, more than they need to be. This is equally true for Canadian citizens as well as citizens of states that lack the wealth and means to take the same actions as Canada can.

Those actions must also be responsible. Canada must use those tools responsibly, in accordance with the RBIS. Specifically, the Framework of Responsible State Behaviour, which Canada publicly committed to at the UN.³ The Framework includes the recognition that international law applies to cyberspace, the adherence and implementation of agreed-to norms (in particular

the 11 UN norms), implementation of cyber-related Confidence Building Measures, and capacity building for developing states⁴.

Using tools responsibly supports and reinforces the RBIS, the same RBIS that has benefitted Canada. This is critical at a time when the RBIS is facing challenges. Real and current challenges from states that are seeking to re-shape the global system to benefit their interests, regardless of the impact on other states, or to benefit from the weakness of other states in a "might makes right" system.

As a democratic country, Canada's responsible state behaviour also includes accountability and transparency. Accountability means Canada adheres to its obligations under applicable international and domestic law, its commitments to voluntary norms and other public commitments, as well as specific, additional governance such as the military chain of command. Transparency means Canada will be public about its capabilities and how it uses them (not including the details of operations) and subject to the appropriate oversight. Both are important to prevent abuse of power and to ensure citizens' confidence in their government.

Turning first to accountability. Technology is used as a tool of state power, which includes AI, whether for espionage, weapons and arms, or other uses not yet foreseen. Yet technology and AI are not separate from the infrastructure that supports it. When I write, "AI will be used as a tool of state power," it also means "AI will be used in cyberspace and as a cyber tool of state power." Cyber is both a domain and a tool. Cyberspace is a domain of civilian and military activity the same as land, sea, air, and space, a place with dimensions through which operations take place. And it is through the RBIS that states worked out how to govern cyberspace. Canada already has clear rules and norms when it comes to cyberspace and using cyber tools, in particular the Framework for Responsible State Behaviour mentioned above. And as AI is integrated into weapons, the use of those weapons will still be governed by rules of engagement and applicable law.

“Canada already has clear rules and norms when it comes to cyberspace and using cyber tools, in particular the Framework for Responsible State Behaviour.”

AI is also more than the next step in cyber, and it is difficult to anticipate all its potential uses. States are aware of this and are currently working within the RBIS to govern how they use AI as a tool of state power. On the military AI side, there are several plural initiatives specific to AI and military use. These include the

2023 United States-led Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy,⁵ which was launched at the Dutch-led Responsible AI in the Military Domain Summit (REAIM 2023). In addition, NATO's 2024 Revised AI Strategy includes an aim specific to responsible behaviour: "to provide a foundation for NATO and Allies to lead by example and encourage the development and use of AI in a responsible manner for Allied defence and security purposes."⁶ On the multilateral side, there is also UN Resolution 79/239 on Artificial Intelligence in the military domain.⁷

Domestically, the Government of Canada is accountable to its citizens for its actions. Actions over the past several years also speak to its credibility as a responsible actor and in meeting its security commitments to its citizens. Actions by the federal government include the publication of a National Cyber Security Strategy in 2018 and in 2024,⁸ the creation of the Canadian Centre for Cyber Security in 2018, the creation of the RCMP's National Cybercrime Coordination Centre, also in 2018, the prevalence of technologies in the Department of National Defence's 2017 Strong, Secure, Engaged,⁹ and 2024 Our North: Strong and Free,¹⁰ and updated legislation for the Communications Security Establishment in 2019.¹¹

Less visible to the public, but equally important was the creation in 2018 of a unit at Global Affairs Canada to focus on cybersecurity policy internationally and which now also includes AI governance. This unit has the expertise required to represent Canada and Canada's security interests at the United Nations and

other multilateral forums and leads on coordinating Canada's contribution to international initiatives such as the United Kingdom- and France-led effort to counter the proliferation of cyber intrusion tools (Pall Mall Process).¹² In addition to this unit, Global Affairs Canada's international law division has lawyers who specialize in cyberspace. This unit contributed meaningfully to the RBIS and to transparency by the Government of Canada by developing and publishing Canada's position on the applicability of international law in cyberspace.¹³

Other measures taken by the Government of Canada for transparency include 2017's Defence strategy Strong, Secure, Engaged, initiative 88, that specifically says the Canadian Armed Forces would "develop the capability to conduct active cyber operations focused on external threats to Canada in the context of government-authorized military missions. The employment of this capability... will be subject to the same rigour as other military uses of force. Cyber operations will be subject to all applicable domestic and international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments."¹⁴ Whether those cyber tools are enhanced by AI or not, they will still be subject to accountability mechanisms. By being public about the military's use of active (also called offensive) cyber operations and how they will be governed, Canada reinforces the RBIS.

The *Communications Security Establishment Act* (CSE Act) is also public about Canada's active cyber operations. Section 30



Late in the night, a member of the Canadian Armed Forces sifts through information and data while at the Command Post located at the Maria Montez International Airport in the Dominican Republic 04 May 2024. Nearly 300 members are currently on deployment in the region taking part in an ongoing operation to aid the Canadian embassy in Haiti's capital.

Photo: MCpl Mark Wanzel, Canadian Forces Combat Camera, Canadian Armed Forces

of the CSE Act states that the Ministers of National Defence and Foreign Affairs authorize active cyber operations and subsequent sections of the CSE Act detail the types of activities authorized and prohibited and the procedures for authorization.¹⁵

In addition, from both a democratic principle and transparency perspective, the National Security and Intelligence and Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP) play key roles. NSIRA's mandate includes the review and investigation of Government of Canada national security and intelligence activities to ensure that they are lawful, reasonable and necessary.¹⁶ Broadly speaking, NSICOP reviews the legislative, regulatory, policy, administrative and financial framework for national security and intelligence and any activity carried out by a department that relates to national security or intelligence.¹⁷ NSIRA and NSICOP must each submit to the Prime Minister an Annual Report, and the Prime Minister tables the Committee's reports in both Houses of Parliament.

On a last note, being a responsible technological actor also gives Canada credibility when increasing cooperation with partners and allies. The scale and scope of the threats mean Canada cannot protect its security alone, and these partnerships are essential. They are essential to understand the threats, develop the best ways to mitigate and manage the threats, and to counter them. Working together takes trust; it takes even more trust to work effectively together. This credibility, from the congruence between Canada's behaviour and its words, helps establish

“Being a responsible technological actor also gives Canada credibility when increasing cooperation with partners and allies.”

Canada as a trusted partner. This includes in longstanding partnerships such as NATO, as well as newly developing and deepening ones as Canada pursues its Indo-Pacific Strategy.

As Canada looks towards the future, as Canada meets its security needs in the years ahead, Canada will continue to be a responsible state player in cyberspace and will be as new technologies are introduced. This includes how Canada will use AI and any other technology as a tool of state power. New technological advancements and the developments associated with them will not change the social contract between Canadians and their government, nor the government's continued work to protect its citizens. The actions taken to date by the GC demonstrate this commitment. Continuing to act as a responsible state player demonstrates the commitment to the governance systems internationally and domestically that have allowed Canadians to prosper.

Notes

- 1 Viscount Palmerston, "Treaty of Adrianople—Charges Against Viscount Palmerston," House of Commons Debates, March 1, 1848, *Hansard*, vol. 97, c. 122. Originally found at: <https://api.parliament.uk/historic-hansard/commons/1848/mar/01/treaty-of-adrianople-charges-against>.
- 2 Jacques J. M. Shore, "An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security," *International Journal of Intelligence and Counterintelligence* 28, no. 2 (2015): 238. Originally found at: <https://doi.org/10.1080/08850607.2014.962356>.
- 3 Global Affairs Canada, "International Cyber Policy," accessed August 11, 2026. Originally found at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyber_policy-politique_cyberspace.aspx?lang=eng, citing UN General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/70/237 (December 23, 2015).
- 4 UN General Assembly, *Group of Governmental Experts*, A/RES/70/237.
- 5 US Department of State, Bureau of Arms Control, Deterrence, and Stability, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, November 9, 2023, <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/>.

- 6 Summary of NATO's Revised Artificial Intelligence (AI) strategy, 5, 11, 10 July 2024. Originally found at: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
- 7 UN General Assembly, *Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security*, A/RES/79/239 (December 24, 2024).
- 8 Public Safety Canada, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age* (Government of Canada, June 2018). Originally found at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrg/ntnl-cbr-scrtrg-en.pdf>; Public Safety Canada, *National Cyber Security Strategy: Securing Canada's Digital Future* (Government of Canada, 2025), <https://www.public-safety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrg-2025/ntnl-cbr-scrtrg-2025-en.pdf>.
- 9 Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy (Government of Canada, June 2017). Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html>.
- 10 Department of National Defence, *Our North, Strong and Free: A Renewed Vision for Canada's Defence* (Government of Canada, April 2024). Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html>.

- 11 Communications Security Establishment Act, SC 2019, c 13, s 76. Originally found at: <https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html>.
- 12 United Kingdom, Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States* (Government of the United Kingdom, April 4, 2025). Originally found at: <https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states>.
- 13 International Law applicable in cyberspace. Originally found at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyberspace_law-cyberespace_droit.aspx?lang=eng.
- 14 Department of National Defence, Strong, Secure, Engaged, p 73.
- 15 *Communications Security Establishment Act*, s30.
- 16 National Security and Intelligence Review Agency Act, SC 2019. Originally found at: <https://laws-lois.justice.gc.ca/eng/acts/N-16.62/page-1.html>.
- 17 *National Security and Intelligence Committee of Parliamentarians Act*. Originally found at: <https://laws-lois.justice.gc.ca/eng/acts/N-16.61/page-1.html>.



Members of HMCS Ottawa's operations department sit in the Operations Room of HMCS Ottawa while the ship sails in the South China Sea during Indo-Pacific Deployment on October 4, 2023.

Photo: Aviator Gregory Cole, Canadian Armed Forces Photo

Introduction to Government of Canada Cyber Basics: A Primer

ALEXANDRA GREEN AND DR. MATTHEW KELLETT

Alex Green served as the first ever Officer in Charge for the Fleet Cyber Team at Maritime Forces Pacific (MARPAF) from 2018 to 2020. She is currently pursuing a Ph.D. in War Studies at the Royal Military College of Canada, where she studies cyber terrorism. In 2024, she received the Franklin Pinch Award for her research on custom terrorist app development.

Dr. Matthew Kellett is Special Advisor, Canadian Armed Forces Cyber Command. He is a former commercial software programmer and defence scientist. His doctorate is in theoretical computer science, specifically on the design and analysis of distributed algorithms. He enjoys chess, running, and curling and is a former president of the Ottawa Curling Club.

The Canadian Armed Forces (CAF) and the Department of National Defence (DND) are rushing to meet the demand for cyber security capabilities. The CAF introduced the Cyber Operator trade in 2017,¹ and the Canadian Forces School of Communications and Electronics (CFSCE) announced the first graduating class in 2021.² Three years later, in September 2024, the CAF officially established the Canadian Armed Forces Cyber Command (CAFCYBERCOM). This command is the single DND/CAF authority for cyber operations, encompassing signals intelligence and joint electronic warfare. The creation of CAFCYBERCOM is significant because it consolidates several pan-domain efforts to leverage cyber capabilities into a single, transparent, unified chain of command, providing a “one-stop shop” for cyber expertise.

In the seven years leading to the stand up of the CAF Cyber Command, the CAF created a new trade and graduated its first Cyber Operator cohort. The CAF is investing in cyber capabilities. Staffing was once a challenge, but the number of qualified operators is growing. Despite this growth, a 2020 report by the Director General Evaluation, entitled “Evaluation of the Cyber Forces,” found that the “Cyber Forces have a sufficient number of positions; however, filling the positions has proven to be difficult” and points to challenges associated with hiring and retaining civilian talent, and matching cyber capability needs with the traditional approach to military professional development. The report specifically cited frustration associated with “the most experienced cyber personnel working for those who have little cyber experience.” The establishment of the Command should go a long way toward resolving these issues.

The situation is improving as the cyber operator trade matures and the Cyber Training Unit produces trained operators. While this capability is growing rapidly, basic cyber literacy in the rest of the DND/CAF has not kept pace. Defence Team members are often posted into positions requiring cyber knowledge without much background. Many of these uniformed members are not digital natives. It is understandable, given that the average age of a uniformed member in the CAF is 36 years old,³ and the World Wide Web became accessible to the broader public 30 years ago, meaning the average CAF member was not born into a world with the Internet. Most senior leaders in the Canadian Armed Forces are older than 30, so it is also fair to assume that many were not born into a fully Internet-connected and mediated world. They represent a generation of the CAF that must interact with cyber militarily, but for whom the Internet was once a novel idea that came about at the start of their careers. As the CAF expands and prioritizes cyber operations and capabilities, many CAF members must quickly adopt and understand cyber terminology.

There are, of course, many members of the Canadian defence community who are familiar with both technical and non-technical elements of cyber security. Those members might find this article to be a helpful refresher, although, for the most part, it is intended to serve as a welcoming primer to establish a baseline knowledge level for uniformed and non-uniformed members who have just been posted into a position where they engage with these concepts.

Aside from introducing some basic terms in a military framework, this article addresses common misconceptions these new team members might encounter. First, we discuss some common terms. While Government of Canada employees may have access to joint doctrine notes, the Defence Terminology Bank, and Termium, we believe that having terminology in one article, along with examples, will help new members adjust more quickly. We outline terms such as *cyberspace*, the *cyber environment*, the *cloud*, *cyber domain*, and *cyber* as an adjective. We then discuss how cyberspace is often viewed as a monolith and explain the nuances between different types of technology that fall under the

cyberspace umbrella. With these nuances in mind, we differentiate cyberspace from the information environment. The two are often confused because cyber teams are often asked to support information effects. We also explain the popular castle analogy, and how it can be used to understand the difference between cyber operations and network operations. The article finishes with two other key distinctions: the first between cyber security and cyber defence and the difference between a cyber event, cyber incident, and cyber attack. After completing this article, readers should have a solid foundation for more in-depth concepts and discussions.

Common Definitions and Terms

First, we explain common terms before diving into the nuanced differences between concepts. Any defence community member knows that the CAF and DND can be an alphabet soup full of acronyms and confusing terms. So, it is pertinent to address some standard terms readers might encounter in their work. For the CAF/DND, the *cyber operating environment*, *cyber environment*, or *cyberspace* for short, is a physical environment like sea, land, air, and space are physical environments. There is a physical infrastructure underlying and inseparable from the virtual world. Every piece of equipment a user touches is connected to another piece of physical equipment somewhere else, either through wires and fibre-optic cables or through photons sent through air and space. The cloud is not actually a cloud; it's usually a giant warehouse filled with networking equipment and computer servers running software that ensures data continues to survive even after the hardware it is stored on inevitably fails. So, instead of storing your data on your physical device, that data is stored on a server or group of servers and accessed over the Internet or some other large network. That's where our first buzzword, cloud, originated from. Network engineers, computer scientists, and other experts drawing network diagrams would conventionally use a cloud-like symbol to act as a placeholder for complex, underlying infrastructure that was outside of the organization's control. As organizations such as Amazon and Google began to offer computing resources remotely, the cloud was marketed as a new type of service delivery, as organizations would interact with those services without direct control of the infrastructure.

Next, the *cyber domain* is cyberspace, plus everything around it that supports it, including people, processes, and infrastructure. The Government of Canada uses this term to describe “all infrastructure, entities, users and activities related to, or affecting, cyberspace.”⁴ The cyber domain can include checking a new employee's identification before giving them their credentials to access the corporate network, the security of the rooms holding servers and networking equipment, and even the people who administer the network, which are all things vital to maintaining cyberspace, yet are not actually in cyberspace. Canada, NATO, and many allies have recognized the cyber domain as a

“*Cyber planning* is just military planning applied to the cyber domain; nothing is particularly cyber about it and it should just be called what it is: planning.”

domain of warfare, just like the maritime, land, air, and space domains. That recognition means the CAF must be prepared to carry out military operations in the cyber environment (i.e., cyberspace), and the CAF must be able to defend its part of the cyber domain.⁵

Cyber, then, is just an adjective, meaning that the thing it modifies is related to the cyber domain or cyberspace. Think about its use in terms of cyber security, cyber operations, and cyber incidents. *Cyber* also gets overused. In a military context, readers might hear people use the term *cyber planning* far too often. *Cyber planning* is just military planning applied to the cyber domain; nothing is particularly *cyber* about it and it should just be called what it is: planning. *Cyber* also should not be used as a noun or verb, although that often happens in informal speech. You should never write, “They should use cyber on this” or “We should cyber that.” In the next section, we will break down the *cyberspace* umbrella and then differentiate it from the information environment.

Breaking Down Cyberspace: OT, PT, and IoT Explained

While it is common practice to lump everything together under the term *information technology* or *IT*, the CAF/DND needs to be more precise about the components of cyberspace to manage them correctly. In CAF/DND, we use *IT* to refer to the traditional office and networking infrastructure to distinguish it from operational technology, which runs physical systems like pumps and heaters, and platform technology, which is operational technology on military platforms like ships, engine controls, and missile guidance systems. We can divide cyberspace into subcategories: information technology (IT), operational technology (OT), and platform technology (PT). It is also worth mentioning where Internet of Things (IoT) devices fit in among these categories. If you are new to the field, you will likely hear these terms used in reference to government assets. We’ve simplified the definitions below to help make the concepts more relatable.

Operational Technology (OT)

Operational technology is all about cyber-physical industrial systems. It includes industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. In your home, the thermostat that controls your furnace is an example of OT. OT provides the interface between cyberspace and physical systems like valves, dampers, and fans on everything from heating, ventilation, and air conditioning (HVAC) equipment to fuel pipelines. While it is often possible to update the computer code of these systems, it usually only happens during infrequent overhauls or, in the worst case, when they are replaced. Sometimes, these systems are hard to update because they support critical systems. You wouldn’t want to shut down a water treatment plant or take safety systems offline at a nuclear power plant regularly to update their software.

In some cases, updating is difficult or impossible because the device is inaccessible. For example, you may have to drain portions of the water treatment plant to access certain equipment, or a critical control may be in a radioactive zone of a nuclear power plant. While OT systems connect cyberspace and physical systems, the best practice is to isolate them on their own networks and not, for instance, connect them directly to the Internet.

Platform Technology (PT)

Platform technology (PT) refers to the operational technology used on military platforms. It includes the hardware and software on ships, aircraft, vehicles, and weapon systems. Like your car, all the chips and wires used to control the functions of an armoured vehicle are examples of PT. PT often includes dedicated processors or chips that control the platform’s functions, like a missile guidance system. It is often nearly impossible to replace these chips, so any vulnerabilities in them exist for the lifetime of the equipment.

Because updating or replacing OT and PT is difficult, we need to ensure their security and ensure that updates don’t introduce vulnerabilities. This protection is part of a larger effort called *cyber mission assurance*, or CMA, which is defined by the Government of Canada as “a process to protect or ensure the continued function and resilience of mission-essential capabilities and assets, in the face of cyber threats or actions, in any operating environment or condition.”⁶ Essentially, CMA is the ability to conduct military operations with military capabilities that rely on cyberspace, which may be contested. In a Navy context, for example, a ship should still be able to use networks and technical capabilities to fight, float, or move in a cyber-contested environment. CMA can also mean ensuring these systems’ security and supply chains during their development and after they are fielded. Given that technical supply chains are often global in nature, there is always the risk that the systems, software, and technical capabilities the CAF acquires will eventually be



Members of 437 Transport Squadron help with the assisted departure of evacuees from Tel Aviv, Israel to Athens, Greece as part of Operation ION on October 15, 2023.

Photo: Corporal Charles Audet, Canadian Armed Forces Photo

exploited. Commanders who adhere to CMA principles must have contingencies to continue to pursue the mission regardless of the cyber threat.

Internet of Things (IoT)

Internet of Things (IoT) devices are becoming less expensive, more convenient, and easily adaptable, so it would not be surprising if IoT devices eventually provide some critical capability in a military operation. The Internet of Things includes low-end, consumer-grade IT and OT. Examples of IoT include smart lights, smart locks, smart appliances, Internet-connected thermostats, Internet-connected cameras, Internet-connected doorbells, and Internet-connected baby monitors. They often provide helpful capabilities, like using a camera to monitor your property or having your smart fridge order more milk when running low. IoT devices are often cheap, use low-powered processors, have minimal or no security, and can be difficult or impossible to update.

As the Canadian Armed Forces face a more complex threat environment and navigate challenging procurement processes, IoT devices, which were previously new and difficult to integrate, now offer easy solutions. However, these devices present a *cheap complexity problem*.⁷ Historically, if the Canadian Armed Forces wanted to acquire a specialized and complex machine or device, they would need to find a specialized supplier. The complex device would cost a great deal, given the effort and resources required to create it. However, things are different with IoT devices. Today, it's often less expensive to take a complex device and have it pretend to be simple, instead of actually building a simple device. By default, due to the economies of scale (it is cheaper to make millions of one item than to make a handful of bespoke items), vendors are incentivized to make IoT devices with

all the bells and whistles: WiFi, cloud storage, machine learning, complex software, Bluetooth, and microphones. But if an organization (such as the CAF) wanted that device for an operational capability without the WiFi connectivity, it is often cheaper and easier to turn off the WiFi connection than to manufacture a bespoke version without that feature. Nevertheless, that lingering feature is still a vulnerability, and as IoT devices are notorious for infrequent firmware updates, it may remain unpatched and open to exploitation.

These characteristics make IoT devices an ideal target for exploitation by malicious actors. For instance, the Mirai botnet was first noticed in August 2016. It took advantage of hundreds of thousands of poorly secured IoT devices, like baby monitors and Internet-connected cameras, to create a network that could flood targets with network packets in a distributed denial of service (DDoS) attack.⁸ While its initial target was *Minecraft*, it has been used for many other attacks and eventually had its source code released in an open-source code repository.⁹ Despite their security concerns, the use of these devices is increasing due to convenience. It would be unsurprising if they were to provide some critical capability in a military operation at some point in the future. If that's the case, we need to be aware of the risks involved, just as we should be of the risks involved in using them in our homes.

The Difference Between Cyberspace and the Information Environment

Readers new to the field might use *information environment* and *cyberspace* interchangeably. But, what is the information environment? The Government of Canada defines the information environment as "an environment comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs."¹⁰ Except that is not the only definition. There are several others, and the Canadian definition is not universal. For example, according to the Tallinn Manual, the comprehensive (but non-binding) academic survey of international law applicability to cyber warfare and cyber operations, the information environment is the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."¹¹ The two definitions differ, as the Tallinn Manual description focuses on the actors and systems only, while the Government of Canada definition includes the actors, systems, and the environment they interact with. On that note, the Government of Canada definition explicitly mentions information as part of the system, while the Tallinn Manual definition does not mention information as a commodity. Furthermore, although the Government of Canada definition defines explicitly the information environment as an environment and emphasizes this context, the definition does not address the broader *environment* as a concept.

“ Unlike the maritime, land, air, space, and cyber environments, the information environment is not physical, although it does interact with the physical environment as a medium.”

Unlike the maritime, land, air, space, and cyber environments, the information environment is not physical, although it does interact with the physical environment as a medium. For example, if troops from country A deploy to allied country B to deter aggression from country C, and country C does not yet want to commit to traditional military action against country B, they can leverage the information environment. Country C could create social media accounts and bots to spread disinformation about country A's activities in country B: that country A troops are terrorizing the local population, leaving garbage, and committing crimes. In this example, all the comments the bots leave on social media are elements of the information environment. Country C uses hardware to enable the bots—servers to host the bot networks, store user data, logs, and power to integrate with social media apps—and that hardware is part of cyberspace. Some of that social media content might make its way to a newspaper, where those claims will be printed in physical form. Country B citizens will view those messages on physical devices, accessed via the Internet. Those devices are also part of cyberspace. If country B citizens believe those claims, and change their opinion about hosting country A, then the information environment has been altered.

This example also illustrates the distinction between information operations and cyber operations, which differ in their objectives and nature. Information operations are focused primarily on the information environment and changing how a target perceives information. Information operations are “coordinated information activities conducted in or through the information environment to create desired effects on the will, understanding and capability of individuals.”¹² There are a few critical elements to this definition: actions or operations must be deliberate and synchronized, with the intention to achieve specific outcomes or results and focus on people as the primary targets. Suppose Bob emails Alice about the highlights of his project with the intent to ask her for funding later. That email is an information operation because Bob positively changes her perception of the project.

While information operations intend to alter the subject's perception or behaviour, cyber operations are used to change the medium of cyberspace by allowing things that would usually be denied, intentionally or not, or to deny things that would usually be allowed, intentionally or not. Cyberspace is central to cyber operations. You cannot achieve a cyber operation without the infrastructure of cyberspace. Standard definitions highlight this connection. For example, the Government of Canada defines a cyber operation as a “set of planned actions in or through cyberspace intended to preserve freedom of action or create effects to achieve military objectives.”¹³ More plainly, the Tallinn Manual lists a cyber operation as “the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.”¹⁴ When we hear *cyber operations*, we tend to think of elaborate, Stuxnet-level capers. However, a cyber operation could be as simple as applying a patch to intentionally combat a known virus and, ultimately, changing cyberspace to improve network health.

Why are cyber operations and information operations often confused, and how do they relate? First, both aim to create effects, whether on the human psyche (information operations) or technical systems (cyber operations), and these effects can sometimes overlap. Some might assume that information operations are cyber operations because cyber operations could be used in conjunction with information operations. As mentioned, cyberspace is a medium that people use to access the information environment (e.g., using a computer to research). We often confuse cables, servers, and routers (the physical elements of cyberspace) with the information environment, because we can use them to communicate information. The two are also often confused because at one point, information operations and cyber operations were treated as the same category. The two concepts are further conflated because cyber-designated teams are usually tasked with affecting the information environment: a cyber operation can have information-related effects, and information operations can leverage cyberspace. For example, if Alice is still hesitant to fund Bob's project, Bob could hire Eve to send a key logger (a hidden app that records keystrokes and sometimes the screen) to infect Alice's computer and gather blackmail-worthy information. Bob could then use that information to influence Alice's decision. But it is possible to carry out that information operation entirely separate from cyberspace. For example, Bob could staple posters with disinformation about Alice's research to stir up unsupportive sentiment on campus.

There are ways to influence the behaviour or decisions of a target audience without cyberspace. We've used a fictional example here to demonstrate the difference between information and cyber operations, and the next section explores the popular castle metaphor to highlight the distinctions between cyber operations and network operations. The article then differentiates between cyber defence and cyber security.

“Beginners might encounter the fortress/castle metaphor as a simplified explanation of how a network or computer is secured.”

The Castle Metaphor: Cyber Operations and Network Operations

Beginners might encounter the fortress/castle metaphor as a simplified explanation of how a network or computer is secured. Using the metaphor, a defender can secure an asset behind layered defences, like medieval rulers who might fortify a structure with a moat and thick castle walls, perhaps rounded to prevent an adversary from scaling, with inner walls to zone the castle into different levels of access (outer bailey, inner bailey, keep). Even though the layers of defences reduce the risk of a breach, there is always the risk that an enemy force might try to breach the defences. Similarly, digging a moat and erecting castle walls does not mean the work is done. The defenders must evolve as their adversary evolves. If the walls protect from arrows and slings, there is no guarantee that the walls and moat will be sufficiently protected from catapults. Additionally, the defender must consistently maintain these defences. The walls must be repaired if damaged and manned to watch for enemies and anyone attempting to scale the walls.¹⁵

There are obvious parallels to a network. The castle walls are often likened to a firewall, allowing entrance to some but not others and providing a defensive perimeter. The inner castle walls are also similar to network zoning, in which different network parts are segmented according to privileged access. So, if an attacker breaches the castle walls, they may be unable to access the inner bailey or the keep. Requiring a password could be similar to lifting the portcullis. Like a castle, the network defences must constantly be updated as enemies evolve: network defenders must apply patches, update malware signature lists, and fine-tune their allow and deny lists. The process is never ending.

The defence can also be even more active. If you were to send your troops out beyond the wall to find the catapult and destroy it, we would call those actions *defensive cyber operations—response actions* (DCO-RA), which is just another way of saying self-defence in the cyber domain to ensure freedom of action.¹⁶ If you were to target the adversary's troops and to destroy their castle, or to capture their flag and plant your own, in the cyber world, we would call those *offensive cyber operations* (OCO), as it is an operation to “project power in or through cyberspace to achieve effects in support of military objectives.”¹⁷ In a cyber security context, that could look like overloading adversary

infrastructure with traffic to disrupt their ability to launch disinformation campaigns.

The castle analogy can also be used to articulate the differences between cyber operations and network operations. We've already touched on cyber operations, but network operations are understood to be the “activities undertaken to provision, secure, configure, operate, extend, maintain and sustain a network.”¹⁸ Following our castle analogy, these would be the general activities needed to sustain the castle: ensuring that the castle walls are maintained, resources such as food, water, and weapons are available, the doors function so people can enter and leave, and that guards are present to guard the castle walls and entrance. These functions are similar to the elements of network operations: firewalls, access control lists, bandwidth availability, and network administrators available to troubleshoot. If the castle walls are falling apart, it may be difficult to know if it is because of an attacker, or because the walls are so poorly maintained. The same can be said with network operations. If some devices are no longer connected to the network, it could be because a malicious actor has targeted them, or because the network operations centre did not update the firmware and the recent patch caused the devices to disconnect. If a network is poorly maintained, as a castle, then it is challenging to know readily whether an issue is routine or malicious.

However, there are general limits to the castle analogy. First, it establishes a dangerous dichotomy between *inside* and *outside*.¹⁹ Not all networks are clear-cut. For example, many networks have demilitarized zones (DMZs) where they host assets accessible to the Internet, yet cannot interact directly with internal databases. So, the DMZ is a type of intermediary zone that is protected by the firewall but is still not entirely internal. Second, the castle analogy suggests that all threats originate externally. While castles did not usually prioritize internal defences, modern networks often use role-based access controls to limit privileges once in the network. However, even with these controls, insider threats (Ortis, Snowden, Reality Winner, Manning, etc.) prove that not all threats are external.²⁰

Cyber Security vs. Cyber Defence: Key Differences Explained

If you're new to cyber security in the Department of National Defence, you might've noticed that sometimes people use cyber security and defence interchangeably, despite the fact that they are entirely different terms within the department. Within the broader government, cyber security would be used to describe the processes for securing the IT portion of cyberspace. However, within DND, cyber security and cyber defence are divided. Unlike other departments, DND has platform technology and must defend that technology from adversaries in operational contexts. Cyber security provides the necessary foundation for all cyber defence activities, which could be part of the reason the

two terms often need clarification. Cyber security includes activities that ensure the health and safe storage of assets, regardless of the presence of a threat actor. Confidentiality, integrity, and availability are priorities. Confidentiality ensures that information is private and accessible only to the people granted permission to see it; integrity ensures that information stays accurate and unchanged; and availability means that users can access the information they need when needed, without delay or difficulty.²¹

In practice, cyber security could involve requiring users to use passwords to access assets or systems, using role-based access controls to control access and privilege (confidentiality), using checksums to check that the software is the proper version for download (integrity), requiring digital signatures (integrity), having a disaster recovery plan in the event of a natural disaster or emergency (availability), or monitoring the system's performance (availability).

So, how is cyber security different from cyber defence? Indeed, cyber security practices can help deter a threat actor from accessing, altering, or denying access to data. However, cyber defence is different because, unlike cyber security, it assumes the presence of a cyber threat actor and involves efforts to detect, prevent, and respond to threats against the network. A cyber threat or threat actor is central to this definition but absent from the cyber security definition.

While no analogy is perfect (as demonstrated earlier with the castle analogy), we can see the difference between the two concepts using a hockey reference. Cyber security is much like the net outside of a hockey game. The smaller the frame of the net, the harder it is for unwanted materials (including a puck) to enter the goal zone. Perhaps the net is still on the ice during public skate hours, and some toddlers wander in accidentally. Hopefully, rink maintenance staff will be present to keep the net intact and out of bounds. If an overzealous skater accidentally slammed into the goal and ripped the netting, rink maintenance staff would repair the tear so the net could function as needed. Maintenance staff will replace the frame if it rusts to preserve structural integrity. The same staff might then remove the net from the rink during public skating to ensure it is accessible for games. These practices are all similar to standard cyber security maintenance—ensuring that unwanted traffic is kept away from the network and that if the network is accidentally damaged, it is repaired and perhaps isolated from any other incidents that could impact network availability—all standard practices.

In contrast, cyber defence is analogous to a hockey game. The net can be thought of as cyber security. The better the cyber security, the smaller the net (and smaller the threat surface). The net can be made of better material, might have a robotic opening, replaced and renewed with every change, etc. All these adjustments make it more difficult for the opposing team to score. In this way, it is similar to cyber security practices, whereby network owners might adjust firewall rules and routinely apply patches to limit the network's threat surface. Nevertheless, like hockey, no

matter how well-crafted your net is (or cyber security practices), if you don't have a goalie, the adversary can easily score. Cyber defence is similar to adding a goalie. The home team puts a goalie in the net to keep pucks out. The bigger the goalie pads and the faster her reaction, the harder it is for the other team to score. The coach might brief the goalie and defence about the other team's forwards and the strategies or plays they like to use. The home team can then use this intelligence to prevent the other team from scoring. Similarly, with cyber defence, the network defenders can invest in malware signature detection tools (new equipment) to prevent a cyber threat actor from breaching the network. They might also use heuristic analysis, intrusion detection systems, or knowledge of techniques, tactics and procedures to identify specific threat actors, mitigate the threat, or improve response times. In this example, the team must take specific defensive actions to protect itself from the other team. However, unlike in a hockey game, cyber defence and cyber security are 24-hour efforts that never truly end. The difference between the two will also be useful for the next section, which outlines the gradient of cyber events, incidents, and compromises.

Distinguishing Cyber Events from Cyber Attacks: Understanding the Scale

Cyber activities or oddities sometimes get lumped together in the *cyber attack* pot. However, there are technical differences. We must distinguish between types of activities so we can scale responses. For example, if you're new to a team and get a phishing email (but didn't click on it) and claim that there's been a cyber attack, that label is wrong and also incorrectly escalates the activity. The Government of Canada uses definitions in the Government of Canada Cyber Security Event Management Plan to differentiate between types of activities.²² The main difference between the categories is the level of severity and our certainty that there was a compromise.

On the less significant end of the scale, we have a *security event*, which is any event that may have resulted in a compromise.^{23,24} Examples of security events include a spear phishing email that the target did not click on or unusual requests stopped by a firewall. While some of these events could be malicious, it's essential to recognize that an event is not the same as a compromise. If an organization treats every event as a breach, it will be overwhelmed by the number of alarms, leading to alarm fatigue, and precious resources will be stretched thin.

A security event can become a *security incident* when a breach occurs, and the system is compromised.²⁵ For example, if a cyber threat actor sends a spear phishing email to an employee and the employee clicks on an embedded malicious URL or opens an infected attachment and downloads malware, the security event (the email) becomes a security incident (successful malware download). The event transitions to an incident as soon as the network is compromised.

Conclusion

We have written for an audience new to the Government of Canada's cyber security community in the hopes of helping those readers identify common misconceptions they might encounter. After reading this article, we believe everyone should have the same foundational knowledge. Readers should see that cyberspace is a physical thing, mundane and unexciting as that might seem to some. The cyber domain is cyberspace and all the things that go around it. It is also one of the five recognized domains of warfare, one that the Canadian Armed Forces is actively operationalizing.

Is this article just splitting hairs? Why do we need an entire article to outline definitions already used in a web of Joint

Doctrine Notes, policy papers, annexes, glossaries, and slide shows? Why does it matter if we say *cyber operation* instead of *information operation* if most people know what we truly mean, anyway? The truth is that the CAF/DND are in a unique situation. Unlike the US, China, and Russia, they are building the foundation of critical military cyber capabilities. As CAF CYBERCOM stands up and several teams interact with this capability, it's important that everyone speaks the same language and uses terms appropriately to avoid confusion and miscommunication. Hopefully, the simplified explanations presented in this article provided a better understanding of how the cyber domain is put together, its relation to the other domains, and why it may actually be more straightforward than people believe it is.

Notes

- 1 Government of Canada, "Cyber Operator: The New Canadian Armed Forces Trade Badge," The Maple Leaf, January 11, 2022. Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2022/01/cyber-operator-canadian-armed-forces-trade-badge.html>.
- 2 "Congratulations to the First Cyber Operator Graduates from the CFSCE," The Maple Leaf, September 21, 2021. Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2021/09/congratulations-first-cyber-operator-graduates-cfsce.html>.
- 3 Government of Canada, "March 2020 - Canadian Armed Forces 101," Defence 101- Transition Binder 2020, n.d., 2. Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101-caf-101.html>.
- 4 Government of Canada, "Cyber Operator: The New Canadian Armed Forces Trade Badge." Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2022/01/cyber-operator-canadian-armed-forces-trade-badge.html>.
- 5 Statistics Canada, "On Guard for Thee: Serving in the Canadian Armed Forces" (Government of Canada, July 13, 2022). Originally found at: <https://www150.statcan.gc.ca/n1/daily-quotidien/220713/dq220713c-eng.htm>.
- 6 Government of Canada, "Cyber Mission Assurance," in *Defence Terminology Bank*, n.d. Originally found at: https://www.btb.termiumpus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=cyber+mission+assurance&codom2nd_wet=1#resultrecs
- 7 Bruce Schneier, "Security and Cheap Complexity," *Schneier on Security* (blog), August 26, 2022. Originally found at: <https://www.schneier.com/blog/archives/2022/08/security-and-cheap-complexity.html>.
- 8 "Heightened DDoS Threat Posed by Mirai and Other Botnets," CISA, n.d. Originally found at: <https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets>.
- 9 Scott J. Shackelford and Scott O. Bradner, "Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything," *Hastings Law Journal* 72, no. 2 (2021). Originally found at: https://repository.uchastings.edu/cgi/viewcontent.cgi?article=3921&context=hastings_law_journal.
- 10 Government of Canada, "Information Environment," in *Defence Terminology Bank*, n.d. Originally found at: <https://www.btb.termiumpus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=information+environment>.
- 11 "Glossary," in *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), 282.
- 12 Government of Canada, "Information Operation," Termium Plus, n.d.
- 13 Government of Canada, "Cyber Operation," Termium Plus, n.d.
- 14 "Glossary."
- 15 Deborah A. Frincke and Matt Bishop, "Guarding the Castle Keep: Teaching with the Fortress Metaphor," *IEEE Security & Privacy*, 2, no. 3 (2004): 69-72.
- 16 Government of Canada, "Defensive Cyber Operation - Response Action," Termium Plus, n.d.
- 17 Government of Canada, "Offensive Cyber Operations," Termium Plus, n.d.
- 18 Government of Canada, "Network Operations," in *Defence Terminology Bank*, n.d.
- 19 Christian Leuprecht, David B. Skillicorn, and Victoria E. Tait, "Beyond the Castle Model of Cyber-Risk and Cyber-Security," *Government Information Quarterly* 33, no. 2 (n.d.): 250-57.
- 20 Christian Leuprecht, David B. Skillicorn, and Victoria E. Tait.
- 21 National Institute of Standards and Technology, "NIST Special Publication 1800-26A" (National Cybersecurity Center of Excellence, 2020). Originally found at: <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html>.
- 22 Government of Canada, "Government of Canada Cyber Security Event Management Plan (GC CSEMP)" (Government of Canada, 2019). Originally found at: <https://www.canada.ca/en/government/system/digital-government/online-security-privacy/cyber-security-guidance-policy/management-security-incidents/government-canada-cyber-security-event-management-plan.html>.
- 23 Government of Canada.
- 24 National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," NIST, n.d. Originally found at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- 25 National Institute of Standards and Technology.



435 Transport and Rescue Squadron transports evacuees from Norway House, Manitoba, due to forest fires during Operation LENTUS, Northern Manitoba on May 30, 2025.

Photo: Aviator Nicholas Zahari, 17 Operations Support Squadron Imaging, Winnipeg

The SIGINT-Cyber Nexus in the Canadian Armed Forces

LIEUTENANT-COLONEL L. J. REDIGER

Lieutenant-Colonel (LCol) Leslie Rediger joined the Canadian Armed Forces as a communications and electronics engineering officer in 2001, graduating in 2006 with a bachelor's in mechanical engineering from the Royal Military College of Canada. For the first 15 years of her career, she enabled air operations as a communications and information systems officer at various RCAF wings and at 1 Canadian Air Division Headquarters. She deployed multiple times in support of Op ATHENA and Op REASSURANCE. In 2016, LCol Rediger transitioned to Signals Intelligence (SIGINT) Operations, serving as officer commanding the support squadron and as deputy commanding officer at Canadian Forces Station (CFS) Leitrim, and as chief of staff of Signals Intelligence at Canadian Forces Information Operations Group Headquarters. She was promoted to her current rank in 2020 and commanded Canadian Forces Station Leitrim from June 2023 to October 2025. She is currently the CAFCYBERCOM liaison officer to the United Kingdom. LCol Rediger holds a Master of Arts in Leadership from Royal Roads University and a Master's in Defence Studies from the Canadian Forces College.

Strong, Secure, Engaged: Canada's Defence Policy, released in 2017, frames the "rapid evolution of technology" as a central driver of change in the global security environment, reshaping the character of conflict.¹ It also notes that the Canadian Armed Forces' (CAF) use of cyberspace and emerging technology "brings significant operational benefits, but also creates critical vulnerabilities."² This means that, to be competitive and to defend Canada's interests, the CAF must be able to protect its assets, defend its freedom to manoeuvre in cyberspace, and be able and ready to leverage that operating environment to carry out its directed mandate.³

To “maximize Canada’s effectiveness in cyberspace” in *Our North, Strong and Free: A Renewed Vision for Canada’s Defence*, the Government of Canada directed the CAF to establish the Canadian Armed Forces Cyber Command (CAFCYBERCOM).⁴ This new command is intended to “improve the CAF’s ability to conduct cyber operations” and “enable the military to generate and employ cyber forces and other specialized capabilities on short notice and contribute to advancing Canadian interests and protecting Canadian, Allied and partner militaries at home and abroad.”⁵

On 26 September 2024, CAFCYBERCOM was established, elevating and transforming the Canadian Forces Information Operations Group from a level-three formation to a command, administratively supported by the Digital Services Group but reporting directly to the Chief of the Defence Staff.⁶ As the defence authority for cyber operations, it is responsible for the employment, generation, sustainment, management, and development of its allocated cyber forces, including signals intelligence (SIGINT) and joint electronic warfare.⁷

Although it is relatively well known in the defence community that the Communications Security Establishment (CSE) is the Government of Canada’s foreign signals intelligence agency,⁸ it is less well known that the CAF has its own integral SIGINT unit. Canadian Forces Station Leitrim has been conducting signals intelligence operations in the defence of Canada for almost 85 years.⁹ The inclusion of the CAF’s SIGINT organization into the new cyber command may, on the surface, seem unusual, given that it is an intelligence function and the CAF already had an intelligence command. However, SIGINT has a particularly important nexus with cyber operations. A nexus that is only growing and gaining relevance in the interconnected, technology-rich world in which the CAF operates. SIGINT and cyber are two sides of the same coin; although they have different purposes, authorities, and capabilities, they are inexorably linked and mutually reinforcing. This article serves as an introductory discussion of the relationship between SIGINT and cyber operations in the military context, with

the aim of illustrating their interdependencies and reinforcing nature, as they make their home in the new CAFCYBERCOM.

Lexicon

To begin this discussion, it is important to first define the terminology. Technological advancements in the information world tend to outpace doctrinal evolution. This means that there are no universally agreed-upon definitions for terms such as “cyberspace,” “cyber operations,” or the “cyber domain.” NATO, allies and partners have slightly different interpretations of these terms, and they are frequently used interchangeably. For this discussion, this article will reference the Department of National Defence’s Defence Terminology Bank for continuity.

Cyberspace and the Cyber Domain

Cyberspace is the “physical environment consisting of all assets that process, store or communicate digital data.”¹⁰ Unlike the other operational environments in which the CAF operates—land, sea, air and space—cyberspace is “omnipresent within all other environments.”¹¹ The cyber domain is a broader term that encompasses not only cyberspace but also the infrastructure that supports and enables it, as well as its users and their related activities.¹²

Cyberspace encompasses the cyber persona layer, which includes online profiles and other ways that people and things are represented online, while the cyber domain extends outward to include the actual humans who interact with cyberspace. Likewise, cyberspace encompasses the physical layer, including all computing hardware, phones, sensors, and data storage devices, while the domain captures that layer as well as the geographical layer, which represents the physical locations hosting the network devices and their surrounding environments.¹³

Cyber Operations

The term “cyber operation” encompasses a wide range of activities conducted in cyberspace aimed at achieving strategic and tactical objectives, which are subdivided into defensive cyber operations (DCO) and offensive cyber operations (OCO). DCO focuses on activities to preserve and ensure freedom of action within cyberspace,¹⁴ such as defending networks and data from adversaries. In contrast, OCO focuses on activities that project power through cyberspace to achieve specific effects.¹⁵ The intent of OCO is to disrupt, degrade, and/or destroy the adversary’s freedom of movement in cyberspace or to affect adversary activities or capabilities in other ways via cyberspace.

The growing dependence of state and non-state actors on cyberspace, its integrated information systems, and sensors has necessitated a proportional increase in cyber operations capabilities within the CAF. It is critically important that the CAF be able to defend its territory in cyberspace and leverage this

“Cyberspace encompasses the cyber persona layer, which includes online profiles and other ways that people and things are represented online, while the cyber domain extends outward to include the actual humans who interact with cyberspace.”

“It is critically important that the CAF be able to defend its territory in cyberspace and leverage this terrain to reach out and affect its adversaries.”

terrain to reach out and affect its adversaries. *Strong, Secure, Engaged: Canada's Defence Policy* sets out the expectation that the CAF's cyber forces are able “to target, exploit, influence, and attack [in cyberspace] in support of military operations”¹⁶ by leveraging emerging platforms across the land, sea, air and space domains for integrated sensor systems.¹⁷ The defence policy also highlights the requirement for the CAF to deny the adversary the ability to affect the CAF's command, control, communication, intelligence, surveillance, and reconnaissance (C4ISR) capabilities, which are necessary to enable CAF operations globally.¹⁸

Signals Intelligence

The term “signals intelligence” encompasses everything from the intelligence discipline itself and the activities conducted to collect information from cyberspace and other parts of the electromagnetic spectrum to the end products fed into the broader intelligence system.¹⁹ In essence, SIGINT is the interception, collection, decryption, translation, and analysis of communications and non-communications signals, as well as the production of

reports to enable the overall intelligence-gathering process.²⁰ Due to the sensitivity of this work, the processes, capabilities and products require special protection and handling and thus cannot be openly discussed.²¹

SIGINT is further broken down into three subcategories: communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation systems intelligence (FISINT). COMINT is comprised of intelligence gathered from the interception of electromagnetic communications, such as voice or text, other than by the intended recipient.²² ELINT focuses on electromagnetic non-communications transmissions, such as from radar systems.²³ These types of transmissions can provide information about their source, such as the frequency used, pulse rate, and direction of arrival, among other characteristics.²⁴ The final category, FISINT, is a more specific field and is defined as “intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and use of aerospace, surface and subsurface systems.”²⁵ FISINT is used to collect intelligence concerning transmissions and data from missile and control systems, for example.²⁶ The three subcategories of SIGINT work together to provide the critical intelligence necessary to enable national and continental defence objectives and to inform national security operations, foreign policy, and cybersecurity.²⁷

SIGINT has a long, clandestine history, closely guarded by those charged with its execution, operating from the shadows to enable CAF operations since the Second World War.²⁸ A cornerstone of military operations, SIGINT provides insight into adversary intentions, capabilities, and activities, underpinning strategic decision-making, defending the continent, and enhancing situational awareness for deployed forces worldwide.²⁹

Like cyber operations, the role that SIGINT plays in CAF operations has only grown in relevance in the context of modern warfare, where technological advancements have reshaped the battlefield, military strategy and intelligence-gathering activities. The increasingly interconnected information environment creates vulnerabilities, allowing the SIGINT enterprise access to adversary communications, sensors and weapons systems to produce critical intelligence on capabilities and intentions. The dramatically increased use of information technology systems, integrated sensors, and command and control systems have compounded the relevance of SIGINT in the defence of CAF assets and the exploitation of our adversaries, paving the way for active defensive and offensive cyber activities to exploit these same adversary vulnerabilities.

The SIGINT-Cyber Nexus

SIGINT operations leverage cyberspace and its embedded technologies to exploit the adversary's reliance on digital communications, interconnected devices, and the pervasive use of sensors to generate intelligence across all operational domains, including cyberspace. Intelligence generated by these processes



A member of the Canadian Armed Forces parachute team, the SkyHawks, gives a wind reading before the parachute show on the beach in Cobourg, Ontario, on May 24, 2023.

Photo: MCpl Nedja Coutinho, Canadian Armed Forces

enables CAF operations at all levels, from the tactical to the strategic. The interception of adversary communications and sensor data provides real-time intelligence on adversary locations and movements across all domains (air, land, sea, space, and cyberspace), informing threat assessments and targeting cycles for decision-makers. At the strategic level, it shapes situational awareness by discovering adversary intentions, capabilities and emerging threats.³⁰

While SIGINT and cyber operations both involve the use of digital technologies and operate in the cyber domain, they differ in scope, methodology and objective. SIGINT is primarily focused on the passive collection of information and the analysis of signals, whereas cyber operations can be both passive and active. Defensive cyber operations focus on safeguarding information and communications systems from intrusion, proactively protecting and securing them and responding to attacks, while offensive cyber operations aim to penetrate, manipulate and exploit adversarial systems. However, conducting cyber operations requires a deep understanding of threat actors, digital infrastructure, and its potential vulnerabilities. SIGINT can support these activities by providing the intelligence needed to identify targets and assess threats.

SIGINT-enabled Cyber Operations

Cyber operations, whether defensive or offensive, rely heavily on accurate and timely intelligence. SIGINT serves as a foundational element in informing cyber operations by intercepting and analyzing communications and non-communications signals to identify vulnerabilities in systems, detect patterns of cyber activity and better understand threat actors. CAF cyber operators must be able to understand the topology of target networks, including how

“ SIGINT serves as a foundational element in informing cyber operations.”

systems are interconnected, the protocols used, and the locations and nature of vulnerabilities within these networks.³¹

For defensive cyber operations, SIGINT can be used to reveal the structure and behaviour of the digital environment, as well as the intent and capabilities of adversaries and other cyber threat actors. Moreover, SIGINT can contribute to threat intelligence by identifying indicators of compromise, allowing the CAF to harden systems, deploy countermeasures and respond to intrusions. For offensive cyber operations, SIGINT can inform target selection, timing and tactics to ensure that cyber actions are precise and effective.

SIGINT can also facilitate attribution—the process of determining who is behind a cyberattack. Attribution is achieved by correlating intercepted communications with known threat actor behaviour. This is especially important in the modern threat landscape, where state and non-state actors employ sophisticated methods to obfuscate their identities.

SIGINT is essential for mapping network topology and understanding cyber threats. Its role in cyber operations extends beyond interception, as it enables comprehensive analysis to inform strategic planning and shape situational awareness for decision-makers. For the CAF, this relationship is underscored by the grouping of both SIGINT and cyber units under the same command. The establishment of CAF CYBERCOM enables better communication and cooperation between these strategically essential capabilities.

Cyber Support to SIGINT

Canada's initial SIGINT evolution was based on two main objectives: leveraging its unique geography to enable sovereign defence and utilizing that unique geography, along with homegrown collection initiatives, to contribute to and benefit from the Five Eyes intelligence partnership with the United States, the United Kingdom, Australia, and New Zealand.³² These requirements still exist today. SIGINT is a team sport because the prevalence of information systems, sensors, and transmitters makes it nearly impossible to parse the digital tsunami generated from all these sources. Finding, decrypting, analyzing, and reporting on the right information to satisfy intelligence requirements to enable CAF operations is immensely challenging. Being able to share that burden with like-minded, collaborative nations increases the amount of data that can be processed and exploited. Without the partnership of Canada's allies, that challenge would likely be insurmountable, particularly when operations take place in cyberspace. Canada's size and proximity to adversarial countries provide a geographic advantage that is leveraged to deliver unique contributions, enhancing relevance in this domain, facilitating access to partner intelligence, and positioning Canada to utilize the full might of the Five Eyes, enabling CAF operations around the world.³³ In the evolving digital landscape, this partnership is more important than ever. By investing in both sovereign and integrated SIGINT infrastructure, Canada ensures that its contributions are not only supplementary but also provide distinct and valuable intelligence to both CAF and Five Eyes operations. These sovereign capabilities enable Canada to align its operations with national security priorities, thereby enhancing the relevance and impact of its intelligence. Their integrated nature also allows Canada to strengthen collective defence and information-sharing across the alliance.

SIGINT operations rely heavily on secure network infrastructure, telecommunications and radio-frequency communications, data flow from sensors, complex computing

functions, automation, data analysis and, most importantly, integration and communication with partners and allies. This infrastructure is spread across the nation and the world, creating a significant and enduring technical and security challenge. All this leverages cyberspace, and none of it would be possible without support from cyber operations. Adversary cyber operations pose a significant threat to CAF operations, including SIGINT, by denying or manipulating information, conducting rapid or sustained collection, or engaging in deception activities.³⁴

It is defensive cyber operations that ensure the freedom of manoeuvre in cyberspace for SIGINT operations while protecting the critical assets, systems and facilities required to seek out, find, analyze and disseminate SIGINT. Moreover, SIGINT and offensive cyber operations work together to identify access points and understand the terrain in cyberspace, enabling intelligence collection and the delivery of effects. This critical nexus between cyber and SIGINT operations ensures that both are effective and sustainable.

Conclusion

The establishment of CAFCYBERCOM reflects a deliberate recognition by the Government of Canada and the CAF that cyberspace is a contested operational environment in which the CAF needs to be able to manoeuvre, defend its terrain, and

deliver effects. In this context, integrating SIGINT and cyber capabilities under a single command is a logical response to the realities of modern conflict. As this article has demonstrated, SIGINT and cyber operations are deeply interdependent. SIGINT provides the intelligence foundation that enables effective defensive and offensive cyber operations, while cyber capabilities protect, enable and amplify SIGINT collection and analysis. Together, they form a mutually reinforcing cycle that enhances situational awareness, supports decision-making, preserves the CAF's freedom of action in all domains, and facilitates the projection of military power through cyberspace.

As threats continue to evolve in scale, sophistication and speed, the importance of this SIGINT-cyber nexus will only increase. Co-locating expertise, authorities and capabilities within CAFCYBERCOM positions the CAF to better integrate signals intelligence and cyber operations, strengthen partnerships with allies, and respond decisively in the omnipresent cyber domain. Ultimately, the effectiveness of the CAF's cyber forces will rest not in the strength of individual capabilities, but in the power of collaboration, integration and innovation.

Notes

- 1 Canada, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Department of National Defence, 2017), 14.
- 2 Canada, *Strong, Secure, Engaged*, 72.
- 3 Canada, *Joint Doctrinal Note (JDN): Cyber Operations 2017-02 2-0* (Ottawa: Department of National Defence, 2017) 1-1.
- 4 Canada, *Our North, Strong and Free: A Renewed Vision for Canada's Defence* (Ottawa: Department of National Defence, 2024), 26.
- 5 Canada, *Our North, Strong and Free*, 26.
- 6 Canadian Armed Forces, *Military Organization Order 2025001-2025006*, 14 July 2025.
- 7 Department of National Defence, "DM/CDS Messages: A New Era for the Cyber Domain: Launch of the CAF Cyber Command, *The Maple Leaf*, 26 Sep 2024, Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2024/09/a-new-era-cyber-domain-launch-caf-cyber-command.html>.
- 8 Communications Security Establishment, "Mandate," Government of Canada, last modified 7 April 2021, <http://www.cse-cst.gc.ca/en/corporate-information/mandates>.
- 9 George T. Fraser and Rober Lynn Wortmann, *History of Canadian Signals Intelligence & Direction Finding* (self-published, 2005).
- 10 "Cyberspace," *Defence Terminology Bank*, record 694338, accessed 6 Feb 2026.
- 11 Canada, *JDN: Cyber Operations*, 2-1.
- 12 "Cyber Domain," *Defence Terminology Bank*, record 694360, accessed 6 Feb 2026.
- 13 Canada, *JDN: Cyber Operations*, 2-3-2.4.
- 14 "DCO," *Defence Terminology Bank*, record 693742, accessed 18 September 2025.
- 15 "OCO," *Defence Terminology Bank*, record 693752, accessed 18 September 2025.
- 16 Canada, *Strong, Secure, Engaged*, 65.
- 17 Canada, *Strong, Secure, Engaged*, 39, 109.
- 18 Canada, *Strong, Secure, Engaged*, 56.
- 19 Canada, *CAF SIGINT Primer* (Department of National Defence, April 2021), 1.
- 20 Canada, *B-GL-005-200/FP-001, Canadian Forces Joint Doctrine 2-0* (Ottawa: Department of National Defence, 2011) 1-16.
- 21 Canada, *CAF SIGINT Primer*, 1.
- 22 "COMINT," *Defence Terminology Bank*, record 3843, accessed 18 September 2025.
- 23 "ELINT," *Defence Terminology Bank*, record 507, accessed 18 September 2025.
- 24 Canada, *CAF SIGINT Primer*, 21.
- 25 "FISINT," *Defence Terminology Bank*, record 695891, accessed 18 September 2025.
- 26 Canada, *CAF SIGINT Primer*, 21.
- 27 Canada, *B-GL-005-200/FP-001, Canadian Forces Joint Doctrine 2-0*, 1-4.
- 28 Fraser and Wortmann, *History of Canadian Signals Intelligence & Direction Finding*.
- 29 Communications Security Establishment, "Foreign Intelligence," *Government of Canada*, last modified 6 April 2023, Originally found at: <http://www.cse-cst.gc.ca/en/mission/foreign-intelligence>.
- 30 Communications Security Establishment, "Foreign Intelligence." Originally found at: <http://www.cse-cst.gc.ca/en/mission/foreign-intelligence>.
- 31 Canada, *JDN: Cyber Operations*, 5-14.
- 32 Wesley Wark, "Favourable Geography: Canada's Arctic Signals Intelligence Mission," *Intelligence and National Security* 35, No. 3 (2020): 319-30, DOI: 10.1080/02684527.2020.1724629.
- 33 Maria A. Robson, "The Third Eye: Canada's Development of Autonomous Signals Intelligence to Contribute to Five Eyes Intelligence Sharing," *Intelligence and National Security* 35, No. 7 (2020), 954-69, DOI: 10.1080/02684527.2020.1768477.
- 34 Canada, *JDN: Cyber Operations*, 1-1.



A soldier from Canadian Forces Combat Camera films the movements of the Unclassified Remote-Sensing Situational Awareness Satellite (URSA) in Manama, Bahrain on January 26, 2017.

Photo: Master Corporal Mathieu Gaudreault, Canadian Forces Combat Camera IS04-2017-0001-004

Forging the Future: An Integrated Canadian Defence AI Ecosystem

LIDIA KORCZYNSKA

Lidia Korczynska is the director of the DND/CAF AI Centre and Data Policy and Governance. She previously worked in Parliamentary and Regulatory Affairs at the Canada Border Services Agency.

The Department of National Defence (DND) and the Canadian Armed Forces (CAF) are entering a decisive phase in the journey to operationalize artificial intelligence (AI). AI is transforming every aspect of our lives, and it is central to modern defence. AI underpins platforms like the F-35 and the River-class destroyer, and it is critical in cyberwarfare, disinformation, and autonomous weapons. AI also presents a unique opportunity for Defence to transform itself, but only if we are willing to seize this moment. The flip side of opportunity is risk. And the biggest risk we can take is to maintain the status quo.

To keep pace with allies and adversaries, Canada must transform Defence AI from fragmented experimentation into an integrated and mission-ready capability. We will do this by aligning talent, data infrastructure, procurement, and partnerships across

Defence to be AI-enabled by 2030. To accomplish that, we are charting a practical path forward—each LI is responsible for its AI systems, while the AI centre establishes clear enterprise guard-rails, shared data and compute foundations, and procurement

pathways allowing rapid piloting and scaling. We are also sustaining engagement with industry, academia, and allies to accelerate delivery, strengthen options for use cases, and ensure that our investments contribute to NATO outcomes.

AI and ROI

A recent MIT report cautioned that 95% of generative AI pilots fail due to poor integration and internal builds.¹ For Defence, AI presents an opportunity to leapfrog some of our technical debt, but only if the Defence Team is willing to do the hard work where it matters. Breaking down legacy silos, transparency and collaboration are not just sound leadership practices--from my perspective, they will make or break our digital transformation efforts. We must be willing to do the painful work of identifying business rules that are overly burdensome or outdated, be courageous enough to work collaboratively, and be humble enough to know that none of us can succeed alone.

Enterprise-wide transformation, which takes years, should also be broken down into shorter pilots and sprints, as technology changes quickly and implementing new digital capabilities may reveal other capability gaps. DND/CAF can implement change more effectively by designing enterprise AI capabilities that start small but are built to scale across the organization. This approach allows Defence to rapidly learn from pilots, scale successful solutions, and continuously adapt to evolving operational and business demands. In a similar vein, we should move away from viewing digital capabilities as merely an enabler and instead position digital as the core of operations, with human capital as the driving force behind it. Defence can build this deliberate and measured approach to innovation through the Defence Industrial Strategy and other collaborative frameworks.

The Vision for an AI-enabled DND/CAF

The DND/CAF AI Strategy commits Defence to becoming an AI-enabled organization by 2030,² using responsible AI in ways that strengthen operational outcomes and modernize corporate functions while maintaining trust. It emphasizes practical application over experimentation, ensuring that AI solutions are developed with and for Defence personnel to address real mission and business needs. This vision underlines DND/CAF's commitment to interoperability with allies and an innovation-ready culture.

To achieve this vision, the DND/CAF AI strategy outlines five main lines of effort that will translate this vision into a decision advantage. These include fielding and employing AI capabilities; driving change management to integrate AI into real workflows; embedding ethics, safety, and trust across the AI lifecycle; building talent and training for an AI-ready workforce; and deepening partnerships with allies, industry, and academia. Together, these aim to deliver and operationalize AI capabilities for CAF personnel.

“AI impacts all layers of the digital foundation, from user devices to networking, hosting, and cybersecurity.”

AI impacts all layers of the digital foundation, from user devices to networking, hosting, and cybersecurity. To capitalize on the opportunities that AI presents, Defence requires quality data, interoperable systems, DevOps orchestration, super-compute platforms and advanced technical skills and partnerships. However, by their nature, Defence organizations are highly distributed with many autonomous parts. This makes coordination and integration difficult and complex.

There are a number of challenges that may prevent us from becoming AI-enabled by 2030. These include fragmented efforts and shadow IT; talent gaps; missing infrastructure; lack of data integration for next-generation platforms and our late start compared to allies and adversaries.

As a public sector organization, National Defence and the Canadian Armed Forces are competing for the same talent as the private sector, and for the same technological innovation as our allies and adversaries. The federal ecosystem also presents a tangled web of matrixed responsibilities, overlapping mandates and at times contradictory objectives.

Luckily, Defence is not starting from scratch. Our civilian AI ecosystem is world-class, anchored by the three Canadian national AI institutes Mila, Vector, and Amii as identified in the Pan-Canadian AI Strategy.³ Internationally, our closest allies have shown what is possible: the United Kingdom's Defence AI Centre has demonstrated how a single hub, supported by an AI Safety Institute, formal AI standards, and transparent playbooks, can unify fragmented efforts, accelerate procurement, and build trust through responsible deployment.⁴ Its AI Model Arena evaluates multiple AI systems against defence scenarios, providing objective data that reduces risks and informs evidence-based procurement. Meanwhile, DAIC brings subject matter experts and academics into the conversation, accelerating innovation while embedding ethical and operational standards at the outset. Canada must now learn from these initiatives and Canadianize these lessons, consolidating our activity, preventing duplication, and demonstrating measurable contributions to NATO's defence investment targets.

Fight from Prototype

The DND/CAF AI Centre enables mission-ready capabilities through a federated or franchise model, where each part of the organization retains ownership and accountability for their AI systems,

but they operate within clear enterprise guardrails. Beginning in 2025-26, the AI Centre is moving beyond drafting policies to implementing them, proving their value through operational pilots, and scaling adoption across Defence.⁵

We work with the CAF to identify AI needs or capability gaps and identify potential solutions, including piloting new capabilities with a view to understanding how they perform in operational scenarios. The AI Centre also works in partnership with Defence Research and Development Canada and academia to bring research and development to production so that innovative AI capabilities can be tested by the CAF.

In 2026/27, pilots will mature into capabilities. This means that sovereign AI pilots will be running and tested across CAF operational functions, visibly demonstrating that Canada is not reliant on foreign solutions for its most sensitive applications. Alongside these pilots, all available procurement pathways will be pursued, ensuring that promising projects can transition to scale. New solutions using emerging AI technologies will have been introduced, and the year will close with a formal lessons-learned report—evidence that our frameworks have been tested in practice and are ready to guide future growth.

If these goals are not achieved on the anticipated timelines, we risk lagging in AI adoption, potentially eroding operational advantage and interoperability with key allies. To mitigate this risk, LIs must embed flexible metrics and maturity assessments that enable course correction and continuous learning from experience.

Within the Digital Services Group, the AI Centre builds connections between the CAF and industry, academia, and allies to deploy mission-ready sovereign AI capabilities. These efforts include the establishment of a robust digital foundation that supports on-premises and cloud environments across unclassified and classified domains, enabling joint operations through unified enterprise cloud services, data, compute, cybersecurity, and application development. Looking ahead, the AI Centre will be an integral part of supporting other whole-of-government efforts to create a Defence-Industrial base and modernize defence procurement.

The strategic intent for the DND/CAF AI Centre is to be a cohering force that supports CAF LIs. The AI Centre will enable secure deployment paths, support AI governance, temporarily embed AI-skilled personnel within each LI, and provide data, tailored advice and support. In turn, LIs will benefit from engaging with

the AI Centre before developing AI independently; we may already have a deployed model for use!⁶ In order to prepare for AI, LIs also need to collaborate on platform design and enterprise tools and do the work to ensure that data is well-governed, usable and interoperable, while adhering to NATO standards.

This cycle—pilot, evaluate, scale—is what turns frameworks from paper to operational doctrine.

Engagement with Industry and Academia

Defence cannot innovate in isolation. The AI Centre is undertaking a comprehensive mapping of industry and academic partners and creating an engagement plan to ensure that our interactions are structured and targeted. In parallel, the AI Centre is working in partnership with Carleton University to organize the first-ever AI in Defence Conference, which will convene Defence, industry, academia, and trusted partners to advance DND/CAF's responsible adoption of AI.⁷ This conference will allow DND/CAF to align with industry partners on a five-year roadmap for AI and data capabilities.

Engagements like the upcoming AI in Defence Conference early in the year prove that Defence is connected to the broader ecosystem. Sustained partnerships will show that Defence is not simply a consumer of innovation but a contributor to Canada's wider AI success story.

Together, the AI Centre must work to identify the AI talent in our organizations and empower them to help us. From a recruitment and retention standpoint, we need to explore every option to bring in the best and brightest. We will all benefit from building collaborative partnerships, and, most importantly, we must all take a hard look at our business processes and ask how we might do things differently for the AI era.

Enabling procurement and NATO Contributions

Underlying every strand of this strategy is procurement. Without pathways tailored to AI, promising pilots will remain trapped as experiments. In 2026/27, the AI Centre will enable new digital procurement pathways to create a continuous cycle of small-scale pilots to quickly deploy and test new technologies. CAF members will be able to collaborate with industry to co-develop innovative technologies with end-users and acquire those that prove effective in piloting. We will also manage a vendor repository to prevent duplication and inform different teams on what has been done and what teams could inform on lessons learned along with best practices for like-minded projects. These near-term steps will build momentum, with classification-ready lots and dynamic purchasing.

At the same time, we will ensure every AI investment is accurately tracked. Each project will be tagged to NATO capability codes,⁸ ensuring that Canada's AI investments are recognized as defence contributions. This means that we will be able to report

“The strategic intent for the DND/CAF AI Centre is to be a cohering force that supports CAF LIs.”

not only the number of projects underway but the proportion of AI investment that qualifies under NATO's defence investment categories—a visible demonstration of Canada's seriousness about emerging technology.

Coordination Across the Federal Ecosystem

Across the federal ecosystem, success will require an appetite for smart risk-taking and regulatory sandboxes to allow experimentation, and industry needs more certainty that there is a future with Defence. None of this will happen overnight; it will require incremental progress with lessons learned along the way.

Our sustained momentum has laid a strong foundation for success; the priority now is to provide clear, accessible pathways and a coherent vision that enables seamless engagement by CAF personnel and industry. Achieving this will require a laser-sharp focus and overcoming key barriers, including slow and complex procurement processes, and inconsistent data and digital readiness. We can surmount these challenges through clear guidance and enterprise coordination.

Conclusion

The coming year promises to be very exciting as the AI Centre moves from developing framework and policies to implementing them. Governance and responsible AI tools will be embedded across LIs, sovereign pilots will be underway, procurement pathways will be enabled, industry and academia will be engaged, and our workforce will be ready. Canada will be able to show NATO and our allies that we are not just talking about AI in Defence—we are adopting it responsibly, at scale, and with impact.

The UK has shown what is possible when ambition meets structure. Canada is now ready to catch up, with a plan that is distinctly ours: rooted in sovereignty, aligned with NATO, and focused on delivering trusted capability to the war fighter.



An officer from 437 Transport Squadron in Trenton, coordinates the air-to-air refueling operations over the Canadian Arctic between a CC-150 Polaris Airbus and two CF-18 Hornets from 401 Tactical Fighter Squadron in Cold Lake during the NORAD Exercise AMALGAM DART 21-2, on March 23, 2021.

Photo: MCpl PJ Letourneau, Canadian Forces Combat Camera

Notes

- 1 Sheryl Estrada, "MIT Report: 95% of Generative AI Pilots at Companies Are Failing," *Fortune*, 18 August 20. Originally found at: <https://fortune.com/2025/08/18/mit-report-95-percent-generative-ai-pilots-at-companies-failing-cto/>.
- 2 Government of Canada, *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy - Canada.ca* *The Canadian Armed Forces Artificial Intelligence Strategy*, 22 Government of Canada, March 22, 2024. Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/dnd-caf-artificial-intelligence-strategy.html>.
- 3 Government of Canada, *Pan-Canadian AI Strategy - CIFAR* *Pan-Canadian Artificial Intelligence Strategy*, 31 October 2025. Originally found at: <https://ised-isde.canada.ca/site/ai-strategy/en/pan-canadian-artificial-intelligence-strategy>.
- 4 UK Ministry of Defence, *Defence Artificial Intelligence (AI) Playbook*, published 1 February 2024, <https://www.gov.uk/government/publications/defence-artificial-intelligence-ai-playbook>; UK Ministry of Defence, *JSP 936: Dependable Artificial Intelligence (AI) in Defence (Part 1: Directive)*, Joint Service Publication, 13 November 2024. Originally found at: https://assets.publishing.service.gov.uk/media/6735fc89f6920bfb5abc7b62/JSP936_Part1.pdf.
- 5 See p. 48 of the DND/CAF Department Plan for a description of how DND/CAF is implementing the AI strategy in 2025-2026. Department of National Defence and the Canadian Armed Forces, *Departmental Plan 2025-26* (Ottawa: Government of Canada Publications, 2025). Originally found at: https://publications.gc.ca/collections/collection_2025/mdn-dnd/D3-37-2025-eng.pdf.
- 6 Government of Canada AI Register (Minimum Viable Product) - Open Government Portal Some of A few of our shared AI tools are available within the Government of Canada AI Registry. See: Government of Canada, *Government of Canada AI Register (Minimum Viable Product)*, 28 November 2025. Originally found at: <https://open.canada.ca/data/en/dataset/fcb0200-79ba-4fa4-94a6-00e32facea6b>.
- 7 Canadian Global Affairs Institute, "AI in Defence Conference | Conférence sur l'IA en défense - Canadian Global Affairs Institute AI in Defence Conference | Conférence sur l'IA en défense," event held 9-10 February 2026. Originally found at: https://www.cgai.ca/ai_in_defence_conference.
- 8 NATO, "NATO's Role in Capability Development," last updated 26 June 2025. Originally found at: https://www.nato.int/cps/en/natohq/topics_49137.htm. NATO's role in capability development | NATO Topic



A member of the Advanced Naval Capabilities Unit, based in Victoria, British Columbia, stations in a control tent, uses a Toughbook Laptop in conjunction with the controller to operate the G15 Sentinel drone to test interoperability in arctic conditions as part of Operation NANOOK-NUNALIVUT in Inuvik, Northwest Territories on February 27, 2025.

Photo: Master Corporal Alana Morin, Joint Task Force - North, Yellowknife

Artificial Intelligence and the Sino-American Techno-Competition: Implications for Canadian and Allied Defence

JENNIFER GEAREY AND MAJOR TYLER CURRIE

Jennifer Gearey is lead of the Strategy, Capabilities and Responsible Artificial Intelligence team in the AI Centre at the Department of National Defence. She has been an executive at the Nuclear Safety Commission, Health Canada, Department of Justice and the Treasury Board, and is a former journalist.

Tyler Currie is the CAF AI Integration & Acceleration officer who works at the DND/CAF AI Centre. Tyler has spent 16 years as part of the Intelligence Branch and has served on deployed operations in Afghanistan and in the international context with Joint Forces Command (JFC) Naples. Tyler holds a Master's in Political Studies from Queen's University as well as a Master of Management in Artificial Intelligence (MMAI) from the Queen's Smith School of Business.

Artificial Intelligence (AI) has shifted from laboratory curiosity to a core enabler of strategy in less than a decade. It will contribute to better logistics chains, intelligence workflows, cyber defence, virtual wargaming, targeting, predictive vehicle maintenance, personnel administration, data management, and the orchestration of complex operations.

Unlike single-purpose platforms, AI is a general-purpose capability. Once the foundations exist—data, compute, and the institutional habits to use them—new military functions can be “written” in software and delivered at software speed. That is why AI is essential to securing decision advantage. Nations that can translate data into timely, reliable decisions across the battlespace will enjoy compounding advantages; those that cannot will discover that exquisite hardware without digital cohesion is an expensive liability. From the United States and China to the European Union and Canada, countries have now implemented defence AI strategies to maximize AI’s potential in defence.¹

The technology competition between China and the United States illustrates this reality. It spans chips and cloud, standards and supply chains, research ecosystems and corporate platforms. The contest is not merely for market share—it is for the ability to set the tempo of operations and the rules of interoperability for decades.

China seeks to compress time—adopting and scaling AI in the service of “intelligentized warfare,” embedding surveillance and command automation across domains and exporting turn-key digital governance through its Digital Silk Road.² The United States, with allies, still owns the most consequential choke-points—advanced chip fabrication equipment, leading models and frameworks, hyperscale cloud, and much of the world’s top AI talent—but democratic procurement cycles and corporate ambivalence can hinder that lead.³

For Canada, the stakes are unusually concrete. As a middle power nested inside alliance architectures (NATO, NORAD, Five Eyes) and dependent on imported compute and commercial cloud, Canada’s choices will determine whether it remains interoperable at the speed and fidelity that AI demands. The Canadian Armed Forces (CAF) will increasingly fight in multidomain task forces and coalitions that link sensors, weapons, and data across all domains.⁴

That future is only plausible if Canada can protect and mobilize its data, secure dependable access to compute and toolchains, reform institutions to field AI responsibly and quickly, and attract and retain the talent to make all three real. Across each of these enablers, AI adoption must remain grounded in human-within-the-loop decision-making, with clearly assigned accountability and the preservation of meaningful human judgement in consequential defence contexts. The alternative is a technologically induced drift—capability gaps that quietly open in peacetime and reveal themselves at the worst possible moment.

To remain a first-rate ally in an AI age, Canada should make deliberate investments and institutional moves that convert democratic values into operational advantage. This imperative already builds on a strong foundation, as Canada has long been an early and sustained investor in AI, with a world-leading AI research ecosystem. The task is now to ensure that this strength is converted into an enduring operational advantage.

“To remain a first-rate ally in an AI age, Canada should make deliberate investments and institutional moves that convert democratic values into operational advantage.”

AI as a Strategic Challenge

At the operational level, AI deconflicts airspace, aligns activities where coordination is required, and fuses dispersed data into a coherent operational picture. At the strategic level, it drives persistent cyber reconnaissance and shapes operations at machine speed. Together, these capabilities compress and accelerate decision cycles.

Three features of AI make it a uniquely difficult security problem for democracies. First, it is dual-use to an extreme.⁵ The very same model that helps draft legal memos can generate targeted phishing kits; the same synthetic-image pipeline that creates benign training data can produce plausible deepfakes; the same optimization engine that routes trucks can plan autonomous threat swarms. Government export controls—rules that restrict the sale of sensitive technologies like advanced computer chips and AI software to certain countries—can slow adversaries’ access to cutting-edge hardware and models.⁶ Ideas and even code spread quickly through academic publications and open-source communities. The CAF should therefore assume that capable adversaries will obtain near-frontier generative AI tools, even if they cannot produce the latest chips themselves.

Second, AI scales with data and compute, not only with budgets. China’s domestic surveillance and commercial super-apps produce oceans of high-granularity data on people, places, and patterns of life; its state-industry alignment allows that data to be repurposed for security aims with little friction.⁷ Meanwhile, access to compute is uneven and increasingly expensive. When global demand for GPUs spikes, training runs that cost millions of dollars become routine for large cloud providers—and out of reach for others.⁸ This creates a world in which those who can pay for sustained training and fine-tuning gain compounding advantages in model capability and alignment.

Third, AI makes deterrence and escalation harder to manage. When machines act with a degree of autonomy, it becomes less clear who is accountable for their decisions.⁹ If adversaries tamper with AI systems, they can trigger unexpected failures. At the same time, AI can now generate fake voices, images and videos so convincingly that the entire information space becomes

a battlefield. Deterrence depends on clear signals and shared understanding of red lines—but this breaks down when the information environment itself is degraded by misinformation, manipulation, and signal noise. In such a world, trust among allies is not optional—it is essential.

For Canada, AI will affect every type of mission.¹⁰ In the Arctic and North Atlantic, where communications are limited, forces will need AI that can process weak and scattered signals directly on ships and aircraft, because there is neither the time nor the bandwidth to send everything back to headquarters. In NORAD modernization, new radar and sensor systems will only be useful if AI helps sift through the flood of data to highlight real threats. On overseas operations, command posts should be able to function even when communications are cut, degraded, or unreliable, using AI models that can run on tough, portable hardware in the field.

Across all missions, adversaries will exploit AI for conducting disinformation campaigns, launching AI-enabled cyberattacks, compromising models through adversarial machine learning, and even issuing voice-cloned orders designed to sow doubt in leadership. Recent incidents, such as the AI deepfakes of images spreading misinformation about wildfires in BC, show that AI-enabled attacks are today's reality.¹¹

Canada's Department of National Defence and Canadian Armed Forces (DND/CAF) AI Strategy provides a strong starting point, particularly in its focus on fielding AI applications at scale and creating ethical safeguards.¹² Canada's newly announced Defence Industrial Strategy also reinforces this direction by prioritizing digital technologies like AI and secure cloud, further advancing defence AI capabilities.¹³ As the AI Strategy shifts from vision to execution, DND/CAF should ensure that these principles translate into operational realities—bridging talent gaps, addressing siloed efforts, improving data readiness, and accelerating procurement pathways—so that AI can be adopted responsibly, at scale, and with impact.

Big Tech, Corporate Agency, and the Defence of Democracy

In previous eras, governments owned or directed the decisive technologies of war: nuclear physics, code-breaking, aerospace, space launch, etc. Today, the most important AI tools—like the largest models, massive cloud platforms, secure teamwork software, and systems that verify whether content is real or fake—are all developed and controlled by just a few big global companies. Alibaba, Tencent, Microsoft, Amazon, Google, and Meta own the clouds and the accelerators; they control the collaboration and identity platforms on which government work actually happens. This is both an opportunity and a vulnerability.

This is an opportunity because big tech firms can move fast, hire talent that governments struggle to attract, and spread costs across their huge commercial markets. When their products

“ For Canada, the lesson is to treat Big Tech not as a monolithic “ally” but as actors with agency whose incentives should be shaped.”

align with allied goals, militaries can save time. Instead of building every AI system from scratch, a defence ministry can buy secure, policy-compliant versions of commercial platforms and then focus only on the mission-specific parts.¹⁴ Features such as cloud regions with national controls, login systems with strict access rules, and software pipelines that verify code integrity are examples where a few smart choices can create major security benefits across the whole enterprise.

Corporate platforms are also a source of vulnerability because they are global. Their revenue and growth depend on multi-jurisdictional operations, including in countries whose legal regimes compel cooperation with state security services.¹⁵ Their product roadmaps should balance shareholder return, brand risk, and internal employee politics alongside national-security requests from governments. The result is structural ambivalence. A company can be a crucial partner to the United States Department of Defense (DoD) while simultaneously maintaining a research presence in China or selling enterprise software into third countries that use it in ways that are misaligned with allied interests. There are recent cases in which universities in the United States conducting DoD-funded research inadvertently supported technologies later linked to Chinese military institutions, which prompted the Pentagon to scale back such funding opportunities.¹⁶ Those entanglements may be lawful and even transparent, but they create exposure for anyone whose mission rests on those platforms.

For Canada, the lesson is to treat Big Tech not as a monolithic “ally” but as actors with agency whose incentives should be shaped. Three design choices follow.

First, write security and exit into the contract. Defence procurement should insist on forensic-grade audit logging such as detailed activity logs, strict separation of customer-managed keys, and default data residency within allied jurisdictions.¹⁷ It should also require practical exit ramps, such as ensuring independent foundation model access, using AI systems that can be moved easily between cloud providers, and ensuring that any custom software works across numerous platforms.¹⁸ This is not hostility to vendors; it is a recognition that interoperability and continuity are warfighting requirements. If a geopolitical shock forces the rapid migration of services, the CAF should not be handcuffed by proprietary bindings. These mechanisms, such as

exit provisions, could be embedded into large defence AI procurement initiatives to safeguard against potential contingencies.

Second, treat governance as something concrete, not just as a promise. Every AI system should come with a basic “governance package” that includes things like model cards to explain how the AI system was built and tested, summaries of where training data came from, red-team testing results to identify system weakness against AI-enabled threats, known limitations, bias checks, and a clear process for handling incidents or rolling back a model if needed.¹⁹

For content authenticity, demand open standards such as digital signatures that prove where content came from, and audit trails that show if anything was altered. For software, require bills of materials that list all components, proof of supply-chain integrity, and reproducible builds for critical code.²⁰ These tools turn vendor claims into verifiable facts and make it possible for allies to work together with confidence.

Third, diversify smartly without creating unnecessary complexity. Using multiple cloud platforms just for the sake of it can make systems fragile and harder to manage. The real goal is to avoid single points of failure, not to spread work evenly across providers. A good approach is to rely on one main platform for day-to-day operations, while keeping secondary platforms on standby for surges or emergencies. Open standards—such as common identity logins, software packages that can run anywhere, and message systems that follow NATO standards—make it easier to switch or connect when needed.

What matters most is how Canada connects with its allies, industry, and partners. Relying too heavily on a few big tech platforms—cloud providers, AI models, or software suites—creates platform risk, meaning that Canada could become dependent on systems it does not control. If those companies change their policies, limit access, suffer outages, or must comply with foreign legal authorities, Canada’s security and operations could be weakened.²¹ But if Canada uses contracts, standards, and clear practices to align these corporate platforms with national needs, it can turn that dependency into an advantage. If not, platform risk will simply become another form of strategic vulnerability. To address these vulnerabilities, DND/CAF is supporting the Canadian defence AI ecosystem and acquiring AI capabilities that align with NATO’s AI strategy.

The Four Battlegrounds of AI Power—and Canada’s Choices

The United States and China are locked in a contest for advantage in artificial intelligence. The competition is not abstract—it comes down to very practical things: who controls the right data, who has access to computing power, who can turn policy into working systems, and who can attract and keep the right people. These four battlegrounds will shape who leads in AI. For Canada, success will depend on the choices we make now.



Canadian Armed Forces tankers from Lord Strathcona's Horse (Royal Canadians) partnered with Polish Armed Forces, instruct Ukrainian soldiers in Leopard tank fundamentals in western Poland, February 13, 2023.

Photo: Canadian Armed Forces photo

Data is the first battleground. China’s model is built on sheer volume and compulsion: endless streams from sensors, and state access to information by default.²² Democracies like Canada cannot and should not copy that approach. Our edge should be in data readiness, not hoarding. That means knowing which datasets matter for defence—like air and maritime tracks, logistics records, or satellite feeds—and organizing them so that they can actually be used by AI. Too often, defence organizations drown in petabytes of unusable data with no clear labels, no information tracking its origins, and no policies for how it should be used.²³ Canada’s task is to turn that haystack into a well-curated library, ready for use by AI systems. Sometimes, when data are scarce or sensitive, the answer will be synthetic or simulated examples—like training submarine-detection models on simulated sonar signals, rather than risking disclosure of real tactics. Readiness also means restraint: allies will only share if Canada can also prove that it knows how to delete or minimize responsibly.

Compute is the second battleground. The most advanced computer chips and access to fabrication equipment remain concentrated within allied and partner ecosystems, though China’s manufacturing capability is strong but still trails the frontier. Export controls primarily restrict adversaries’ access to the highest-end compute while allowing continued flows within trusted supply chains. Access and scaling of the most advanced AI systems are still shaped by access to cutting-edge chips. This only matters if Canada can actually access the computing power it needs, when it needs it. Cloud markets are volatile, and defence workloads can easily be crowded out by commercial demand.²⁴ data centres on Canadian soil, connected to secure networks; and rugged edge computers that can run AI models in the field, even when communications are down. The goal is not to build the next GPT-4 from scratch, but to make sure that Canada can adapt and run capable models without waiting in line. Compute, in this

sense, is like fuel: scarce, strategic, and something that must be carefully planned, budgeted, and conserved.

The third battleground is institutions. AI power is not just about drafting principles; it is also about putting working tools into the hands of operators quickly and safely. That means building habits that defence organizations often lack: rapid experimentation, continuous testing, fast but accountable approval pipelines, and budgets that carry pilots through to real programs.²⁵ Canada's Defence AI Centre should be the hub, but every formation needs small teams that bring operators, engineers, lawyers, and ethicists together to turn ideas into deployable systems. Risk-tiered pathways are key. An AI assistant that searches doctrine does not need the same scrutiny as a model that informs targeting decisions. Procurement also needs to evolve—buy outcomes in increments, fund the people who will maintain and adapt the models, and assume that systems will need regular updates, not just one-time deliveries.

As DND/CAF accelerates AI deployment, this requires embedding assurance by design through automated testing, AI sandboxes, as well as modular, staged deployment models that allow capabilities to scale rapidly from pilots to operations. In parallel, developing sovereign AI compute resources that can be reused across numerous projects and leveraging a trusted domestic AI ecosystem ensures that sensitive defence capabilities can be fielded quickly without strategic dependency.

Finally, talent. Few can outspend Silicon Valley in hiring hundreds of senior engineers, and they do not have to. What we need is a barbell approach: a small group of deep experts to solve the hardest problems, a broad base of digitally fluent operators who can use AI tools in their daily work, and translators in the middle who connect policy to engineering and operations to data. This also requires modular and open-source AI systems so that capabilities can be adopted more easily, alongside training that enables CAF operators to be equipped with the skills to maintain and upgrade them over time. Beyond technical specialists, talent pipelines should explicitly build capacity and training for ethicists, commanders, human-centred designers, and communication experts to ensure that AI adoption remains safe and grounded. The DND/CAF is already completing some of these steps, as talent and training is one of the core pillars of the Defence AI Strategy.

DND/CAF can build quick wins through scholarships tied to service, secondments with leading AI institutes, streamlined security clearances for key skills, and training to promote AI awareness. More ambitious initiatives should follow as medium- and long-term investments. A key example is the establishment of a digital reserve corps that would enable industry experts to surge in during exercises or crises. DND/CAF could cultivate a protected nucleus of senior AI specialists with a variety of expertise that are supported with modern AI-enabled workflows and tools, as well as recognition that does not require leaving technical tracks for management. Retaining this talent ultimately requires autonomy, purpose, and recognition—and a system that values

“ The challenge for allies is not only the possibility of espionage, but also the spread of architectures designed for highly centralized oversight. Once embedded, such systems tend to shape the practices around them.”

deep expertise as a strategic asset. Above all, they must be protected, because those who work on defence AI could be targeted by espionage and harassment campaigns.

Canada's choice is clear: we can either treat these four battlegrounds as separate problems—data, compute, institutions, and talent—or we can approach them as a single strategic posture. Success means readiness, access, speed, and people.

Huawei, the Digital Silk Road, and the interoperability challenge

Huawei is often thought of as just a telecom company, but its role is broader. Through its “safe city” platforms and China's wider Digital Silk Road initiative, Huawei bundles together cameras, sensors, analytics, and command software into ready-made technology packages.²⁶ These are marketed as tools for modernization. For governments working under tight budgets, the pitch is hard to ignore: low-cost financing, quick deployment, and the appearance of tighter control over security and infrastructure.

The challenge for allies is not only the possibility of espionage, but also the spread of architectures designed for highly centralized oversight. Once embedded, such systems tend to shape the practices around them.²⁷ When these architectures enter partner networks, allied operations can inherit their constraints.

Canada's decision to exclude Huawei from 5G networks was an important step, but challenges remain. Risks now come from indirect exposure: subcontractors embedding Huawei components in otherwise “clean” systems; partner nations in regions such as the Indo-Pacific, Africa, or Eastern Europe adopting Huawei-based networks and later hosting allied exercises, or even local procurements in Canada that bring surveillance technology into critical infrastructure.²⁸ In a shared environment, interoperability is only as strong as its weakest link. A single vendor with opaque update channels can create persistent uncertainty.

DND/CAF's practical response should focus on three areas. First, it is not enough to check the main vendor; we also need to know what parts and software are coming from their

subcontractors. Basic disclosure rules and simple tools can make hidden risks visible before they cause problems.²⁹

Second, provide real alternatives. Telling other countries not to use a certain supplier does not work if there are no affordable options to choose from. Canada should work with allies to offer technology packages that are reliable, respect privacy, and come with long-term support.

Third, show up where the rules are written. International standards decide which systems can connect and work together. Canada should be at those tables, pushing for open and transparent rules that make trusted infrastructure the easiest option.

By taking these steps, DND/CAF and its partners can reduce risks, build stronger cooperation, and support a digital ecosystem that is open, secure, and resilient, without raising tensions unnecessarily.

Procurement, market volatility, and the economics of speed

DND/CAF and its allies may have an edge when it comes to advanced chips and cloud platforms, but that edge means little if governments cannot buy and field new tools quickly. Today, procurement is often the bottleneck. Slow competitions for large, one-size-fits-all systems can take so long that the technology is outdated before it is even awarded. In Canada, major defence procurement cycles can take seven to eight years.³⁰ Evaluation methods tend to reward familiar vendors rather than innovative ones.³¹ Legal challenges can stall progress for months or years. Meanwhile, AI technology evolves every three to six months, not decades.³²

DND/CAF can close the gap between the speed of commercial innovation and the slower pace of defence procurement with practical steps, leveraging its vibrant AI research and innovation ecosystem.³³ One way to do that is to buy in smaller increments rather than betting on massive projects, an approach demonstrated by NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) Rapid Adoption Service in allied operational trials.³⁴ Breaking programs into manageable pieces, each with clear performance tests, reduces risk and allows adjustments along the way.³⁵ Payments should be tied to milestones measured through metrics showing faster data analysis or shorter decision cycles, rather than just the delivery of software. Another step is to prepare for market volatility. Access to computing power is usually routine until it suddenly is not. Contracts should include clauses that guarantee priority access during crises, cap prices for baseline use, and give Canada the flexibility to move workloads across regions.³⁶ Maintaining small, steady contracts with multiple vendors can act as insurance against shortages or sudden disruptions.³⁷

Evaluation should also be treated as central, not secondary. The real cost of an AI system is not the software licence, but the ongoing work of testing, monitoring, and retraining. Defence

needs dedicated resources for red-team exercises, tools to detect drift or manipulation, and clear records of a system's limits.³⁸ If commanders are to rely on AI in high-stakes decisions, they should be able to demonstrate how the tool was tested and what its boundaries are. Allies such as the United States and the UK already use metrics to evaluate the reliability and security of their defence AI models, including how often systems get decisions right, whether they speed up operations, and how safely and predictably they perform in realistic tests, including when battlefield conditions change.³⁹

DND/CAF also needs to bridge the "valley of death," which is where successful prototypes often fail to become deployed tools. Too often, pilots die because no unit is ready or funded to adopt them.⁴⁰ In the United States, for example, only 16 percent of defence innovation funding transitions into full-time production.⁴¹ A dedicated fund could carry successful pilots into operational use, with a receiving organization identified from the outset. Pilots themselves should be designed with deployment realities in mind—such as classification requirements, identity management, and logging of security-related events—so that they can move smoothly into production.

Finally, cost management should be treated as part of security. Hidden expenses like cloud transfer fees, the scaling of AI tools across the organization, or ballooning storage can quietly consume budgets.⁴² Embedding financial oversight directly into technical teams keeps costs predictable, makes trade-offs transparent, and prevents unexpected bills from derailing adoption.

Taken together, these steps can help DND/CAF align defence procurement with the rapid pace of AI development, so that technological advantage translates into operational advantage.

Implications for Canada and NATO: A contained Agenda

Turning analysis into action means focusing on what can realistically be done now, and what should be built for the future. For Canada, the immediate horizon is the next 12 to 18 months. Beyond that, we need to think in terms of the next two to four years.

In the near term, Canada's priority is to create the conditions for AI to be adopted quickly but safely.

Rather than matching commercial AI's pace, DND/CAF's priority is to remove avoidable delays and align procurement and testing rhythms with allies through rapidly deployable pilot projects that scale as capability matures. That begins with clear guidance across the defence enterprise. Not all uses of AI carry the same level of risk, and decision-makers need a simple framework that makes low-risk applications easy to approve while reserving stricter processes for higher-risk uses. Alongside this, Canada would benefit from a dedicated hub for testing, evaluation, and red teaming—a place where new systems can be pushed to their limits, their vulnerabilities exposed, and their performance monitored in real-world conditions. To build a sovereign AI



Canadian and Polish Armed Forces soldiers assess Ukrainian soldiers in the Leopard 2A4 tank simulator during Operation UNIFIER in south-western Poland, on February 20, 2023.

Photo: Corporal Marco Tijam, Operation UNIFIER, Canadian Armed Forces Photo

“ The current system of one-time approvals for software cannot keep up with AI, which evolves on a weekly basis.”

ecosystem, DND/CAF requested the Canadian Defence AI Centre to build AI research and experimentation capacity while contributing to innovative AI solutions. Access to computing power is another urgent need. DND/CAF cannot afford to be left waiting in line when demand for advanced chips spikes. That means securing cloud resources with priority rights, building modest on-site capacity for sensitive work, and certifying portable edge devices that can operate even in degraded communications environments.⁴³ It also means ensuring that DND/CAF has sufficient compute resources to reduce reliance on foreign vendors. At the same time, Canada should start preparing its data. Select mission areas, such as Arctic surveillance, intelligence imagery, or equipment maintenance records, should be elevated to gold-standard quality, complete with proper metadata, privacy safeguards, and synthetic data where needed. These exemplars can set the bar for the rest of the enterprise.

Governance also needs to become part of the product, not an afterthought. Every AI tool procured for defence should come with basic documentation: what it was trained on, how it performs, where it struggles, and how it can be safely shut down if something goes wrong. Exercises should also evolve. Major NATO or Five Eyes drills should now include AI-generated deepfakes and

narrative manipulation, giving public affairs teams the chance to practise rapid detection and coordinated responses.⁴⁴

Looking further ahead, the medium-term agenda is about institutional change. The current system of one-time approvals for software cannot keep up with AI, which evolves on a weekly basis. DND/CAF will need to move toward continuous assurance models, where security is monitored and enforced in real time. The United States and the European Union provide model AI assurance metrics that DND/CAF could consider adopting, which could include developing AI models that have robust model design, monitor continuously for anomalous behaviour, demonstrate clear human escalation protocols, and have segmented model pipelines. Working with allies, DND/CAF should also help create a shared model exchange, with common packaging and documentation so that partners can use each other's work rather than reinventing it.⁴⁵

There is also a geopolitical dimension. Many countries are adopting surveillance-heavy technologies as part of urban security programs. Canada, working with G7 partners, could develop affordable and privacy-preserving alternatives that demonstrate a democratic model of “safe city” technology.⁴⁶ Alongside this, the human dimension cannot be neglected. DND/CAF will need faster clearances for critical skills, as well as career paths that allow technical specialists to advance without being forced into management roles. DND/CAF can retain access to its critical AI workforce by ensuring access to compute through shared public-sector procurement and by building shared verification frameworks. Protecting researchers through tailored counter-espionage programs will also be vital.⁴⁷ This includes ensuring that they complete their due diligence to understand funding sources and who they are engaging with. If they are developing new products, they need to be trained to take basic precautions, such as limiting exposure to sensitive or proprietary information, filing patents before disclosure, or using nondisclosure agreements.⁴⁸

Finally, coalitions like NATO depend on interoperability. That requires budget lines explicitly set aside for integration—adapters, test environments, and joint trials. Without this, ambition outpaces reality. And as AI systems become more powerful, red-teaming should be institutionalized. Models should be stress-tested not only by engineers, but also by linguists, psychologists, and operators who can spot weaknesses that adversaries might exploit. Initiatives focusing on testing and evaluation already exist—NATO's DIANA program has opened 16 test centres and two accelerators across Canada focused on developing dual-technologies like AI. Taken together, this agenda is not about racing toward the frontier at any cost. It is about sequencing the practical steps that DND/CAF can take now, while laying the foundation for NATO and allied partners to integrate AI responsibly over the longer term.

Conclusion

The China-U.S. contest over AI is not a distant spectacle; it is the context in which Canada's defence choices will either mature into allied advantage or ossify into vulnerability. Canada and other democracies have the institutional and collaborative foundations to advance defence AI, but their effectiveness depends on maintaining public trust, agile governance, and resilient innovation ecosystems.⁴⁹ Democracies also hold measurable strengths: they have the world's best computing ecosystems, and the talent to keep pushing the frontier—but advantage is perishable. Autocratic rivals will move quickly where law and ethics constrain us; corporate platforms will tilt toward profit unless we bend incentives toward security; and procurement will default to slow unless leaders deliberately buy speed.

DND/CAF's task is not to match the superpowers chip for chip or model for model. It is to be interoperable on timelines that match the pace of our allies and our operational needs, to protect and mobilize the data that matter, to secure assured access to compute, to reform institutions so that good ideas reach troops before they stale, and to nurture the talent that makes all of that possible. In doing so, DND/CAF will not only defend its own

“AI will not replace strategy, but it will reward those who treat it as strategic.”

interests but also strengthen the coalition logic on which our security rests. AI will not replace strategy, but it will reward those who treat it as strategic—who convert values into governance, governance into capability, and capability into combined effect.

By moving deliberately, DND/CAF can ensure that AI strengthens decision-making, protects resilience in the information domain, and reinforces credible deterrence. Done right, these capabilities will enhance the security of Canada and its allies and demonstrate that advanced technologies can be integrated responsibly in the service of free and democratic societies.

Notes

- 1 AI advancements in defence aim to balance innovation with responsible and ethical AI development, while other stakeholders are focused on using it for decision superiority. See: Mind Foundry, "Defence and National Security AI Strategies - The Global Landscape," 27 November 2025.
- 2 Meredith Chen, "China's Growing Civilian-Defence AI Ties Will Challenge US, Report Says," *South China Morning Post*, 7 September 2025. Originally found at: <https://www.scmp.com/news/china/military/article/3324727/chinas-growing-civilian-defence-ai-ties-will-challenge-us-report-says>.
- 3 Cullen O'Keefe, "Chips for Peace: How the U.S. and Its Allies Can Lead on Safe and Beneficial AI," *Lawfare*, 10 July 2024. Originally found at: <https://www.lawfare-media.org/article/chips-for-peace-how-the-u.s.-and-its-allies-can-lead-on-safe-and-beneficial-ai>.
- 4 Department of National Defence, *Pan-Domain Command & Control (PDC2) Concept Paper* (Government of Canada, 9 December 2024). Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/pan-domain-command-control.html>.
- 5 Branka Marijan, "The Dilemma of Dual-Use AI," *The Ploughshares Monitor*, 18 September 2023. Originally found at: <https://ploughshares.ca/the-dilemma-of-dual-use-ai/>.
- 6 Karen M. Sutter, *U.S. Export Controls and China: Advanced Semiconductors* (Congressional Research Service, 9 September 2025). Originally found at: <https://www.congress.gov/crs-product/R48642>.
- 7 Enrique Dans, "Super Apps: A Path to Surveillance in China and Russia," Center for European Policy Analysis, 12 September 2025. Originally found at: <https://cepa.org/article/super-apps-a-path-to-surveillance-in-china-and-russia/>.
- 8 KPMG, "Future Forward: Following the Money in AI," 2025. Originally found at: <https://kpmg.com/xx/en/our-insights/value-creation/future-forward.html>.
- 9 Erica Stanford, "Who is Responsible When AI Acts Autonomously & Things Go Wrong?," *Global Legal Insight*, 15 May 2025. Originally found at: <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/autonomous-ai-who-is-responsible-when-ai-acts-autonomously-and-things-go-wrong/>.
- 10 Department of National Defence and Canadian Armed Forces, *Artificial Intelligence Strategy*, Government of Canada, 3 March 2024. Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/dndcaf-ai-strategy.pdf>.
- 11 Akshay Kulkarni, "AI-Generated Wildfire Images Spreading Misinformation in B.C., Fire Officials Warn," *CBC News*, 6 August 2025.
- 12 Department of National Defence, "The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy," 3 March 2024. Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/dndcaf-ai-strategy.pdf>.
- 13 Department of National Defence, *Security, Sovereignty and Prosperity: Canada's Defence Industrial Strategy*, March 2026. Originally found at: <https://www.pm.gc.ca/en/news/news-releases/2026/02/17/prime-minister-carney-launches-canadas-first-defence-industrial>.
- 14 Nicolas Chaillan, "The Fast Track to Mission-Ready AI: Buy What Works, Skip the Build," *Government Technology Insider*, 8 July 2025. Originally found at: <https://governmenttechnologyinsider.com/the-fast-track-to-mission-ready-ai-buy-what-works-skip-the-build/>.
- 15 Margarida Ramos Borges da Silva, Jasper van Teeffelen, and Çağrı Çavuş, "Big Tech Acquires a New Company Every 11 Days," *SOMO*, 15 April 2025. Originally found at: <https://www.somo.nl/big-tech-acquires-a-new-company-every-11-days/>.
- 16 Didi Tang and Collin Binkley, "Pentagon-Funded Projects Helped Chinese Military: House GOP Report," *AP News*, 5 September 2025. Originally found at: <https://apnews.com/article/china-pentagon-funding-research-military-bf8640d0e04c-016f4af513350078d58c>.
- 17 U.S. National Security Agency and Cybersecurity and Infrastructure Security Agency, *Use Secure Cloud Key Management Practices*, March 2024. Originally found at: <https://media.defense.gov/2024/Mar/07/2003407858/-1/-1/0/CSI-CloudTop10-Key-Management.PDF>.
- 18 Office of the Under Secretary of Defense for Research and Engineering, *Software Engineering for Continuous Delivery of Warfighting Capability* (U.S. Department of Defense, April 2023). Originally found at: <https://www.cto.mil/wp-content/uploads/2023/07/SWE-Guide-April2023.pdf>.
- 19 James Kavanagh, "AI Model Lifecycle Governance," *Ethos AI*, 23 June 2025. Originally found at: <https://www.ethos-ai.org/p/ai-model-lifecycle-governance?>

- 20 Cybersecurity and Infrastructure Security Agency, *Securing the Software Supply Chain: Recommended Practices for Suppliers* (Department of Homeland Security, September 2022). Originally found at: https://www.cisa.gov/sites/default/files/2024-08/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS_508.pdf.
- 21 For example, amendments to the United States (U.S.) CLOUD Act in 2024-2025 reaffirm that US authorities may compel U.S.-based cloud and technology providers to provide access to data under their legal control, regardless of the data's physical storage location.
- 22 World Economic Forum and Accenture, *Blueprint to Action: China's Path to AI-Powered Industry Transformation*, January 2025. Originally found at: https://reports.weforum.org/docs/WEF_Blueprint_to_Action_Chinas_Path_to_AI-Powered_Industry_Transformation_2025.pdf.
- 23 Robert O. Work and Tara Murphy Dougherty, "It's Time for the Pentagon to Take Data Principles More Seriously," *War on the Rocks*, 6 October 2020. Originally found at: <https://warontherocks.com/2020/10/its-time-for-the-pentagon-to-take-data-principles-more-seriously/>.
- 24 Harry Davies and Yuval Abraham, "Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support during Gaza War," *The Guardian*, 23 January 2025. Originally found at: <https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft>.
- 25 Brodi Kotila et al., *Strengthening the Defense Innovation Ecosystem* (RAND Corporation, 7 March 2023). Originally found at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1352-1/RAND_RR1352-1.pdf.
- 26 Stefan Vladislavjev, "Surveying China's Digital Silk Road in the Western Balkans," *War on the Rocks*, 3 August 2021. Originally found at: <https://warontherocks.com/2021/08/surveying-chinas-digital-silk-road-in-the-western-balkans/>.
- 27 Thomas Morley and Matthew Schrader, "Huawei Espionage Arrests in Poland: A Wake-up Call to Europe," German Marshall Fund of the United States, accessed 25 September 2025. Originally found at: <https://www.gmfus.org/news/huawei-espionage-arrests-poland-wake-call-europe>.
- 28 Innovation, Science and Economic Development Canada, *Policy Statement - Securing Canada's Telecommunications System* (Government of Canada, 18 May 2022). Originally found at <https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement-securing-canadas-telecommunications-system.html>.
- 29 Darren Death, "Understanding and Addressing Supply Chain Risks in AI Systems," LinkedIn, 8 January 2025. Originally found at: <https://www.linkedin.com/pulse/understanding-addressing-supply-chain-risks-ai-systems-death-kz2jc>.
- 30 House of Commons, *Standing Committee on National Defence, Evidence*, 45th Parliament, 1st Session, Meeting No. 9, 23 October 2025 (Canada). Originally found at: <https://www.ourcommons.ca/DocumentViewer/en/45-1/NDND/meeting-9/evidence>.
- 31 Chloe Autio, Kate Cummings, Brinson S. Elliott, and Beth Simone Noveck, "A Snapshot of Artificial Intelligence Procurement Challenges," The GovLab, 2023. Originally found at: <https://files.thegovlab.org/a-snapshot-of-ai-procurement-challenges-june2023.pdf>.
- 32 Akhil Gupta, "Government AI Adoption: Unique Challenges in Pricing and Procurement," Agentic AI Pricing, 6 January 2025. Originally found at: <https://www.agenticaipricing.com/government-ai-adoption-unique-challenges-in-pricing-and-procurement/>.
- 33 Defence Research and Development Canada (DRDC) has a long history of working in AI across domains like ISR data fusion, pan-domain situational awareness, cybersecurity, robotics, and training. Other key initiatives that could accelerate the commercial development of Canadian Defence AI solutions include Defence Excellence and Security (IDEaS), Mobilizing Insights in Defence and Security (MINDS), and the newly opened Bureau of Research, Engineering and Advanced Leadership in Innovation and Science (BOREALIS).
- 34 Through NATO DIANA's Rapid Adoption Service, DND/CAF is in the process of acquiring an autonomous uncrewed vehicle from a firm called HonuWorx, which will be controlled through a cloud-based mission platform and contribute to DND/CAF's ability to maintain, operate and manipulate deep sea infrastructure and other subsea objects.
- 35 Alex McPhail, and Alexander Rudolph, and Phillippe Lagassé, "Defence Agile Procurement: Insights and Analysis (DAPIA) Report," EXA Consulting Group, 10 July 2025. Originally found at: <https://static1.squarespace.com/static/5cd08376797f742115eaa7cc/t/68af61b380a0f3571c695ae9/1756324275338/Final+Report++Defence+Agile+Procurement+Insights+and+Analysis.pdf>.
- 36 Carlo Munoz, "Pentagon Rolls Out JWCC Cloud Accelerator Initiative," *Janes*, 31 October 2023. Originally found at: <https://www.janes.com/osint-insights/defence-news/defence/pentagon-rolls-out-jwcc-cloud-accelerator-initiative>.
- 37 U.S. Defense Innovation Board, *Scaling Nontraditional Defense Innovation*, Department of War, 8 January 2025. Originally found at: <https://innovation.defense.gov/Portals/63/DIB%20Scaling%20Nontraditional%20Defense%20Innovation%20250113%20PUBLISHED.pdf>.
- 38 MITRE Corporation, *AI Red Teaming: Advancing Safe and Secure AI Systems*, July 2024. Originally found at: <https://www.mitre.org/sites/default/files/2024-07/PR-24-01820-4-AI-Red-Teaming-Advancing-Safe-Secure-AI-Systems.pdf>.
- 39 For further guidance on these evaluation practices, see the U.S. Department of Defense Responsible AI Toolkit, which provides lifecycle assessments and assurance tools for AI systems, and the UK Ministry of Defence's JSP 936, which sets out requirements for dependable, safe, and robust defence AI capabilities. See: Department of Defense, *Responsible Artificial Intelligence (RAI) Toolkit*, Chief Digital and Artificial Intelligence Office, 14 November 2023. Originally found at: <https://rai.tradewindai.com/>; Ministry of Defence, JSP 936: *Dependable Artificial Intelligence (AI) in Defence (Part 1: Directive)*, 13 November 2024. Originally found at: <https://www.gov.uk/government/publications/jsp-936-dependable-artificial-intelligence-ai-in-defence-part-1-directive>.
- 40 Michael Houghton, "Canada's Innovation Pipeline Is Stalling: Sir Michael Houghton Calls for a VC Mindset Shift," *Digital Journal*, 24 September 2025. Originally found at: <https://www.digitaljournal.com/business/canadas-innovation-pipeline-is-stalling-sir-michael-houghton-calls-for-a-vc-mindset-shift/article>.
- 41 U.S. Congress, Senate Committee on Small Business and Entrepreneurship, *Golden Age of American Innovation: Reforming SBIR-STTR for the 21st Century*, S. Hrg. 119-20, 119th Cong., 1st sess., 5 March 2025. Originally found at: <https://www.congress.gov/event/119th-congress/senate-event/LC74425/text>.
- 42 IBM, "What Is Cloud Cost Management?," 5 October 2023. Originally found at: <https://www.ibm.com/topics/cloud-cost-management>.
- 43 Treasury Board of Canada Secretariat, *Government of Canada White Paper: Data Sovereignty and Public Cloud* (Government of Canada, 2018). Originally found at: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html>.
- 44 NATO, "NATO's Approach to Counter Information Threats," 3 February 2025. Originally found at: https://www.nato.int/cps/en/natohq/topics_219728.htm.
- 45 Ann M. Fitz-Gerald, Carsten Maple, and Halyna Padalko, "Collaborative AI Governance: A Policy Roadmap for Canada and the UK," Royal United Services Institute, 13 November 2024. Originally found at: <https://www.rusi.org/explore-our-research/publications/commentary/collaborative-ai-governance-policy-roadmap-canada-and-uk>.
- 46 Steve Feldstein, "The Global Expansion of AI Surveillance," *Carnegie Endowment for International Peace*, 17 September 2019. Originally found at: <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en>.
- 47 Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2025-2026* (Government of Canada, 2024). Originally found at: <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf>.
- 48 Canadian Security Intelligence Service, "Safeguarding Western Tech Startups: Exploitation of International Pitch Competitions," 8 September 2025.
- 49 Pew Research Center, *Representative Democracy Remains a Popular Ideal, but People Around the World Are Critical of How It's Working* (Washington, DC: Pew Research Center, 28 February 2024). Originally found at: https://www.pewresearch.org/global/wp-content/uploads/sites/2/2024/02/gap_2024.02.28_democracy-closed-end_report.pdf.



Canadian and French Joint Terminal Attack Controller (JTAC) set up lasers for air strike and look through binoculars to ensure the drop zone is clear during EX MAPLE STRIKE at Shaver drop zone located at Jimmy Lake, Alberta.

Photo: Corporal Connie Valin, Canadian Armed Forces photo

Allied Interoperability Under Pressure: AI, Procurement, and the Future of Defence Cohesion

SAMUEL PAQUETTE AND MAJOR TYLER CURRIE

Samuel Paquette is a policy analyst within the DND/CAF AI Centre. He recently completed a master's degree in international affairs at Carleton University and previously worked as a graduate researcher attached to the strategic joint staff at Defence Research and Development Canada (DRDC).

Tyler Currie is a CAF AI integration and acceleration officer who works at the DND/CAF AI Centre. Tyler has spent 16 years as part of the Intelligence Branch and has served on deployed operations in Afghanistan and in the international context with Joint Forces Command (JFC) Naples. Tyler holds a master's in political studies from Queen's University as well as a Master of Management in Artificial Intelligence (MMAI) from the Queen's Smith School of Business.

Artificial Intelligence (AI) is becoming the connective tissue of modern defence alliances, linking data, platforms, and decision-making across borders.

For the Department of National Defence and Canadian Armed Forces (DND/CAF) and NATO, the central challenge is ensuring that AI adoption consistently strengthens interoperability, a core foundation for effective joint operations. Allies face constant pressure from shortages of advanced semiconductors, shifting technology markets, rigid procurement processes, and differing AI rules and standards. These pressures make it even more important to reinforce interoperability. They impact how quickly allies can integrate new capabilities, how reliably systems communicate in the field, and how effectively AI-enabled tools support commanders during operations. The stakes are high, and with shared standards and resilient procurement strategies, AI can accelerate decision-making, deepen integration, and deliver a decisive edge in the battlespace.

NATO has declared AI a transformative capability, but realizing its full potential depends on secure NATO-standard cloud systems, seamless allied networks, and common data languages that let Canadian platforms connect directly with coalition systems. These foundations enable AI to compress decision cycles, produce clearer intelligence, and strengthen deterrence. Delivering this advantage requires common standards, joint testing and certification, and shared data architectures. AI's operational value depends on preserving human judgment at critical moments, ensuring that commanders remain accountable for the use of force and that human oversight remains embedded across the decision cycle. By focusing on these enablers, DND/CAF and NATO can ensure that AI strengthens interoperability every day, turning technological progress into collective advantage.

At the same time, several factors challenge allied operations. Volatile markets for chips, cloud capacity, and critical minerals strain readiness; persistent procurement friction slows the fielding of fast evolving AI capabilities; and emerging NATO standards and governance frameworks should mature to ensure trusted, interoperable systems. Together, these pressures shape Canada's procurement posture and determine how effectively it can remain aligned with allies as AI accelerates the tempo of modern warfare.

For Canada, a committed middle power and trusted voice in NATO, procurement and governance are front-line enablers of security and will be essential to achieving the DND/CAF AI Strategy's objective to become AI-enabled by 2030. When designed with interoperability in mind, they create the conditions for DND/CAF to integrate seamlessly with allies, contribute distinctive strengths, and remain a credible partner in collective defence. By embedding modular procurement practices, championing open standards, and aligning governance frameworks with NATO principles, DND/CAF can help ensure that new AI systems are trusted, agile, and rapidly deployable across the alliance. These choices turn AI into a true force multiplier, enhancing DND/CAF's ability to contribute to deterrence, deepening allied collaboration, and safeguarding our relevance in tomorrow's battlespace.

“ The race to adopt AI in defence does not unfold in a vacuum. It is directly shaped by the volatility of global markets for the hardware, infrastructure, and talent that make AI possible.”

Market Volatility and Readiness

The race to adopt AI in defence does not unfold in a vacuum. It is directly shaped by the volatility of global markets for the hardware, infrastructure, and talent that make AI possible—without them, even the most ambitious defence strategies risk stalling.

At the core of this challenge is the global chip supply chain. Training advanced AI models requires high-performance processors such as Nvidia's H100, chips produced almost exclusively by a single company that controls more than 90 percent of the world's leading-edge production.¹ For allied militaries, this creates unequal access to computing power, which in turn risks fragmenting the pace at which nations can field interoperable AI-enabled capabilities. Exploding demand across civilian industries has driven up costs and strained availability.² For militaries, delays in acquiring computing power translate directly into operational gaps.

Cloud infrastructure is equally critical, since access to chips and cloud together determines whether a state can train, deploy, and scale AI systems. Data centres themselves have become national security assets, both indispensable and vulnerable to cyberattacks, insider threats and sabotage. Governments and industry are investing heavily to secure these facilities, recognizing that resilient computing ecosystems confer lasting advantages in domains such as cyber operations, autonomous systems, and space surveillance.³ Without secure and scalable cloud capacity, allies cannot train shared models, exchange operational data, or run AI-enabled tools across multinational missions.

Geopolitics further amplifies this volatility. Supply chains for critical minerals remain concentrated, and export restrictions have at times limited access to rare earths and other essential inputs. These disruptions drive up costs and delay infrastructure projects, underscoring the importance for DND/CAF and its allies to strengthen supply chain resilience, diversify sources, and invest in domestic and allied capacity to sustain long-term readiness.⁴ For Canada, which has limited domestic semiconductor

fabrication capacity, these disruptions pose a heightened risk compared to larger allies with more diversified industrial bases.

Within NATO, some members can buffer market shocks by sponsoring domestic semiconductor production, investing in AI start-ups, or stockpiling critical minerals.⁵ Others contribute by pooling resources, supporting multinational initiatives, or leveraging regional strengths.⁶ What matters is that these varied approaches reinforce one another, ensuring capability development remains balanced and command-and-control integration is strengthened across the alliance. For Canada, the stakes are immediate. The country faces ongoing challenges in scaling secure cloud and AI infrastructure, has limited advanced hardware manufacturing capacity, and relies on a small but steadily growing defence tech industry. As a middle power, it cannot rely on scale or spending alone but should secure its position through resilience and collaboration. While larger allies may absorb shocks through sheer investment, Canada should focus on resilience planning, stockpiling critical components, diversifying supply chains, and deepening allied compute partnerships. This effort is already underway. Since 2016, Canada has committed more than \$4.4 billion to AI research and digital infrastructure, including the 2025 AI Sovereign Compute Strategy, which directs \$2 billion toward building a sovereign cloud, expanding domestic computing capacity, and reducing reliance on foreign-owned platforms.⁷ Canada also holds one of the world's richest reserves of rare-earth elements—resources that, if managed responsibly, can support allied supply security well into the future.⁸

“Traditional defence procurement was designed for ships and aircraft that take decades to develop, not for algorithms that can become obsolete in months.”

Advanced processors, resilient cloud infrastructure, and reliable supplies of critical minerals are as essential to defence as ships, aircraft, or satellites. They determine whether AI tools can function at scale and in coordination with allies. For Canada, this means using its middle-power leverage strategically—investing at home, collaborating abroad, and anticipating market cycles before they become crises. By reinforcing resilience in this way, DND/CAF can ensure that its AI adoption strengthens alliance cohesion and safeguards its role as a trusted and capable partner in NATO.

Procurement Friction

Even when funding is available, procurement systems struggle to keep pace with AI's rapid innovation cycle. Traditional defence procurement was designed for ships and aircraft that take decades to develop, not for algorithms that can become obsolete in months. As a result, organizations may identify urgent needs but spend years moving from requirements-setting to contracts to delivery—only to field systems that are outdated by the time they arrive.

The U.S. Department of Defense's cloud modernization illustrates this vulnerability. First announced in 2017, the Joint Enterprise Defense Infrastructure (JEDI) aimed to consolidate cloud services under a single \$10 billion contract with one company.⁹ Years of legal challenges followed, and by 2021 the contract was cancelled, obsolete before it was implemented. It was replaced in 2022 with the Joint Warfighter Cloud Capability (JWCC), a multi-vendor and more flexible model.¹⁰ The lesson was clear: fixed, single-vendor contracts risk locking militaries into rigid solutions that cannot keep pace with technological change.

The same pattern applies across other fast-evolving areas of AI. By the time a procurement process is completed, the models or sensors originally specified may already have been overtaken by more capable versions. In domains such as autonomous drones, cyber defence, and natural language processing, multi-year acquisition cycles risk producing systems that are new for the warfighter but are already outmatched by new capabilities from adversaries that have faster acquisition cycles.¹¹

Other states face fewer constraints. China's centralized civil-military fusion strategy moves AI rapidly from civilian research to military application, without public scrutiny or transparent competition. State-owned enterprises with direct ties to China's People's Liberation Army are awarded contracts, accelerating development in areas such as autonomous vehicles, electronic warfare, and automated target recognition.¹² While DND/CAF and its allies rightly reject this approach on ethical and governance grounds, the pace at which adversaries can field AI highlights the urgency of modernizing procurement to remain competitive.

For DND/CAF, these dynamics translate into familiar but persistent challenges. Like many allies, procurement culture is risk-averse and layered with reviews and compliance checks that can extend timelines into decades.¹³ These systems were designed to manage accountability for major long-life platforms, but they do not align with the tempo of AI innovation. As a result, integrating rapidly evolving capabilities at the same pace as partners experimenting with more agile approaches—and competitors able to field new systems quickly—can present ongoing challenges.

Agile procurement is vital not only to keep pace with AI innovation but also to ensure that every supplier complies with Defence cybersecurity standards. Legacy procurement operates through monolithic contracts that often deliver closed “black box” systems that accumulate technical debt over time: software



A Royal Canadian Navy member on aboard HMCS HARRY DEWOLF operates the radar system to monitor the ship's surroundings as it approaches the port of Montego Bay, Jamaica during Operation CARIBBE, December 1, 2021.

Photo: Canadian Armed Forces Photo

is hard to update, vulnerabilities linger, and opaque subcontracting chains obscure supply-chain risk. By contrast, modular and open architectures enable continuous patching, component-level upgrades, and greater transparency in supplier evaluation. Rather than concentrating risk within a single proprietary ecosystem, these architectures distribute and manage it across interoperable components. In this way, agile procurement strengthens resilience, ensures that all suppliers prioritize open-source solutions, and operate to the same cybersecurity baseline required by Defence. DND/CAF is actively supporting evolving procurement processes so that AI can be integrated at the speed required for modern operations. This involves testing more agile approaches and creating pathways for rapid prototyping and iteration so that new capabilities remain relevant over time, can be updated as technology advances, and are designed to interoperate with allied systems from the outset.

There are promising paths forward. DND/CAF has also begun experimenting through Innovation for Defence Excellence and Security (IDEaS), which uses contests, test drives, and sandboxes to accelerate innovation.¹⁴ These tools allow new ideas to be tested quickly and at low cost, without locking the CAF into long-term commitments before technologies have proven their value.

Some experts also point to flexible contracting mechanisms like the Other Transaction Authorities (OTAs) used by the U.S. Defence Innovation Unit, which enable rapid prototyping and bypass many of the bureaucratic hurdles of traditional procurement.¹⁵

Agile contracts and pilot projects should be tied directly to common data architectures, modular certification, and NATO assurance frameworks. In this way, procurement becomes a foundation for cohesion, ensuring that new AI capabilities are not only delivered faster but also fielded in ways that strengthen alliance trust and interoperability.

NATO Standards and Cohesion

NATO's advantage rests on interoperability, on the ability of allies to share data, trust each other's systems, and fight as one. In practice, this requires more than compatible equipment alone: it depends on shared rules, standards, and governance frameworks that give every member confidence in how AI systems are designed, tested, and deployed. As allies pursue different approaches to regulation, the alliance has made standard-setting a priority.

One example of this emerging work is the concept of an AI Exchange under discussion within certain NATO countries. The

idea is to develop a shared mechanism for testing and validating AI systems against agreed alliance principles. If developed, the passport would function much like a security clearance for technology; once a system is certified by one ally, others could adopt it without duplicating the process. This reduces costs and delays, while also giving militaries assurance that AI-enabled tools meet NATO's requirements for safety, accountability, and reliability.

For DND/CAF, the value of this initiative is twofold. First, it offers a way to avoid duplicating certification, ensuring Canadian-developed technologies are ready for allied use the moment they are fielded. Second, it provides DND/CAF with a chance to shape the framework itself, contributing lessons from its own experience in responsible AI. Having already helped advance global norms through the OECD, the G7 Hiroshima Process, and the Responsible AI in the Military Domain Summit, DND/CAF is well-positioned to translate that experience into NATO's operational context. Aligning procurement processes with this kind of mechanism would ensure that Canadian systems—whether cloud-based command tools or AI-enabled surveillance platforms—integrate smoothly with those of allies.

More broadly, the AI Exchange demonstrates how NATO can transform national differences into collective strength. Member states may legislate or regulate AI in different ways, but the passport would create a common language of trust. It reflects the alliance's ability to coordinate without erasing national sovereignty, ensuring that innovation in one country can become a capability for all.

The AI Exchange offers middle powers like Canada a practical way to avoid being locked into systems that do not align defence priorities, while reducing the risk of procuring sovereign solutions that cannot be interoperable with allies. For example, sovereign AI-enabled ISR, logistics, or decision support tools may struggle to be integrated with systems when assurance standards diverge. By providing a shared assurance standard, the AI Exchange maintains flexibility for middle powers to agree upon technical safeguards and prevents larger states from setting standards through scale alone. This work is especially timely because allies are advancing distinct governance models. The European Union's AI Act is the most ambitious, creating a comprehensive risk-based framework that applies to nearly all uses of AI.¹⁶ It imposes strict requirements on high-risk systems such as biometric identification, critical infrastructure, and health-care—and while it exempts military uses, it still shapes dual-use technologies that often cross into the defence sphere.¹⁷ For NATO, this means that Europe's regulatory environment will strongly influence how companies develop AI and how those systems can be shared across borders.

The United States has taken a different path, preferring sector-specific guidance and principle-based frameworks over a single law. The White House AI Bill of Rights and the U.S. National Institute of Standards and Technology's (NIST) AI Risk Management Framework are prominent examples, alongside

executive orders, directing agencies to safeguard innovation while protecting rights.¹⁸ This approach encourages private-sector leadership and rapid scaling, but because it is decentralized, additional NATO assurance mechanisms are often needed before U.S. systems can be fully trusted in allied operations.

Canada's trajectory has been more complicated. The Artificial Intelligence and Data Act (AIDA), introduced in 2022, was intended to establish a national framework for regulating AI according to risk. Inspired partly by the EU model but designed with U.S.-style flexibility, it sought to balance oversight with innovation. However, with the prorogation of Parliament in January 2025, AIDA died on the Order Paper, leaving Canada without a dedicated AI law.¹⁹ Even so, the experience sharpened national debates and clarified future directions. Canada continues to apply existing human rights, privacy, and consumer protection laws, while building credibility through its DND/CAF AI Strategy, AI Strategy for the Federal Public Service, and contributions to NATO discussions.

These diverging approaches underscore why mechanisms like the AI Nexus are essential. Without them, some dual-use technologies developed under commercial standards may not align with NATO testing and evaluation requirements, creating potential for security gaps that could complicate deployment if imported to another country. With the EU advancing strict legal frameworks, the U.S. relying on sectoral guidance, and Canada recalibrating after AIDA, NATO needs common certification to bridge these models. For Canada, this is an opportunity to act as a bridge, helping align transatlantic practices in ways that are operationally effective yet still reflect democratic oversight.

At first glance, these governance differences may seem technical. In reality, they shape whether allies can trust and use each other's AI systems. A dual-use application such as a drone navigation algorithm might be fully legal in one jurisdiction but face restrictions in another due to certification conflicts. Data localization laws could limit cross-border model training, and differing interpretations of "responsible AI" could complicate shared assurance mechanisms. These vulnerabilities may create supply chain delays, slow system upgrades and model retraining across allied systems, and ultimately undermine trust. Practical mechanisms are therefore indispensable to ensure systems interoperate across borders and contexts.

NATO has already taken steps in this direction. Its AI Strategy (2021, updated in 2024) sets out five guiding principles: lawfulness, responsibility, reliability, governability, and bias mitigation.²⁰ While not legally binding, these principles provide a baseline of shared expectations. To move from principle to practice, NATO has launched mechanisms such as the Data and Artificial Intelligence Review Board (DARB), which brings together governments, industry, and academia to shape standards for testing, validation, and certification, and the Defence Innovation Accelerator for the North Atlantic (DIANA), which runs joint trials at test centres across Europe and North America.²¹ Together,

these initiatives demonstrate the alliance's commitment to building trust and ensuring interoperability at scale.

For Canada, the task is to contribute actively to this translation of principle into practice. This means aligning domestic implementation of NATO's AI principles while navigating a balanced path between the EU's risk-based regulatory model and the United States' sector-specific approach, enabling adaptive certification across jurisdictions. A modular, shared governance framework would facilitate cross-border AI deployment through open architectures and reinforce operational trust among allies. By shaping certification frameworks, embedding interoperability into procurement, and ensuring that governance mechanisms advance trust as well as speed, DND/CAF can help NATO preserve its most decisive advantage: the ability to act collectively, with confidence, and at pace.

Governance as an Enabler

Governance is often described as a brake on innovation, but in practice it is what makes innovation usable, reliable, and trusted at scale across an alliance. For NATO, governance functions less like a stoplight and more like a navigation system: it does not slow progress, it ensures that members move in the same direction and arrive together. This becomes visible in exercises such as Steadfast Duel, where AI-enabled tools were integrated into multinational command-and-control structures and tested against shared doctrines, responsible AI principles, and interoperability standards before adoption.²² It is the engine that ensures AI adoption is not only rapid but also responsible, interoperable, and enduring.

If Canadian, American, or European personnel are to rely on AI-enabled tools in combined operations, they should know that the underlying data, algorithms, and safeguards meet agreed standards. Without that assurance, hesitation could creep into the decision cycle.²³ With it, commanders can act decisively, knowing that an AI-generated course of action or intelligence product from one ally can be trusted by all. Common approaches to testing, validation, and certification make this possible, turning national capabilities into collective strength.

In practice, NATO operationalizes governance by developing joint doctrines, shared technical standards, and coordinated testing environments. Standardization agreements establish common data-exchange and interface requirements, while Allied joint publications integrate emerging technologies into shared operational concepts. On the AI front, mechanisms such as DARB and DIANA aim to give nations shared assurance that AI tools meet NATO's principles for reliability and safety. The task now is to deepen and expand these efforts, broadening certification to cover more use cases, linking test centres more directly to operational commands, and ensuring that lessons learned from trials are rapidly integrated back into procurement.

Beyond NATO, the Five Eyes intelligence community, including Canada through the Communications Security Establishment (CSE), reinforces these efforts. By issuing joint technical advisories on safe AI deployment and cyber defence, they provide common guidance on issues like system hardening, data integrity, and risk mitigation.²⁴ This coordination helps ensure that allied militaries face the same threats with consistent defensive measures, whether against data poisoning, adversarial manipulation, or cyber intrusion. Taken together, these initiatives show how governance can be operationalized, not as high-level statements, but as concrete mechanisms that build trust and ensure AI systems are deployable across borders.

Canada has a unique role to play in strengthening these initiatives. The Directive on Automated Decision-Making and the DND/CAF AI Strategy already embed values such as lawfulness, transparency, and accountability.²⁵ By linking these domestic frameworks to NATO certification and testing processes, Canada can demonstrate how principles enshrined at the national level can directly reinforce alliance interoperability. This dual anchoring ensures Canadian systems are interoperable from the start and provides a model other middle powers can follow.

Governance should also be agile. NATO's principles should be applied through modular certification, sandbox environments, and iterative testing processes that evolve alongside the technology.²⁶ A modular approach means a system does not need to be re-certified in its entirety every time a component is updated, saving time while preserving trust. Sandboxes allow experimentation in controlled environments, giving innovators space to push boundaries while ensuring safety. Iterative testing ensures that once systems are fielded, they remain trustworthy under real-world conditions. This approach allows allies to field new AI capabilities quickly, while still maintaining the shared assurance that underpins interoperability.

Operationalizing governance also requires confronting concrete supply-chain and cyber threats. AI-enabled defence systems face risks ranging from firmware tampering, hardware backdoors, and third-party software vulnerabilities to adversarial machine learning techniques such as poisoned training data and evasion attacks, as well as emerging quantum decryption risks. Left unmanaged, these vulnerabilities can erode trust and undermine interoperability across allied networks.

Mitigating them demands embedded supply chain management safeguards: zero-trust principles that continuously verify users and devices; persistent monitoring through anomaly detection; shared cyber threat intelligence among allies; and regular red-teaming and joint certification under NATO assurance frameworks. Practical safeguards such as mitigating prompt injection, sanitizing inputs, restricting high-risks tools, and filtering outputs to reduce the likelihood of AI misuse can reduce AI system compromise.²⁷ By integrating these measures into procurement and certification processes, DND/CAF can ensure that AI-enabled

systems remain secure, resilient, and trusted across the alliance. In short, governance is not a constraint but a force multiplier. It transforms AI from a collection of national projects into a shared capability, allowing NATO to move fast together rather than each member advancing in isolation. For DND/CAF, championing governance as an enabler ensures that investments in AI are not only responsible but also interoperable, strategically relevant, and firmly embedded in the trust that defines the alliance.

What Does this Mean for the Canadian Procurement Posture?

The DND/CAF AI Strategy sets a bold ambition to be an AI-enabled force by 2030, using “ethical, inclusive, and trusted AI for interoperability and advantage in the battlespace.”²⁸ Achieving this goal requires more than strategy documents. It demands a cultural and structural shift. Procurement should be treated as a central enabler of interoperability from the very beginning, not as an afterthought. Every acquisition decision needs to guarantee that Canadian systems connect seamlessly with allied platforms and remain adaptable as technology evolves.

Meeting that challenge calls for a shift from traditional, rigid models of procurement toward approaches that are modular, agile, and talent-driven. Modularity ensures that capabilities can be refreshed without being replaced. Instead of locking into closed, single-vendor systems that age quickly, the CAF should prioritize open architectures that allow incremental upgrades as new algorithms, sensors, and communications tools emerge. This mirrors the shift in many allied militaries toward plug-and-play systems that reduce dependence on one supplier and maximize flexibility. Agile, life-cycle integration is equally essential. AI systems are never static; they learn, drift, and should be retrained. Procurement should reflect this reality by adopting iterative testing, flexible requirements, and continuous dialogue with suppliers.²⁹ Rather than waiting years for a capability to be delivered, the CAF can use rolling upgrades to keep systems aligned with the pace of innovation. For example, the UK’s integrated procurement model commits to fielding a minimum deployable capability quickly and then iteratively improving it over time, shortening timelines for digital systems while embedding continuous upgrades throughout the acquisition lifecycle.³⁰

People are as important as platforms. Governance frameworks only succeed when personnel are able to apply them. Canada faces a shortage of AI, cybersecurity, and data specialists, limiting the speed at which DND/CAF can deploy and assess AI systems. Competition with the private sector makes it difficult to recruit and retain technical personnel.

To mitigate these factors, the CAF needs to invest in career tracks for AI specialists and data scientists, develop a technical reserve corps to surge expertise into short-term projects, and equip operators with practical skills. This means building training pipelines that combine technical knowledge with the military

context—for example, integrating AI modules into officer and non-commissioned officer professional development, establishing partnerships with Canadian AI institutes, and offering secondments where military personnel rotate through industry and academic labs.³¹ These exchanges would strengthen skills while embedding a culture of collaboration. Training should also cover practical application, responsible uses, and how to address cybersecurity risks, including access control of AI systems. From managing data pipelines to prompting large language models, operators need confidence that AI tools save time and sharpen decision-making rather than add complexity.³² Building trust between humans and machines will be just as important as the technical performance of the systems themselves.

Finally, procurement choices should reinforce DND/CAF’s resilience and allied cohesion. Short-term savings on low-cost technologies that cannot be integrated or trusted may appear attractive, but they ultimately undermine sovereignty and interoperability.³³ This lesson applies not only to hardware but to software models as well. Closed or opaque systems developed by non-allied suppliers can introduce hidden vulnerabilities or restrict DND/CAF’s ability to update and certify tools. Prioritizing Canadian and allied sources of hardware and software, supported by open standards and transparent development practices, helps ensure both security and interoperability. It also strengthens Canada’s defence-industrial base, giving domestic firms a clearer role in NATO supply chains.

DND/CAF’s role is not simply to buy equipment faster, but to shape the market around the principles of openness, resilience, and trust. By joining joint procurement initiatives with allies, pooling demand for secure cloud infrastructure, and leveraging its natural advantage in rare-earth elements, DND/CAF can amplify its influence far beyond what its budget size might suggest. In this way, procurement becomes a tool of strategy as much as of logistics—aligning domestic industry, allied standards, and operational needs in one coherent framework.

Taken together, these steps will allow DND/CAF to balance fiscal discipline with the need for speed and trust. They will also ensure that the CAF can integrate AI into new platforms, such as the F-35, River-class destroyers, and NORAD modernization systems, in ways that are adaptable, resilient, and fully interoperable. Procurement, in this context, is no longer just about acquiring material. It is about embedding interoperability, resilience, and strategic relevance into every decision. By doing so, DND/CAF not only strengthens its national defence but also reinforces NATO’s ability to act collectively, ensuring that its voice as a trusted partner remains strong in the alliance.

Conclusion

AI adoption will shape the future of defence, and its success will depend on how well allies move together. For NATO and DND/CAF, the opportunity is not simply to acquire new technologies, but to

integrate them in ways that build trust, reinforce interoperability, and sustain cohesion across the alliance. Governance and procurement are not obstacles to be overcome; they are the levers that make adoption rapid, ethical, and enduring.

The stakes are clear in DND/CAF's own modernization agenda. Delivering on that vision will require turning principles into practice across every program, ensuring ethical AI principles and AI governance mechanisms are implemented across the organization. New platforms such as the River-class destroyers and the F-35s will generate vast volumes of operational data, creating both opportunities and demand for AI-enabled analysis.³⁴ NORAD modernization, with its cloud-based command and control capabilities, is already demonstrating how AI can compress decision cycles, provide commanders with real-time courses of action, and strengthen the shared defence of North America.³⁵ These initiatives underscore a central truth, that interoperability is not optional; it is the foundation of continental and allied security.

Meeting this moment will require sustained investment in three areas.³⁶ First, shared standards that make AI tools trusted across borders, so that a Canadian system can be adopted seamlessly by an American or European commander in the field. Second, open and flexible procurement practices that allow new algorithms, sensors, and software to be integrated without locking into closed architectures. Third, resilient supply chains that ensure Canada and its allies have secure access to the chips, minerals, and cloud infrastructure that make digital systems possible.

For Canada, this means embedding interoperability across acquisitions, leveraging its reputation for responsible AI governance, and working closely with allies to align certification and assurance frameworks. It also means nurturing domestic strengths, Canada's AI research ecosystem, its supply of critical minerals, and its defence innovation programs—so that national contributions are both distinctive and indispensable to the alliance. By combining resilience at home with collaboration abroad, DND/CAF can ensure that new capabilities are not only technically advanced but also strategically relevant, trusted, and usable across NATO.

Looking ahead to 2030, DND/CAF's ambition to be an AI-enabled force will only be realized if every decision related to procurement, governance, training, and investment are shaped with interoperability in mind. Success will not be measured by how many AI systems DND/CAF fields on its own, but by how effectively those systems integrate into the collective capabilities of the alliance.

By aligning its 2030 ambition with allied frameworks, DND/CAF not only secures its own AI-enabled future but also strengthens the cohesion that ensures NATO remains prepared for the challenges of the digital battlespace. In doing so, DND/CAF helps preserve the alliance's greatest strategic advantage—the ability to act collectively, with trust and speed, in defence of democracy.

Notes

- 1 Karen Hui, "Taiwan, Canada, and the Global Semiconductor Race," *Asia Pacific Foundation of Canada*, February 10th, 2025, Originally found at: <https://www.asiapacific.ca/publication/taiwan-canada-and-global-semiconductor-race>.
- 2 Koc Cagan, Ian King, and Jillian Deutsch, "ASML, Europe's Most Valuable Tech Firm, Is at the Heart of the US-China Chip War," *Bloomberg*, April 26th, 2023, Originally found at: <https://www.bloomberg.com/news/articles/2023-04-26/asml-europe-s-most-valuable-tech-firm-to-define-us-china-chip-war>.
- 3 Janet Egan, "Global Compute and National Security: Strengthening American AI Leadership Through Proactive Partnerships," *Center for a New American Security*, July 29th, 2025, Originally found at: <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/AE-Report-Global-ComputeFINALv2.pdf>.
- 4 Gracelin Baskaran and Meredith Schwartz, "The Consequences of China's New Rare-Earths Export Restrictions," *Center for Strategic & International Studies*, April 14th, 2025, Originally found at: <https://www.csis.org/analysis/consequences-chinas-new-rare-earths-export-restrictions>.
- 5 Peter Flory, "EIES Insights – NATO Summit," *Secure Energy Europe*, July 7th, 2025, Originally found at: <https://www.secureenergyeurope.org/eies-insights-nato-summit>.
- 6 Daniella Cheslow, "NATO Sparks an AI Gold Rush," *Politico*, June 30th, 2025, Originally found at: <https://www.politico.com/newsletters/digital-future-daily/2025/06/30/nato-sparks-an-ai-gold-rush-00433756>.
- 7 Prime Minister of Canada, "Strengthening Transatlantic Partnerships and Securing Canada's AI Advantage," Government of Canada, February 12th, 2025, Originally found at: <https://www.pm.gc.ca/en/news/news-releases/2025/02/12/strengthening-transatlantic-partnerships-and-securing-canadas-ai>; Innovation, Science and Economic Development Canada, *Canadian Sovereign AI Compute Strategy*, Government of Canada, May 6th, 2025, <https://ised-isde.canada.ca/site/ised/en/canadian-sovereign-ai-compute-strategy>.
- 8 Natural Resources Canada, "Rare earth elements facts." Government of Canada, September 19th, 2025, Originally found at: <https://natural-resources.canada.ca/minerals-mining/mining-data-statistics-analysis/minerals-metals-facts/rare-earth-elements-facts>.
- 9 Joe Walsh, "Pentagon Scraps Microsoft's \$10 Billion Cloud Computing Deal After Lawsuit from Amazon," *Forbes*, July 6th, 2021, Originally found at: <https://www.forbes.com/sites/joewalsh/2021/07/06/pentagon-scraps-microsofts-10-billion-cloud-computing-deal-after-lawsuit-from-amazon/>.
- 10 U.S. Department of War, "Department of Defense Announces Joint Warfighting Cloud Capability Procurement," December 7th, 2022, Originally found at: <https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/>.
- 11 Kateryna Bondar, "Unleashing U.S. Military Drone Dominance: What the United States Can Learn from Ukraine," *Center for Strategic & International Studies*, July 18th, 2025, Originally found at: <https://www.csis.org/analysis/unleashing-us-military-drone-dominance-what-united-states-can-learn-ukraine>.
- 12 Jacob Stokes, "Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition," *Center for a New American Security*, February 1st, 2024, Originally found at: <https://www.cnas.org/publications/congressional-testimony/military-artificial-intelligence-the-peoples-liberation-army-and-u-s-china-strategic-competition>.

- 13 House of Commons Standing Committee on National Defence, *A Time for Change: Reforming Defence Procurement in Canada*, June 2024, Originally found at: <https://www.ourcommons.ca/documentviewer/en/44-1/NDDN/report-12/page-126>.
- 14 Department of National Defence, "Innovation for Defence Excellence and Security (IDEaS)," Government of Canada, July 22nd, 2025, Originally found at: <https://www.canada.ca/en/department-national-defence/programs/defence-ideas.html>.
- 15 Derek Dobson, "Modernizing the Defence Procurement Ecosystem," LinkedIn, April 25, 2023, Originally found at: <https://www.linkedin.com/pulse/modernizing-defence-procurement-ecosystem-canada-derek-dobson->.
- 16 Matt Kosinski and Mark Scapicchio, "The EU AI Act: What You Need to Know," IBM, September 20th, 2024, Originally found at: <https://www.ibm.com/think/topics/eu-ai-act>.
- 17 Ian Reynolds and Yasir Atalan, "Calibrating NATO's Vision of AI-Enabled Decision Support," *Center for Strategic and International Studies*, July 8th 2024, Originally found at: <https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-support>.
- 18 European Parliamentary Research Service, "US approach to artificial intelligence," European Parliament, 2024, Originally found at: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATAG\(2024\)757605_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATAG(2024)757605_EN.pdf).
- 19 Innovation, Science and Economic Development Canada, *Artificial Intelligence and Data Act (AIDA) – Companion Document*, Government of Canada, January 31st, 2025, Originally found at: <https://isde-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>.
- 20 Zoe Stanley-Lockman and Edward Hunter Christie, "An Artificial Intelligence Strategy for NATO," October 25th, 2021, Originally found at: <https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html>.
- 21 NATO, "NATO's Data and Artificial Intelligence Review Board," October 17th, 2022, Originally found at: https://www.nato.int/cps/en/natohq/official_texts_208374.htm; NATO, "DIANA | Accelerator," 2025 Originally found at: <https://www.diana.nato.int/accelerator-programme.html>.
- 22 Steadfast Duel 2025 used the Project Maven Smart System, which uses large language models and machine learning to enhance intelligence fusion and accelerate decision-making. See: NATO Communications and Information Agency, "NCIA enables Steadfast Duel 25, NATO's largest computer-assisted command post exercise," NATO, October 29 2025. Originally found at: <https://www.ncia.nato.int/newsroom/news/ncia-enables-steadfast-duel-25-natos-largest-computer-assisted-command-post-exercise>.
- 23 Zoe Stanley-Lockman, "Responsible and Ethical Military AI," *Center for Security and Emerging Technology*, August 2021, Originally found at: <https://cset.georgetown.edu/publication/responsible-and-ethical-military-ai/>.
- 24 Cybersecurity and Infrastructure Security Agency, "Joint Guidance on Deploying AI Systems Securely," Department of Homeland Security, April 15th, 2024, Originally found at: <https://www.cisa.gov/news-events/alerts/2024/04/15/joint-guidance-deploying-ai-systems-securely>.
- 25 Treasury Board of Canada Secretariat, *Directive on Automated Decision-Making*, Government of Canada, June 24, 2025, Originally found at: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>; Department of National Defence and Canadian Armed Forces, *Artificial Intelligence Strategy*, Government of Canada, March 3rd, 2024, Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/dndcaf-ai-strategy.pdf>.
- 26 Daniel Fata, "NATO's Evolving Role in Developing AI Policy," *Center for Strategic and International Studies*, November 8, 2022, Originally found at: <https://www.csis.org/analysis/natos-evolving-role-developing-ai-policy?>.
- 27 Canadian Centre for Cyber Security, "Top 10 artificial intelligence security actions: A primer - ITSAP10.049," March 2026, Originally found at: <https://www.cyber.gc.ca/en/guidance/top-10-artificial-intelligence-security-actions-primer-itsap10049>.
- 28 Department of National Defence and Canadian Armed Forces, *Artificial Intelligence Strategy*, Government of Canada, 2024, Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/dndcaf-ai-strategy.pdf>.
- 29 Alex McPhail, and Alexander Rudolph, and Phillippe Lagassé, *Defence Agile Procurement: Insights and Analysis (DAPIA) Report*, *EXA Consulting Group*, July 10th, 2025, Originally found at: <https://static1.square-space.com/static/5cd08376797f742115eaa7cc/t/68af61b380a0f3571c695ae9/1756324275338/Final+Report++Defence+Agile+Procurement+Insights+and+Analysis.pdf>.
- 30 UK Ministry of Defence, "Integrated Procurement Model: Driving pace in the delivery of Military Capability," February 28 2024, Originally found at: <https://www.gov.uk/government/publications/integrated-procurement-model-driving-pace-in-the-delivery-of-military-capability/integrated-procurement-model-driving-pace-in-the-delivery-of-military-capability>.
- 31 Department of National Defence and Canadian Armed Forces, *Artificial Intelligence Strategy*, Government of Canada, March 3rd, 2024, Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/dndcaf-ai-strategy.pdf>.
- 32 Alexander Salt, "Reflections on Artificial Intelligence and Canadian Defence," *Canadian Global Affairs Institute*, August 2025, Originally found at: https://www.cgai.ca/th_pp_reflections_on_artificial_intelligence_and_canadian_defence.
- 33 Joshua Kurlantzick, "Assessing China's Digital Silk Road," *Council on Foreign Relations*, December 18th, 2020, Originally found at: <https://www.cfr.org/blog/assessing-chinas-digital-silk-road-transformative-approach-technology-financing-or-danger>.
- 34 Alexander Salt, "Reflections on Artificial Intelligence and Canadian Defence," *Canadian Global Affairs Institute*, August 2025, Originally found at: https://www.cgai.ca/th_pp_reflections_on_artificial_intelligence_and_canadian_defence.
- 35 Department of National Defence, "Canadian Air Defence Sector Introduces New Cloud-Based Command and Control System," Government of Canada, January 26th, 2024, Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/rcat/2024/01/canadian-air-defence-sector-introduces-new-cloud-based-command-and-control-system.html>.
- 36 Ian Bremmer and Mustafa Suleyman, "The AI Power Paradox: Can States Learn to Govern Artificial Intelligence—Before It's Too Late?" *Foreign Affairs*, August 16th, 2023, Originally found at: <https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox>.



Tactical Air Control Party (TACP) member inserts coordinates for the next air strike taken during EX MAPLE STRIKE on June 25, 2026 at Jimmy Lake, Alberta.

Photo: Corporal Connie Valin, Canadian Armed Forces photo

Navigation by Sextant & Astrocompass: A CAF Approach for AI Adoption¹

COLONEL ADAM MOORE AND MATTHEW DA MOTA

Colonel Adam Moore was commissioned into Princess Patricia's Canadian Light Infantry and has served as an infantry officer in the Canadian Armed Forces since 1996. Colonel Moore's career includes a range of command and staff roles, notably as Commanding Officer of Third Battalion, PPCLI, from 2018 to 2020. He has deployed internationally four times, including to Bosnia-Herzegovina, Afghanistan, and Iraq, as well as on five domestic operations. A graduate of the Royal Military College of Canada, he holds a Bachelor of Engineering and a Master of Defence Studies. He has completed professional military education at the Canadian Army Command and Staff College and the Canadian Forces College. Colonel Moore has been a Fellow at the Centre for International and Defence Policy at Queen's University since 2024-2025 and is currently the Chief of Staff of the 4th Canadian Division.

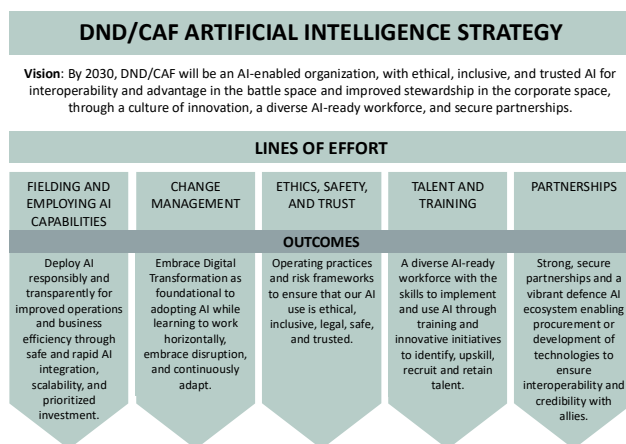
Matthew da Mota is Research Director, Emerging Technology and National Security at the Canadian Shield Institute for Public Policy. His work explores how emerging technologies and shifting geopolitical dynamics reshape security, governance, knowledge, and sovereignty—with a focus on the implications of AI and digital infrastructure. Matthew previously worked on international AI governance and security at the Centre for International Governance Innovation. His Ph.D. research examined the relationship between historical narrative, written evidence, and political power. Matthew is also a fellow in Technology and Security at Queen's University's Centre for International and Defence Policy, and he serves on multiple standardization technical committees.

Acknowledgement: This paper is firmly focused on AI disruption in military decision-making processes. Other AI implications in the military, such as the integration of AI with robotics, are important but separate considerations that are not addressed in this paper. Readers should treat this paper as a snapshot of AI development as of mid-2025, which may have changed in key areas.

Canada's largest national security institutions, the joint Department of National Defence and Canadian Armed Forces (DND/CAF), face an institutional imperative: become AI-enabled by 2030 or risk strategic irrelevance. Yet AI integration introduces hazards—cognitive deskilling, accountability dilution, automation bias—that remain poorly understood in high-stakes military environments. The rapidly evolving global threat environment—characterized by strategic competition, regional instabilities, and non-state disruption—intensifies this challenge, demanding rapid adoption while effectively managing operational risks.^{2,3}

The DND/CAF Artificial Intelligence Strategy (DCAIS) articulates this ambition through five interrelated lines of effort (LoEs): (1) Fielding and Employing AI Capabilities, (2) Change Management, (3) Ethics Safety and Trust, (4) Talent and Training, and (5) Partnerships.⁴ While the 2030 timeline appears distant, it represents an immediate challenge in defence procurement terms, requiring organizational and cultural transformation that bridges technical expertise with institutional knowledge.⁵

Figure 1: DND/CAF AI Strategy's Lines of Effort⁶



This paper explores AI integration using the metaphor of navigating by sextant and astrocompass—emphasizing the importance of grounding innovation in established professional frameworks. Drawing on the CAF's cognitive hierarchy, the authority, responsibility, accountability (ARA) model, and institutional risk assessment language, the analysis treats AI not as a solution but as a suite of powerful yet incomplete tools that must remain subordinate to professional judgment, institutional logic, and the realities of military decision-making.

The paper argues that meaningful AI adoption requires deliberate, risk-informed action and dual fluency: the ability to operate effectively in both AI-enabled and technology-denied environments. Using the DCAIS as a framing document for understanding DND/CAF's plans for AI integration, it examines how established CAF decision-making frameworks can guide responsible integration, concluding with policy recommendations to support informed advancement within existing institutional logic.

Guiding Stars for AI Integration

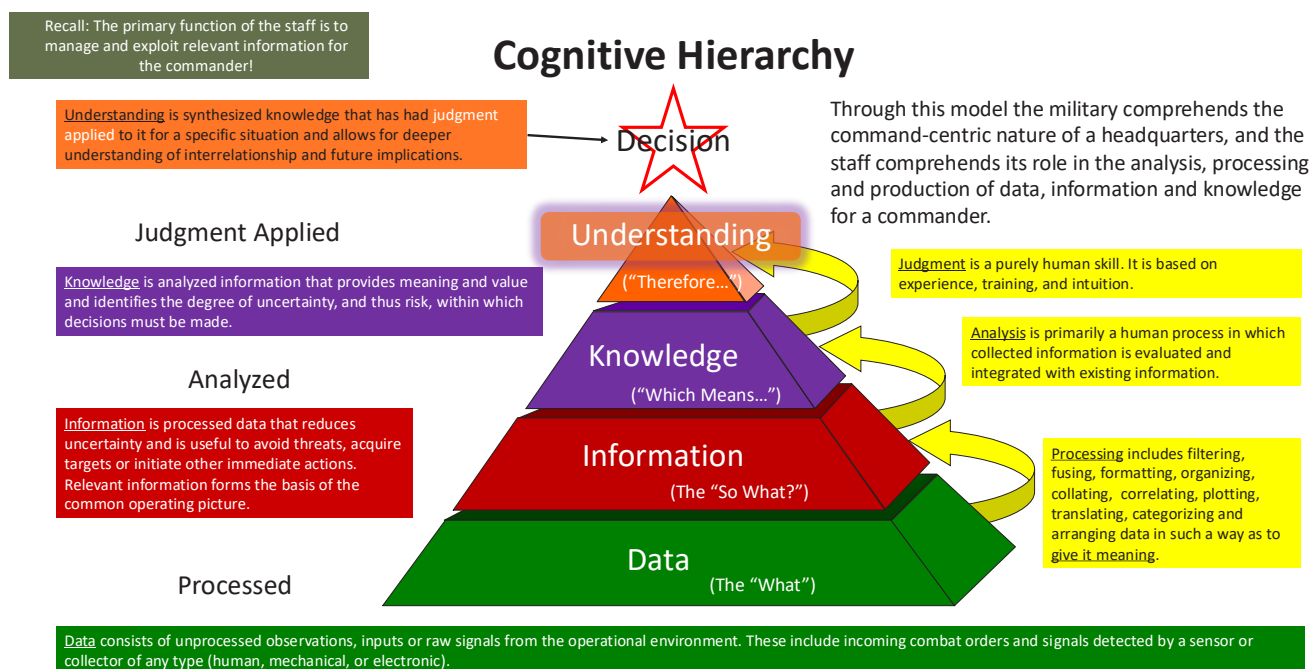
Like celestial navigation on the ocean, AI integration within DND/CAF requires fixed reference points to maintain course and bearing. The sextant measures angles between known celestial bodies and the horizon; the astrocompass helps to determine true north. For AI adoption within the defence enterprise, three institutional constants should serve as guiding stars: the CAF cognitive hierarchy model; the ARA framework; and the structuring logic of risk that runs through all levels of DND/CAF. While not AI-specific, these frameworks govern how CAF members engage with and make use of information across all contexts—making them essential for understanding how AI, a fundamentally information-based suite of technologies, will integrate within existing and emerging DND/CAF systems.

As AI systems begin to influence decision environments across DND/CAF, these foundational decision-making and knowledge production models continue to serve as essential navigation aids. They ensure that technological innovation remains rooted in proven institutional logic and professional judgment.

Cognitive Hierarchy

The CAF's cognitive hierarchy model (Figure 2) offers a structured framework for transforming raw data into actionable understanding. The model is based on four ascending stages: data, information, knowledge, and understanding, each representing a qualitative leap in cognitive processing. While AI can augment this hierarchy, it cannot replace the foundational role of human judgment.

Figure 2: The Cognitive Hierarchy⁷



AI tools can significantly enhance this hierarchy through assisting in cleaning and tagging data, automating cross-cueing,⁸ and extracting relevant information to support data collection and processing. More advanced systems may support analysis to generate knowledge and even offer structured inputs that inform human judgment in pursuit of shared understanding. Nonetheless, judgment remains a distinctly human function shaped by experience, intuition, and ethical discernment. In a command-centric environment, where staff serve to manage and interpret relevant information on behalf of commanders, the cognitive hierarchy reinforces the mission command philosophy of the CAF, emphasizing decentralized decision-making and trust. Any AI-enabled decision support must therefore be subordinate to, and anchored in, expert and ethical human judgment.

The ARA framework in DND/CAF

The triad of accountability, responsibility, and authority is the decision-making backbone of DND/CAF, applying across both military and civilian components of the joint institution.⁹ Just as the relationship between true north and celestial bodies remains fixed, these concepts maintain constant relative positions even as contexts change.

Accountability, the obligation to answer for responsibilities carried out, is non-delegable, residing within the legal and institutional structures of one's home organization. *Responsibility* is the obligation to perform assigned duties, which may be delegated but never

wholly relinquished. *Authority* denotes the right to make decisions, to give formal orders or instructions, and to direct actions—whether in a command, administrative, or functional capacity.

ARA takes on a unique character in the appointment to command, where each element is indivisibly vested in a single person exercising legal authority to direct military operations. Command appointments carry the exclusive legal and moral burden of decision-making; the commander holds personal accountability for mission success or failure. All other participants—staff members, headquarters personnel, supporting organizations—derive their authority through delegation bounded by parameters established by the accountability holder.

This hierarchical structure ensures unity of command and clarity of accountability, reinforced by DND/CAF's dual structure, where CAF members and DND employees operate under separate chains with distinct legal authorities, where legal accountability rests with one's institution, thereby ensuring clear delineation of responsibility.¹⁰

AI systems will primarily interface at the staff and command post levels, where information is processed, fused, and converted into actionable insights. These layers manage inputs, conduct analysis, and generate recommendations. The introduction of AI raises important questions—especially in the higher tiers of the CAF's cognitive hierarchy—about the potential dilution or displacement of human judgment. These questions are taken up and explored in greater depth in the section "Hazards of AI Integration."

Risk as a Structuring Logic in DND/CAF

Risk is a fundamental logic across operational and institutional domains of DND/CAF. Two complementary frameworks guide its application: *Risk Management for CF Operations* provides the doctrinal underpinning for military risk in tactical and operational contexts, while the *Defence Enterprise Risk Management Guideline* governs enterprise-level considerations.¹¹ Though distinct in emphasis, both frameworks reinforce a common logic: risk is not simply a calculation—it is a discipline of professional judgment anchored in context, authority, and responsibility.

In the military, commanders use risk to navigate decision-making. Staff play a critical advisory role in identifying hazards, proposing mitigations, and framing risk trade-offs. Risk is characterized not only by *probability* and *severity*, but also by factors such as *urgency* and *controllability*. Risk can only be accepted by individuals who both possess delegated authority over the proposed mitigations and operate within their defined residual risk acceptance authority.

Risk accountability in DND/CAF is personal, not procedural, representing more than a bureaucratic safeguard. Processes cannot be held accountable; only people can. The enduring principle is that *accountability attaches to the individual who accepts the risk*. This raises important institutional questions: When risk accepted in the past materializes in the present, who bears accountability? Is that accountability transferred to successors and, if so, are those individuals fully aware of the risks they now hold?

DND/CAF would benefit from treating risk as a shared currency of communication, promoting common language across operational and institutional functions to enhance coherence and decision clarity. Not all members of DND/CAF use risk frameworks in this way, but consistent risk language use could help to standardize and align risk awareness around AI across contexts.¹² The greater challenge lies in recognizing that seemingly discrete, low-stakes risks can accumulate across systems and, through compounding effects, create aggregate risk profiles that exceed the sum of their parts, remaining invisible to any single risk manager but capable of placing the entire enterprise in jeopardy.¹³

These guiding stars help orient the institution in uncharted space, but they do not eliminate uncertainty. With these reference points fixed, attention can now turn toward the hazards ahead—not along a predetermined route, but with the navigational discipline that sextants and astrocompasses once demanded: observation, calculation and orientation before movement.¹⁴

Hazards of AI Integration

As in any journey, navigating AI integration in DND/CAF has a roughly charted destination as defined in the DCAIS, but the actual process of navigation must be agile and adaptable to known and emerging risks, able to shift course as needed but still find the way.

“It is essential to recognize that AI—particularly generative models—does not understand anything in the human sense.”

Firstly, it is essential to recognize that AI—particularly generative models—does not understand anything in the human sense. These systems operate as highly sophisticated pattern recognition engines, capable of generating plausible outputs based on statistical regularities in training data.¹⁵ While they can achieve superhuman accuracy in well-defined contexts, their reliability degrades sharply when confronted with edge cases—so-called *1% problems*—where atypical inputs fall outside learned patterns.¹⁶ This limitation does not constitute a risk in itself, but becomes a factor that must be considered when assessing the suitability of AI tools for specific tasks or domains.

The following hazards are grouped by cognitive and institutional dynamics rather than technical domains, reflecting how AI integration will reshape decision-making processes across the defence enterprise.

Cognitive Offloading & Deskilling and the Erosion of Judgment

AI systems promise to reduce cognitive load by automating data-intensive tasks, theoretically allowing personnel to shift from production to evaluation mode—accelerating movement up the cognitive hierarchy toward understanding and judgment. This cognitive offloading mirrors familiar practices where humans delegate mental tasks to algorithmic systems.¹⁷

However, habitual reliance introduces a critical trade-off. When delegation becomes dependence, cognitive deskilling occurs—the gradual loss of independent reasoning ability—distinct from offloading in that it risks long-term erosion of judgment.¹⁸ Persistent reliance on AI-enabled tools may erode individual and institutional judgment by denying exposure to the subjective, experience-based activities at lower levels of the cognitive hierarchy. The result may be technically proficient leaders who lack the intuitive judgment required to navigate ambiguous or degraded environments.

In military contexts, this means personnel need to both excel at interpreting AI-generated intelligence summaries and have the experience necessary to recognize when source data has been compromised or patterns manipulated. But in a future where AI systems handle most processing and synthesis tasks, what happens when the human in the loop lacks the personal experience to verify the output? What happens when the volume of data exceeds a human operator's capacity for meaningful review? Should

the CAF deliberately retain non-AI-enabled, human-generated products—however inferior—to train personnel in independent judgment? And while such delegation may be acceptable in benign contexts, how should responsibility be assigned when an AI-enabled decision contributes to the unlawful application of lethal force: does accountability rest with the developer, the contracted programmer? Who gets charged with the war crime? A decision brief in 2035 might involve AI-generated outputs presented with high confidence, but if that data has been poisoned or the model sabotaged, and the attending human lacks depth of knowledge to challenge it, the outcome may not just be flawed—it may be undetectably wrong. In such environments, trust in automation must be matched by an equally strong commitment to developing judgment-capable leaders.

AI adoption in defence does not reduce the burden of professional development—it increases it. To operate in both technologically degraded and technologically enhanced environments, CAF personnel will require dual fluency in human-centred judgment and machine-assisted analysis. Like navigating the seas, the ability to recognize when something is off course depends less on upgrading the instruments than on remembering how to use them.¹⁹

Automation Bias and Algorithm Aversion

AI-enabled decision support introduces a dual hazard: uncritical reliance on algorithmic outputs (automation bias) and outright dismissal even when statistically superior (algorithm aversion).²⁰ Both exist on a continuum, with impact particularly acute under time pressure within action-oriented institutions.

Military decision-making has long depended on intermediaries—staff officers, advisors, planning cells—who filter information and frame choices. AI support represents digital bureaucracy structured by rules and neural networks.²¹ However, commanders have always understood that staff bring implicit biases, interests, and analytical limitations. The distinctive risk with AI is algorithmically induced bias: distortions embedded in training data, model assumptions, or environmental inputs, often obscured from end users and difficult to detect. Solutions to algorithmic bias are uncertain, but a clear solution in the interim is to ensure a system of checks and balances with humans in and on the loop to verify AI outputs.

Traceability—the ability to understand how a recommendation was generated—has become a major concern in this context.²² Yet this, too, has precedent. Expert human judgment is often grounded in tacit knowledge that resists formal articulation.

Within DND/CAF, the challenge lies not in eliminating bias or aversion, but managing them through sound processes and deliberate human oversight.²³ If human oversight on AI recommendations become mere checkboxes to enable speed, decision support utility is lost.²⁴ Conversely, if skepticism leads to paralysis, the advantage of AI is never realized. Success requires clearly

defined authorities and accountabilities delineating who verifies outputs, when to pause for deeper analysis, and how to escalate when something appears wrong.

Moral Crumple Zones and the Illusion of Accountability

The concept of *moral crumple* zones introduced by Madeline Elish refers to the human tendency to absorb blame when autonomous systems fail—regardless of actual control or authorship.²⁵ The person “in the loop” verifying an automated system’s outputs becomes the face of accountability, even when decision-making has been substantially delegated to an opaque and distributed system. This illusion of accountability becomes increasingly problematic as system complexity grows and explanation becomes less accessible.²⁶

Looking ahead to a 2030 AI-enabled DND/CAF, this concern shifts from theoretical to real. If future AI tools continue to function as black boxes, producing outputs without transparent or interpretable reasoning, accountability structures must be re-evaluated. Rapid AI development, increasing complexity and autonomy of systems, and potential for recursive improvement and self-modification of AI systems threaten to push these systems beyond human comprehension.²⁷ As the line between authority and responsibility blurs in increasingly automated systems, the burden of accountability remains sharply focused—often disproportionately—on the closest human.

This raises pressing questions for human-machine teaming: who is accountable when something goes wrong?²⁸ The operator, tactical commander, project manager, contracted company, or model training team? While failures may be infrequent, their severity can be significant for both affected people and institutional trust.

In practice, it is highly likely that some person will be blamed for AI-related failures, but the downstream consequences of that blame merit attention. If DND/CAF intends to remain ethically grounded while scaling AI integration, it must equip all relevant personnel not only with tools to make decisions, but with frameworks to share accountability and process moral complexity.

Institutional Ownership and Generative Intellectual Property

The 2019 *Lukits v. DND* ruling by the Federal Public Sector Labour Relations and Employment Board upheld a Royal Military College professor’s right to retain ownership of handwritten lecture notes.²⁹ While the *Lukits* ruling appropriately upheld academic freedom,³⁰ it also reveals institutional vulnerability in how the Crown asserts ownership over knowledge produced by its workforce. How well is DND/CAF positioned to manage intellectual property in an era of AI?

Generative AI tools complicate this further. Unlike handwritten lecture notes, Generative AI outputs are shaped by statistical prediction, informed by user prompts, and processed through commercial infrastructure. The resulting products—text, images, code, design concepts—may be refined by the user, but are not easily traceable in terms of authorship or custody. Treasury Board guidance for employees to consult legal services, review licensing terms, and stay informed about evolving AI law,³¹ is well-intentioned but impractical. Not all DND/CAF personnel are intellectual property specialists, and no capacity has been allocated to ensure the average DND/CAF user of AI is able to manage this burden. Responsibility for managing intellectual property risk should not be downloaded onto individual users.

Crown ownership over co-developed Generative AI outputs cannot be assumed. If data or design artifacts generated within DND/CAF are absorbed or monetized by commercial vendors through unclear licensing arrangements,³² the resulting impact could be significant. The issue is not a lack of policy but a failure to deliver clear, unambiguous direction.

A designated authority—such as the DND/CAF AI Centre—should be empowered to issue enforceable guidance on ownership, licensing, and data use across all adopted AI tools. This is an immediate requirement, not a matter for further study. Expecting military or civilian personnel to self-manage legal compliance is unreasonable, risks losing institutional control over mission-critical knowledge, and opens the door to the erosion of information integrity.

Valuation of Data: Contextual Significance and System Blindness

AI systems infer value statistically, but military planning often relies on sparse, context-specific information.³³ This becomes complex as models are trained on large volumes of unstructured, inconsistently governed data.³⁴ An operations order's intent paragraph may appear once while administrative details repeat throughout—yet AI may overvalue repetition over judgment-critical content. Without enterprise capability to signal authoritative inputs, systems cannot distinguish between delegated authority and administrative noise, substantially increasing risk.

It remains unclear whether current DND/CAF enterprise capability exists to signal that certain inputs should be treated as more authoritative than others. How does the CAF ensure a revised Chief of Defence Staff Directive or an order that changes the rules of engagement for a deployed task force registers as a meaningful shift rather than just another document? How is superseded content prevented from continuing to shape outputs simply because it appears more frequently in datasets?

Data significance is contextual and changes over time, while AI models optimize for patterns, not meaning. The same data point may be critical in one context, irrelevant in another, and misleading in a third.³⁵ DND/CAF must either develop mechanisms

that recognize and preserve shifting context over time or formalize human-in-the-loop roles specifically aimed at preserving contextual meaning within AI-enabled processes.³⁶

Pressing Forward Despite Uncertainty³⁷

DND/CAF should treat AI as a general-purpose technology requiring immediate preparation. The trajectory of AI development and its convergence with key military domains strongly suggests that it will reshape both the battlespace and the institutional environment in which DND/CAF operates. This warrants a deliberate shift toward AI-readiness: institutional, procedural, and cultural. Preparing now lays essential groundwork for confronting future disruptions from other emerging technologies, including quantum-era threats.

Sovereignty concerns should be viewed as a constraint to manage, not a barrier to overcome. The scale of infrastructure required for current and future AI models is vast and not likely to be possible for Canada to develop a “sovereign AI stack” within the short term.³⁸ Some degree of reliance on existing private and foreign cloud and data infrastructure will continue to be necessary. However, not all data or processes require maximum classification or control.³⁹ For those that do, secure sovereign data centres may already exist, or else such centres can be built. For those in the grey zone in between, DND/CAF can make use of privacy-enhancing technologies (PETs), data enclaves, and other tools to maximize sovereignty and data protection while continuing to make use of high-quality private infrastructure hosted in allied nations.⁴⁰ So long as there is clarity on what must remain sovereign and what can be responsibly externalized with safeguards, a reasonable degree of protection can be ensured.⁴¹

“If Canada intends to shape how AI is used ethically and operationally, DND/CAF must maintain credible presence in those conversations.”

Digital interoperability is now strategic. In an environment where allies rapidly integrate AI into operations, Canada must keep pace to retain influence and credibility.⁴² A country that lags risks becoming a standards taker rather than shaper. If Canada intends to shape how AI is used ethically and operationally, DND/CAF must maintain credible presence in those conversations through meaningful capability and demonstrated experimentation.

Canada's domestic AI ecosystem is a national advantage.⁴³ Academic expertise, innovation capacity, and industry already exist. The DCAIS LoE calls for the development of trust-based partnerships that serve both mission assurance and Canadian national interests.

Policy Recommendations

The following recommendations chart a deliberate course toward responsible AI integration in DND/CAF, reflecting the integrated LoEs outlined in the DCAIS and guided by enduring institutional reference points:

1. Treat AI as a general-purpose technology for planning purposes and begin structured implementation accordingly.
2. Treat the CAF Digital Campaign Plan and the DCAIS as enterprise reinvention guides, not as discrete initiatives.
3. Institutionalize risk as a shared language across operational and institutional spheres, improving the ability to track and manage aggregate risk accumulation, particularly where AI introduces distributed decision-making.
4. Develop dual capability: personnel must operate effectively in both AI-enabled and technology-denied environments.
5. Distinguish sovereignty requirements pragmatically between data/processes requiring full government control and those enabling secure externalization.
6. Leverage interoperability as a strategic influence vector, not just technical compatibility, helping Canada shape emerging defence AI standards.
7. Integrate DND/CAF AI adoption within full-ecosystem planning, ensuring defence contexts inform broader governmental AI governance.

Conclusion

These guiding stars—cognitive hierarchy, the ARA framework, and the structuring logic of risk—shine more brightly in an AI-enabled environment, not despite technological transformation, but precisely because of it. In a doctrinal Ends-Ways-Means framing, AI fundamentally shifts the *means* by which decisions are made through data-enabled models, probabilistic reasoning, and systems capable of exponentially more rapid adaptation. These new means demand new *ways*—revised processes, doctrinal adjustments, upskilling and digital literacy enabling personnel to interrogate the reliability, traceability, and mission relevance of AI-generated outputs. The *ends*—effective decision-making within volatile, uncertain, complex, and ambiguous environments—remain consistent.

Canada's strategic advantage lies in doing AI adoption well—in a way that is aligned with Canadian values and sensitive to national needs. Canada's legitimacy stems from world-class research, professional military training, and strong partnerships, but fundamentally from respect for rights and values. Channeling these principles into AI frameworks creates superior tools and more desirable outcomes.

The metaphorical sextant and astrocompass remind us that while tools evolve, navigation discipline endures. Canada's path forward demands deliberate progress guided by institutional wisdom and democratic values—navigation principles that chart a course through uncertain waters while maintaining true bearing.

Notes

- 1 Developed by Col. Adam Moore during a defence sabbatical (August 2024–May 2025) while a Visiting Fellow at Queen's University. A longer version appeared with the Centre for International and Defence Policy (CIDP), Queen's University, 2025.
- 2 Canadian Security Intelligence Service, *CSIS Public Report 2023*, 2024. Originally found at: <https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2023.html>; Department of National Defence, *Pan-Domain Command & Control Concept Paper*, 2024. Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/pan-domain-command-control.html>. See Jamali, Nahlah, "DeepSeek AI Shakes American Swagger and Upends Assumptions," BBC News, January 28, 2025. Originally found at: <https://www.bbc.com/news/articles/cd643wx888gq>.
- 3 See Lloyd, Ron, "Public Service Culture, Risk Management and Governance: The Prerequisite of Effective Strategic Governance to Realizing Our Digital Ambition," Canadian Global Affairs Institute, 2024. Originally found at: https://www.cgai.ca/public_service_culture_risk_management_and_governance_the_prerequisite_of_effective_strategic_governance_to_realizing_our_digital_ambition.
- 4 Department of National Defence (DND), *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy (DCAIS)*, 2024. Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/dnd-caf-artificial-intelligence-strategy.html>.
- 5 Inspired by the Canada School of Public Service's curation of Stewart-Weeks, M., and Cooper, S. (2019) "We're Missing the Point of Digital Government - Here's Why. Opinion: Digital Experts Understand Tech - but Do They Understand Government?" *Apolitical*, August 13. Originally found at: <https://apolitical.co/solution-articles/en/why-were-missing-the-point-in-digital-government>.
- 6 Reproduction of an image from DND, *The DCAIS*, 2024, pg. 1.
- 7 Author-adapted representation inspired by the U.S. Army's Mission Command Training Program. This representation aligns with the CAF's Cognitive Hierarchy explanations in DND, *B-GI-300-003/FP-001 Command in Land Operations*, 2007; DND, *B-GI-331-001/FP-001 Command Support in Land Operations*, 2008; and DND, *Canadian Forces Joint Publication 01: Canadian Military Doctrine*, 2nd ed. 2024. The source image can be found in U.S. Army, *FY 24 Mission Command Training Program Key Observations*. Center for Army Lessons Learned, 2025. Figure 2-1, "Cognitive Hierarchy," 10. Originally found at: <https://api.army.mil/e2/c/downloads/2025/02/24/aea2698e/25-04-946-fy-24-mctp-key-observations-feb-25.pdf>.
- 8 Cross-cueing "entails one sensor passing detection, geolocation and targeting information to another sensor, which improves efficiency." DND, *Royal Canadian Air Force Doctrine: Intelligence, Surveillance and Reconnaissance*, 2017, p. 2-2.

- 9 DND, *Accountabilities, Responsibilities, and Authorities*, Corporate Secretariat, 2024.
- 10 DND, *Canadian Forces Joint Publication 01: Canadian Military Doctrine*, 2nd ed. 2024.
- 11 DND, *Risk Management for CF Operations*, 2007. DND, *Defence Enterprise Risk Management Guideline*, 2018.
- 12 The National Institute of Standards and Technology, *AI Risk Management Framework*, NIST AI 100-1. 2023. Originally found at: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>, offers useful guidance for institutional risk analysis.
- 13 See Lloyd (note 3).
- 14 The Treasury Board's Algorithmic Impact Assessment (AIA) tool emphasizes impact severity over probability, misaligning with defence risk models that require both factors: Since many DND/CAF applications involve minimal Canadian personal data, strict AIA adherence may unnecessarily delay high-utility operational applications. A tailored assessment model or controlled exceptions may better serve defence requirements while maintaining ethical oversight. Treasury Board Secretariat, "AI Strategy for the Federal Public Service 2025-2027," March 4, 2025. Originally found at: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/gc-ai-strategy-overview.html>.
- 15 Vallor, Shannon, *The AI Mirror: How to Reclaim Our Humanity in an Age of Machine Thinking*, Oxford University Press, 2024.
- 16 Max Lamparth and Jacquelyn Schneider, "Why the Military Can't Trust AI," *Foreign Affairs*, 2024. Originally found at: <https://www.foreignaffairs.com/united-states/why-military-cant-trust-ai>. Karine Perset and Sara Fialho Esposito, *How Are AI Developers Managing Risks? Insights from Responses to the Reporting Framework of the Hiroshima AI Process Code of Conduct*, OECD Artificial Intelligence Papers (Paris: OECD Publishing, 2025), 33. Originally found at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/how-are-ai-developers-managing-risks_fbaeb3ad/658c2ad6-en.pdf.
- 17 Grinschgl, Sandra, Frank Papenmeier, and Hauke S. Meyerhoff, "Consequences of Cognitive Offloading: Boosting Performance but Diminishing Memory," *Quarterly Journal of Experimental Psychology* 74, no. 9 (2021): 1477-96. Originally found at: <https://doi.org/10.1177/17470218211008060>.
- 18 Thiele, Leslie Paul, "Rise of the Centaurs: The Internet of Things Intelligence Augmentation," in *Towards an International Political Economy of Artificial Intelligence*, edited by Tugrul Keskin and Ryan David Kiggins, 39-61. Springer International Publishing, 2021. Originally found at: <https://link.springer.com/book/10.1007/978-3-030-74420-5>. Cognitive deskilling is closely related to the concept of moral deskilling. For an in-depth discussion of the latter, see Vallor, Shannon, "Moral Deskilling and Upskilling in a New Machine Age: Reflections on the Ambiguous Future of Character," *Philosophy and Technology* 28, no. 1 (2015): 107-24.
- 19 Further research is needed on AI's impact on tacit knowledge within the CAF. Since AI systems operate on structured, explicit data while military expertise relies heavily on unrecorded, experiential knowledge, overreliance risks eroding expert judgment if systems displace rather than augment human experience. For more on the devaluation of professional judgment see Nichols, Tom M., *The Death of Expertise: The Campaign against Established Knowledge and Why It Matters*, Oxford University Press, 2017.
- 20 The term "automation bias" here draws directly from Nadibaidze, Anna, Ingvild Bode, and Guangyu Zhang, *AI in Military Decision Support Systems: A Review of Developments and Debates*, 2024. Originally found at: https://findresearcher.sdu.dk/ws/portalfiles/portal/275893410/AI_DSS_report_WEB.pdf; "algorithm aversion," is more loosely defined according to Jussupow, Ekaterina, Izak Benbasat, and Armin Heinzl, "Why Are We Averse Towards Algorithms? A Comprehensive Literature Review on Algorithm Aversion," in *ECIS 2020 Proceedings*, Virtual: Association for Information Systems, 2020. Originally found at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1167&context=ecis2020_rp.
- 21 Stimulated by a logical extrapolation from the idea that "if the economy is an information processing system, does that mean that every corporation is an artificial intelligence?"; Davies, Dan, *The Unaccountability Machine: Why Big Systems Make Terrible Decisions—and How the World Lost Its Mind*, Profile Books, 2024, p. 63.
- 22 Taddeo, Mariarosaria, David McNeish, Alexander Blanchard, and Elizabeth Edgar, "Ethical Principles for Artificial Intelligence in National Defence," *Philosophy & Technology* 34, no. 4 (2021): 1707-29. Originally found at: <https://doi.org/10.1007/s13347-021-00482-3>, p. 1717-1718; DND, The DCAIS, 2024, p. 18.
- 23 Davies, *The Unaccountability Machine*, 78-79.
- 24 Nadibaidze, Bode, and Zhang, *AI in Military Decision Support Systems*, 33.
- 25 Elish, Madeleine Clare, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction," *Engaging Science, Technology, and Society* 5 (March 23, 2019): 40-60. Originally found at: <https://doi.org/10.17351/ests2019.260>.
- 26 Devitt, S. Kate, "Bad, Mad, and Cooked: Moral Responsibility for Civilian Harms in Human-AI Military Teams," in *Responsible Use of AI in Military Systems*, edited by Jan Maarten Schraagen, 248-77, Chapman and Hall/CRC, 2024. Originally found at: <https://doi.org/10.1201/9781003410379-16>.
- 27 Mustafa Suleyman has warned about these risks (Suleyman, Mustafa, and Michael Bhaskar, *The Coming Wave: Technology, Power, and the Twenty-First Century's Greatest Dilemma*, Crown, 2023.), and Dan Davies makes a similar observation: when explanation breaks down, parsing source code offers no real insight into cause or consequence (Davies, *The Unaccountability Machine*, 76.)
- 28 See Elish "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction," 54; Nadibaidze, Bode, and Zhang, *AI in Military Decision Support Systems*, 40-41.
- 29 *Lukits v. Treasury Board (Department of National Defence)*, 2019 FPSLREB 20 (CanLII), *Federal Public Sector Labour Relations and Employment Board*, March 13, 2019. Originally found at: <https://decisions.fpslreb-crtespf.gc.ca/fpslreb-crtespf/d/en/item/407680/index.do>.
- 30 Treasury Board Secretariat, "University Teaching (UT): Agreement Between the Treasury Board and the Canadian Military Colleges Faculty Association." Originally found at: <https://www.tbs-sct.canada.ca/agreements-conventions/view-visualiser-eng.aspx?id=27#toc2112221127>.
- 31 Treasury Board Secretariat, "Guide on the Use of Generative Artificial Intelligence," May 30, 2024. Originally found at: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html>.
- 32 See, for example, McManus, Sean, "Why Employees Smuggle AI into Work," *BBC News*, February 3, 2025. Originally found at: <https://www.bbc.com/news/articles/cn7rx05xq2go>.
- 33 Goldfarb, Avi, and Jon R. Lindsay, "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," *International Security* 46, no. 3 (2022): 7-50. Originally found at: https://doi.org/10.1162/isec_a_00425.
- 34 Goldfarb, Avi, and Jon R. Lindsay, "Artificial Intelligence in War: Human Judgment as an Organizational Strength and a Strategic Liability," *Foreign Policy at Brookings*, 2020. Originally found at: https://www.brookings.edu/wp-content/uploads/2020/11/fp_20201130_artificial_intelligence_in_war.pdf.
- 35 Vallor, *The AI Mirror*, 26-27; Nadibaidze, Bode, and Zhang, *AI in Military Decision Support Systems*, 36-38.
- 36 On contextual data in AI deployment, see da Mota, M., "Toward an AI Policy Framework for Research Institutions," Centre for International Governance Innovation, 2024. Originally found at: <https://www.cigionline.org/publications/toward-an-ai-policy-framework-for-research-institutions/>.
- 37 Author's reflection from knowledge gained during defence sabbatical; no public or academic sources cited.
- 38 For more on the debates over a Canadian "sovereign stack" for AI, see emerging work from the Canadian AI Sovereignty and Innovation Cluster. Originally found at: <https://caisic.ca/>; the Council of Canadian Innovators <https://www.canadianinnovators.org/>; the Canadian AI adoption Initiative Originally found at: <https://www.aiadoption.ca/>; and Innovation, Science and Economic Development Canada, *Canadian Sovereign AI Compute Strategy*, 2025. Originally found at: <https://ised-isde.canada.ca/site/ised/en/canadian-sovereign-ai-compute-strategy>.
- 39 For a critical review of Canada's classification framework through a digital lens, see: Lloyd, Ron, "Canada's Security Classification Framework: The Biggest Impediment to Realizing Our Digital Ambition," Canadian Global Affairs Institute, 2024. Originally found at: https://www.cgai.ca/canadas_security_classification_framework_the_biggest_impediment_to_realizing_our_digital_ambition.
- 40 For more on PETs for enhancing AI sovereignty see: OECD, "Sharing Trustworthy AI Models with Privacy-Enhancing Technologies," *OECD AI Papers*, no. 38, 2025. Originally found at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/sharing-trustworthy-ai-models-with-privacy-enhancing-technologies_5df6fd05/a266160b-en.pdf.
- 41 Shared Services Canada and the Communications Security Establishment have been and continue to be building infrastructure and defining lines to enable those policies.
- 42 For example, see: NATO, "Summary of NATO's Revised Artificial Intelligence (AI) Strategy," 2024. Originally found at: https://www.nato.int/cps/en/natohq/official_texts_227237.htm.
- 43 DND, "Adopting Artificial Intelligence with Security in Mind," DDN2-V46, Canadian School of Public Service, 2024. Originally found at: <https://www.cspes-efpc.gc.ca/video/ai-security-eng.aspx>.



Members of the Canadian Armed Forces Talon Company conduct Reconnaissance (Recce) during Exercise Wolverine Shield/Strike at Camp Adazi, Latvia, March 7, 2023.

Photo: Canadian Armed Forces Imagery Technician

Authenticity as a Weapon: The Canadian Armed Forces' Advantage in AI-Enabled Information Warfare

ALI MANOUCHEHRI AND MAJOR TYLER CURRIE

Ali Manouchehri is currently a senior advisor with the DND/CAF AI Centre. Prior to joining the DSG, he served as the Manager of Data and Analytics in ADM(RS), DND.

Major Tyler Currie is the CAF AI Integration and Acceleration Officer who works at the DND/CAF AI Centre. Tyler has spent 16 years as part of the Intelligence Branch and has served on deployed operations in Afghanistan and in the international context with Joint Forces Command (JFC) Naples. Tyler holds a master's in political studies from Queen's as well as a Master of Management in Artificial Intelligence (MMAI) from the Queen's Smith School of Business.

The Department of National Defence (DND) and the Canadian Armed Forces (CAF) operate in an information environment where the first casualty of crisis is certainty.

For example, in a North American Aerospace Defense Command (NORAD) aerospace incident, while forces track and respond to an unidentified aircraft, commanders and public affairs teams may also face a parallel hazard—AI-generated manipulated audio, video, and text, arriving at machine speed.¹

What once demanded studios, budgets, and weeks, can now be produced in minutes with widely available AI services and editing apps, and can quickly reach the public.

This operational reality points to a different kind of challenge based on trust. Generative artificial intelligence accelerates the manufacture of persuasive but false content, altering what people believe in the first moments of an incident, complicating crisis response at the most dangerous time. When trust slips, orders take longer to issue and follow, coordination slows, and the risk of serious consequences rises.

Against this backdrop, Canada faces the same pressures across multiple mission sets. We operate with allies abroad, where close coordination of messages and decisions is critical to maintaining unity of effort in coalition operations. At home, the DND/CAF supports Canadians in moments of crisis—wildfires, floods, search and rescue—often under intense scrutiny, where communication must be fast, accurate, and trusted.

In the North, vast distance, harsh weather and modest infrastructure shape how information moves and how communities experience danger. In every one of these settings, the ability to authenticate an official signal, to reassure calmly in the face of misleading claims, and to stay ahead in the information fight is essential to mission success.

The argument is straightforward. Canada, together with its allies, can effectively compete with adversaries in terms of technical sophistication and computational power and even outperform them in select emerging technologies thanks to its highly skilled and multicultural workforce and its collaborative approach to working with allies. What matters is proving that our signals are ours, verifying new information before we act on it, and addressing the public early when we encounter mis- and disinformation. By making these habits standard across policy, training, procurement, and leadership, the DND/CAF sustains its credibility and operational tempo against state actors, proxy groups, and opportunistic individuals who seek to exploit information chaos for strategic advantage.

We do not need to out-code adversaries; however, it is imperative that we be able to prove that our signals are ours, to verify new information before we act on it, and to address the public early when we encounter mis- and disinformation.

The New Conditions of Deception

Generative systems learn from large collections of text, images and audio, then produce new material that fits those patterns. They do not reason like people.² Because they are built to mimic style rather than check facts, they can produce fluent content

“Generative artificial intelligence accelerates the manufacture of persuasive but false content.”

that looks and sounds right even when it is wrong. When that output carries familiar cues such as a known voice, official phrasing or a realistic image, people are inclined to treat it as credible.

Canadian defence operations now contend with adversaries who can generate convincing imitations of official content in minutes, not weeks.³ A fabricated article, an altered image, or a cloned voice can be produced quickly and pushed across multiple platforms at a negligible cost.

For Defence practitioners, these changes introduce three reinforcing pressures:

- **Speed.** Adversaries can inject manipulated material into the information environment while events are still unfolding. A forged audio clip of an evacuation order can spread across social media before provincial authorities have even had time to draft the real message.⁴ In an operational setting, a fabricated command fragment can reach a unit before headquarters has confirmed the actual order. Speed is the adversary's advantage, because even a short hesitation can interrupt tempo and sow doubt.
- **Cost.** Generative tools are widely available, user-friendly, and inexpensive. What once demanded professional editing suites and trained operators can now be achieved with a laptop and a few dollars' worth of subscription software. This means that hostile states, proxy groups, or even lone actors can all play at scale. Defence therefore faces not only state-sponsored disinformation but also opportunistic interference from actors with little to lose.⁵
- **Precision.** Adversaries can test and refine messages in near real time, adapting to what gains traction in specific audiences. A manipulated clip that fails to resonate with one community can be quickly re-framed and re-released to another.⁶ This iterative precision allows adversaries to tailor content not just by language or region, but by exploiting the specific narratives or fears of targeted groups, including military families, diaspora communities, or allied partners.

For the DND/CAF, the consequence is an operational environment where uncertainty can be manufactured faster, cheaper, and more accurately than ever before. An order delayed, a message clouded by doubt, or an instruction competing with a convincing imitation all erode trust. Adversaries no longer need to deceive

“Adversaries no longer need to deceive everyone; they merely need to create hesitation in enough people, at enough key moments, to disrupt coordination.”

everyone; they merely need to create hesitation in enough people, at enough key moments, to disrupt coordination.

To counter this, authentication must become a routine feature of military communications, reinforced by training and leadership until it is second nature. Authentication here refers to verifying the origin and integrity of a message within the chain of command. The broader perception of authenticity—how audiences assign trust to official communications—remains critical but is distinct from technical safeguards.

When authentication is habitual, whether in confirming orders within the chain of command, embedding markers in public updates, or rehearsing verification in exercises, tempo and credibility stay with the institution rather than with those who seek to disrupt it.⁷ In this way, it is not simply a communications practice but a form of operational security—it protects speed, safeguards unity, and preserves decision advantage.

Truth Under Pressure in a Democracy

The same dynamics that complicate operational decision-making do not stop at the tactical level. They reach into the broader environment where the DND/CAF must explain decisions to Canadians, uphold accountability before Parliament, and coordinate with allies. When synthetic material blurs what is real, the consequences go well beyond a temporary disruption in the field. It corrodes public confidence in the institutions that protect Canadians.⁸ It weakens the credibility of leaders when their words and actions can be plausibly dismissed as fabrications. And it injects friction into allied cooperation, where even fleeting doubt can slow collective decisions or distort perceptions of Canada's reliability. In this sense, synthetic manipulation is not simply a battlefield nuisance but a strategic threat that targets the very foundations of trust that democratic defence requires.⁹

Generative systems complicate trust by producing convincing imitations of official material. The deeper problem is that once the public knows such forgeries exist, genuine records can also be doubted. A video that actually shows misconduct, a document that really records a breach, or an audio clip that captures an ill-judged remark can all be dismissed as fabrications. This is what scholars call the “liar's dividend—the ability of bad actors

to escape accountability by claiming that authentic evidence has been manipulated”.¹⁰

Addressing this challenge requires more than technical verification. Institutions must build resilience through consistent communication practices, transparent correction of errors, and public education about what authentic updates look like and through which channels they will appear. When the DND/CAF openly and promptly corrects errors and explains processes, it shows that credibility comes from transparency and accountability, not from projecting a false image of perfection. When it explains in advance how official communications will be marked and distributed, it equips Canadians to recognize imposters. These practices do not eliminate the liar's dividend entirely; they help reduce its impact by making authenticity a consistent expectation rather than an afterthought.

Canada's Distinct Information Environment

The challenge of generative systems is more than a technical issue. It is a question of trust that affects how we operate in contexts that are uniquely Canadian.

Defence faces these pressures in ways shaped by our geography and our institutions. As a result of Canada's geography, we have to contend with large distances, harsh weather, and limited infrastructure, especially in the North. Institutions add their own complexity, as Canada is a federation where responsibilities are shared across levels of government, where Indigenous leadership holds recognized authority, and where continental defence is conducted through binational arrangements like NORAD. These features shape how information moves, who speaks with authority, and how trust is earned.

Unlike more centralized states, Canada's layered system of governance means that no single institution controls the narrative in a crisis. A wildfire evacuation order may come from a municipality, be reinforced by a province, and receive support from the Canadian Armed Forces. In these conditions, clarity is essential because adversaries can exploit even small gaps between jurisdictions to inject doubt.

Domestic crises reveal how pressures multiply when larger populations and multiple jurisdictions are involved. Wildfires, floods, and public health emergencies require responses that cross municipal, provincial, territorial, and federal boundaries. In these moments, a false alert that looks official or a rescindment of an evacuation order can spread rapidly across social media.¹¹ Even a few minutes of hesitation can make evacuation routes more dangerous or emergency services harder to coordinate.

Domestic crises also expose the fragility of the systems Canadians rely on. Wildfires can damage cell towers, floods can cut power, and surges in demand can overwhelm local networks. For the DND/CAF, supporting civil authorities means preparing for both physical disruption and the possibility of synthetic



A Flight Engineer with 440 Transport Squadron based in Yellowknife, Northwest Territories, helps ground guide the CC-138 Twin Otter aircraft for landing at Tuktoyaktuk Airport as part of Operation NANOOK-NUNALIVUT on March 3, 2026.

Photo: Corporal Borden Webb-Brown, Imagery Technician, 14 Wing Greenwood

interference arriving at the same time. In Canada's North, conditions for communication are different and the consequences of confusion can be immediate. Towns are small, close-knit, and often distant from large centres. Infrastructure is modest, and communications can be disrupted by weather, geography, or limited bandwidth.¹²

In many communities, word-of-mouth, local radio, and community Facebook pages are still go-to communication channels.¹³ That closeness is a strength, but it also makes northern communities vulnerable. Rumours spread quickly because people care deeply for one another and act fast when they believe neighbours may be at risk. A fabricated message about a missing person, a hazardous spill, or an evacuation order can travel at the speed of conversation, long before an official update is noticed or believed.

For the DND/CAF, this means credibility in the North cannot rest only on technical fixes. It depends on human relationships that are built long before an emergency. Indigenous elders, local broadcasters, and community leaders often carry more authority in practice than distant officials.¹⁴ When the DND/CAF works with these actors to model authentic communication and demonstrates it during routine patrols, training exercises, and seasonal operations, it invests in a network of trust that is uniquely Canadian. These networks do not just pass along information, they translate it into the cultural and linguistic context of the community, making it both recognizable and actionable.¹⁵

The strength of this approach comes not just from visual cues like logos or branding—which can be copied—but from the trusted individuals who share information with established credibility and who are well-regarded. This includes trusted knowledge bearers who may have specialized knowledge and best understand how to reach the greatest number of individuals in their respective communities.

When residents know what an official message looks like and where it will appear, and when they have seen that practice tested in calmer conditions, they are more likely to disregard screenshots or forwarded messages. For the DND/CAF, this is not only a matter of communication technique, it's about respect for northern communities, recognition of Indigenous leadership, and partnership with local organizations that hold trust beyond what federal authorities can achieve on their own.

The North American and Allied Lens

In binational aerospace defence, the ability to issue trusted updates in near real time is integral. When a balloon or aircraft, for example, attracts public interest, Canadians and Americans will look for immediate reassurance.

NORAD rests on the premise that Canada and the United States respond as one, and that confidence in that unity is visible to citizens, political leaders, and adversaries alike. Timely, credible communication is therefore not an accessory to continental defence, it is one of its systems.¹⁶ Just as radar networks provide a shared view of the skies, consistent and authoritative updates provide a shared view of events.

The same logic applies to Canada's broader alliances. Coalition exercises and deployments are particularly vulnerable because they demand high levels of trust and synchronization among diverse partners. Adversaries understand this.¹⁷ A single synthetic provocation, a forged after-action report suggesting a capability failure, a fabricated image implying misconduct, or a falsified message hinting at disunity among commanders, can be timed to coincide with a critical decision point. Even if debunked within hours, such incidents consume valuable bandwidth, delay coordination, and erode confidence within the coalition.

These disruptions rarely break alliances outright, but their cumulative effect narrows the margin for error and makes collective action harder. Differences in national priorities are natural within coalitions, but synthetic manipulation weaponizes those differences, magnifying suspicion and slowing unity of effort.¹⁸

When Canada and the United States employ recognizable methods of authentication—consistent visual markers on updates, cryptographic signatures embedded in imagery and video, and habitual use of official channels—the public learns what to look for and journalists can report with greater confidence under pressure.¹⁹ In this way, authentication becomes not only a safeguard against confusion but a strategic asset that underpins the credibility of continental defence.

For Canada, credibility in allied operations depends not only on the professional conduct of our forces but also on the speed and clarity with which that conduct is represented to partners and the public alike. Authentication in this sense becomes operational currency; it buys tempo, steadies confidence, and denies adversaries the space to turn doubt into delay. Whether in continental defence, northern communities, or international operations,

the CAF requires habits of disciplined communication that are routine long before a crisis begins.

Public Affairs and the Canadian Voice of Credibility

The habits of verification that protect the chain of command must also extend to how the DND/CAF speaks to the public. Culture is expressed in the tone, timing, and clarity of how we communicate. Public Affairs therefore begins well before a crisis. If the DND/CAF explains in plain language that convincing fakes are now part of the information environment, demonstrates how authentic updates will appear, and makes a habit of steady communication when the stakes are low, the public learns what to expect when the stakes are high.²⁰ In a crisis, Canadians respond best to clarity about process: what steps are being taken to verify, when the next update will arrive, and how to avoid spreading harm while the facts are gathered.²¹

Canada's public voice must also reflect who we are. Canadians value fairness and straightforward speech. A short video from a commanding officer, posted quickly on an official channel, carries moral weight because it is both personal and institutional. A statement that sets out what information will be released and when earns credibility, because it commits the DND/CAF to a clear timeline and shows the public what to expect. In bilingual communications, speaking with equal clarity in both official languages signals care and strengthens trust. Where Indigenous communities are involved, direct engagement with community leadership in culturally appropriate ways, and through trusted intermediaries, reinforces legitimacy and helps verification habits spread.

Verification in the Chain of Command

Synthetic interference does not need to deceive an entire formation to have effect. When many elements must move together, hesitation by a single unit is enough to erode momentum, introduce risk, and give an adversary room to manoeuvre. The danger lies not in mass deception, but in the small fractures of confidence that can ripple through a formation when information cannot immediately be trusted.

This risk is not new. Armed forces have always needed ways to ensure that orders are genuine. Historically, units relied on call-signs, code phrases, or even physical couriers to verify instructions. During the Second World War, for example, challenge-and-response codes were a routine safeguard, and even in modern operations radio checks remain a basic discipline.²² The principle has always been the same; no matter how urgent the moment, units must be sure that what they are acting on is authentic. Modern communications have increased speed, but they have also multiplied the points where a false or manipulated message could enter the system. What changes in the age

of synthetic content is how convincing a forged instruction can appear, and how little time there may be to question it.²³

An unexpected order received during a manoeuvre illustrates the problem. The message may look or sound authentic, but if its timing raises doubts and there is no agreed way to check, the safest choice is often to pause until higher authority can confirm.²⁴ If the order was genuine, that pause has already cost time in a critical window. If it was false, the unit may have avoided a mistake—but only by slowing down and surrendering their initiative. Either way, uncertainty extracts a price. In a high-tempo environment, even seconds of hesitation can alter the outcome of an engagement, shift the balance of initiative, or create openings for an adversary to exploit.

Defence practice must therefore emphasize simple, rapid methods of confirmation. A pre-arranged signal, a short exchange over an alternate channel, or another agreed procedure can resolve doubt in seconds. These safeguards are not new—radio checks, challenge-and-response protocols, and confirmation through alternate channels have long been standard practice. What has changed is the operational context: synthetic audio that mimics a commander's voice with high fidelity, fabricated video that appears to show orders being issued, or text messages that replicate the style and format of legitimate communications with precision.

Current DND/CAF procedures assume that most communications can be trusted unless there is specific reason for doubt. In an environment where convincing forgeries can be produced at scale and speed, this assumption no longer holds. The gap is not that verification procedures do not exist, but that they are not consistently applied when information arrives through familiar channels. Training often focuses on verifying orders that are obviously suspicious—those that arrive through unusual means or contradict known plans—but does not routinely rehearse verification of plausible-seeming instructions that may have been subtly manipulated.

Moreover, operational constraints can limit the effectiveness of existing procedures. During domestic emergencies such as floods or wildfires, infrastructure disruption may degrade alternate communication channels, making it harder to confirm orders through independent means. Similarly, generative-AI-enabled manipulation may spread misinformation that undermines CAF operations, such as fake alerts about disasters, slowing response efforts.²⁵ In coalition operations, differences in national procedures or language barriers can slow verification when speed is most needed. And in high-tempo combat scenarios, the pressure to act quickly can override the instinct to verify, especially when an order appears to come from a trusted source.

What is required is not the invention of new procedures but the consistent integration of existing ones into routine practice, adapted to account for synthetic threats. This means rehearsing verification drills not only for obviously suspicious orders but for routine-seeming instructions that arrive during exercises. It means

ensuring that alternate communication channels are tested and maintained as rigorously as primary ones. And it means training personnel to recognize that in the current environment, verification is not a sign of hesitation but of professionalism—a discipline as fundamental as weapons handling or navigation.

Leadership is central to this discipline. Commanders set the expectation that surprising instructions are always checked, and that verification under pressure is not a sign of weakness but of professionalism.²⁶ Units that rehearse these drills in exercises will find them instinctive in operations. When leaders consistently reinforce that verification is expected, and when they acknowledge it as sound judgement rather than hesitation, the culture of an entire formation begins to shift. The result is not only to prevent mistakes, but to preserve confidence inside the chain of command when adversaries attempt to sow confusion.

Embedding Trust in Policy, Training, and Leadership

Credibility cannot rely on technology alone. It must be reinforced through the full machinery of Defence in policy, in training, and in leadership practice. Law and policy need not chase every technical novelty to be useful. They need to give clarity and confidence to those responsible for speaking and deciding. For the DND/CAF, this means that doctrine, guidance, and standard operating procedures must all reflect the reality that synthetic content is not an anomaly but a persistent feature of the environment. Policy alone is not sufficient. Training is where principles become second nature. Just as soldiers learn to conduct radio checks or execute standard drills, DND/CAF personnel can learn to handle ambiguous information without hesitation. A watch officer who encounters a suspicious clip should know immediately whom to call and what to say. A commander who receives an unusual order should be prepared to seek confirmation through an alternate channel.

The challenge is not that this knowledge is absent, but that it is not routinely practiced under realistic conditions. Current training often treats information verification as a secondary concern, addressed in classroom settings rather than integrated into field exercises. Personnel may know in principle whom to contact when they encounter suspicious material, but without regular rehearsal under stress, that knowledge does not translate into instinctive action. After-action reports from recent exercises have noted instances where units hesitated or acted on unverified information because verification procedures, though known, were not habitual.²⁷

These moments should not be left to improvisation in the field. They need to be woven into exercises at every level, from basic training to large-scale joint exercises, so that CAF members instinctively practice verification in the same way they already practice battle drills, navigation, or radio discipline.

Public Affairs officers should have language pre-cleared that allows them to act quickly when false or misleading material is



An Observer, Controller, Trainer (OCT) responsible for the evaluation of ex GLOBAL RESOLVE, tracks and updates troop movements in the training area with a Tactical Assault Kit (TAK) tablet, allowing real-time communication between different OCT elements in the field. Image taken in the Yukon Training Area near Fairbanks, Alaska, on February 17, 2026.

Photo: Cpl Dustin LeVasseur Pearce

circulating. This means they are not waiting for legal or policy approval in the middle of a crisis, but can immediately acknowledge that contested material exists, caution the public that it has not been verified, and point directly to trusted official sources where updates will appear. Having this language prepared in advance prevents silence from being mistaken for confirmation, and ensures that the first word from the DND/CAF is one of clarity and direction. Moves like these may seem minor on their own, but together they create a posture of readiness that allows operations and communications to continue steadily even when adversaries try to inject confusion. Exercises that test these communications drills, complete with simulated forgeries and fabricated clips, would make verification as routine for Public Affairs as weapons handling is for infantry.

Leadership is the hinge that turns principles into habits. When senior officers and officials model disciplined verification under pressure, subordinates see it not as hesitation but as professionalism. A commander who insists on a quick confirmation before acting on an unusual order sets a tone that spreads through the formation. A Public Affairs leader who corrects an earlier statement with the same speed and visibility as the first release shows that credibility is built on candour. These examples travel quickly inside a military culture where tone and timing at the top shape behaviour across the ranks.

Ultimately, trust must be embedded across all levels of Defence—written into doctrine, reinforced through routine training, and modelled by leaders in both calm and crisis. These three pillars—policy, training, and leadership—work together to ensure that the CAF does not face synthetic interference as an improvised challenge but as an environment for which it is fully prepared.

Measuring a Canadian Standard of Success

Defence is experienced at measuring readiness, and the same discipline applies in the information environment.²⁸ The most important measure is time. The institution must track how long it takes to classify suspicious material, provide internal guidance on confidence, and issue a trusted public update. It must also record how quickly units confirm or dismiss unusual orders through established procedures, and how often these drills are rehearsed in exercises. Just as operational readiness reports measure ammunition stocks, equipment serviceability, or personnel strength, the DND/CAF can measure information readiness by how quickly and reliably the system can validate or reject contested material.²⁹

Performance must show steady improvement, just as in other areas of readiness.

For example, if a formation currently requires twenty minutes to escalate and resolve a suspicious order, exercises should aim to reduce that to ten minutes, then five, without sacrificing accuracy or safety. If Public Affairs teams need an hour to coordinate a first statement during a domestic emergency, the goal should be to bring that down to minutes through pre-cleared language, distributed authorities, and clear escalation channels. Each iteration becomes an opportunity to shorten the cycle while strengthening trust.

Surveys and feedback loops can add further texture. Canadians should be asked whether they know where to find authentic DND/CAF updates and whether they can describe what those updates look like. Journalists and civil society partners can be consulted on whether verification tools are accessible and reliable. Allies can be surveyed on whether Canadian methods are interoperable with theirs, and whether our signals can be trusted instantly in multinational settings. These forms of measurement, though qualitative, are as critical to resilience as quantitative metrics. Scholars researching institutional trust and trustworthiness have created useful frameworks for assessing these dimensions.³⁰

They will continue to appear, and adversaries will continue to innovate. Success will mean that Canada responds calmly, speaks quickly, and retains trust when they appear. In practice, this

translates to fewer pauses in operations because of unauthenticated instructions, fewer instances where false alerts outpace real ones during domestic emergencies, and fewer occasions where fabricated narratives distract from the purpose of allied exercises or deployments. When measured consistently, these benchmarks allow Defence to know not only whether it is prepared, but whether Canadians and allies share confidence in that preparation.

Conclusion

Generative artificial intelligence has transformed the conditions under which truth must compete for attention; it has made falsehood cheap, fast, and convincing. That reality touches the heart of military effectiveness.³¹ If a forged message can slow a decision, if a fabricated video can fracture allied unity, or if a false alert can pull Canadians into danger, then adversaries have succeeded without firing a shot. This is the contest in which the Canadian Armed Forces now operate.

Canada is not powerless in this fight. Defence does not need to eliminate every forgery; it needs to prove what is real faster than falsehoods can spread. That means commanders who expect verification before manoeuvre, Public Affairs teams who speak early with candour, policies and tools that make authentication ordinary, and leaders who practice discipline in communication as rigorously as they do in operations. It means making the DND/CAF voice recognizable across every setting—whether in NORAD's command posts, in northern communities, during domestic crises, or on coalition operations abroad.

The DND/CAF has always defined itself by professionalism, integrity, and the ability to act under pressure.³² In the information battles now unfolding, those same qualities are the foundation of advantage. By proving authenticity, protecting tempo, and speaking with a voice that reflects Canadian values of honesty and respect, the DND/CAF needs to shield itself from deception and protect the democracy it serves.

Notes

- 1 Joseph Vossler, Gerald Mazur, Andre Slonopas, Danyl Miller, Edward Olbrych, Aaron Sweeney, and Jacob Strahan, "Artificial Intelligence as a Force Multiplier in U.S. Military Information Campaigns," *Cybersecurity and Information Systems Information Analysis Center (CSIAIC)*, October 28, 2024. Originally found at: <https://csiac.dtic.mil/articles/artificial-intelligence-as-a-force-multiplier-in-u-s-military-information-campaigns/>.
- 2 Cole Stryker and Mark Scapicchio, "What Is Generative AI?," *IBM Think*, March 22, 2024. Originally found at: <https://www.ibm.com/think/topics/generative-ai>.
- 3 Canadian Security Intelligence Service, "Implications of Deepfake Technologies on National Security," Government of Canada, July 14, 2025. Originally found at: <https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future/implications-of-deepfake-technologies-on-national-security.html>.
- 4 Akshay Kulkarni, "BC Wildfire Service Faces Challenges from AI-Generated Misinformation," *CBC News*, August 6, 2025. Originally found at: <https://www.cbc.ca/news/canada/british-columbia/bc-wildfire-service-ai-misinformation-1.7602041>.
- 5 Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2025-2026," Government of Canada, October 30th, 2024. Originally found at: <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf>.
- 6 "An existential threat: Disinformation 'single biggest risk' to Canadian Democracy," *Digital Forensic Research Lab (DFRLab)*, March 19, 2024. Originally found at: <https://dfriab.org/2025/03/19/canada-disinfo-existential-threat/>.
- 7 National Security Agency, Federal Bureau of Investigation, and Cybersecurity and Infrastructure Security Agency, *Contextualizing Deepfake Threats to Organizations*, September 12, 2023. Originally found at: <https://media.defense.gov/2023/Sep/12/2003298925/-1/0/CSI-DEEPPFAKE-THREATS.PDF>.
- 8 *Increasing Threats of Deepfake Identities*, Department of Homeland Security, accessed September 29, 2025. Originally found at: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.
- 9 Di Cooke, Abigail Edwards, Alexis Day, Devi Nair, Sophia Barkoff, and Katie Kelly, *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*, Center for Strategic and International Studies, November 1, 2024. Originally found at: <https://www.csis.org/analysis/crossing-deepfake-rubicon>.
- 10 Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6, December 2019. Originally found at: <https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security>. Also see Vaccari, Cristian & Andrew Chadwick (2020). "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media + Society*, 6(1).
- 11 Akshay Kulkarni, "AI-Generated Media and Misinformation of N.W.T. Wildfires Circulating, Fire Officials Warn," *CBC News*, August 6, 2025. Originally found at: <https://www.cbc.ca/news/canada/north/ai-generated-media-and-misinformation-of-n-w-t-wildfires-circulating-fire-officials-warn-1.7623579>.
- 12 Alexander Dalziel and Daniel Nikoula, *Polarized: Climate Change, Geopolitics and Disinformation in the Arctic*, Information Integrity Lab, University of Ottawa, July 2025. Originally found at: <https://infoilab.uottawa.ca/comm/Uploaded%20files/PDI%20files/Polarized-EN-FINAL.pdf>.
- 13 Rob McMahon, Michael B. McNally, Eric Nitschke, Kyle Napier, María Alvarez Malvido, and Murat Akçayir, "Codesigning Community Networking Literacies with Rural/Remote Northern Indigenous Communities in Northwest Territories, Canada," *Journal of Computer-Mediated Communication* 29, no. 1, January 2024. Originally found at: <https://doi.org/10.1093/jcmc/zmad042>.
- 14 Department of National Defence, "Department of National Defence Indigenous Reconciliation Program - Grants and contributions," Government of Canada, March 27, 2025. Originally found at: <https://www.canada.ca/en/departement-national-defence/programmes/indigenous-reconciliation-funding.html>.
- 15 Jayde Lavoie, Jill Barclay, and Wilfrid Greaves, *Improving the Canadian Armed Forces' Recruitment and Retention of Indigenous People: Best Practices from the New Zealand Defence Force, North American and Arctic Defence and Security Network*, Queen's University, September 8, 2020. Originally found at: https://www.naadsn.ca/wp-content/uploads/2020/09/20-September_Policy-Brief-CAF-1.pdf.
- 16 Department of National Defence, "Joint Statement on Norad Modernization," Government of Canada, August 14, 2021. Originally found at: <https://www.canada.ca/en/departement-national-defence/news/2021/08/joint-statement-on-norad-modernization.html>.
- 17 Jill Goldenziel and Daniel Grant, "Information Resilience: Countering Disinformation and Its Threat to the U.S. Alliance System," *War on the Rocks*, November 15, 2023. Originally found at: <https://warontherocks.com/2023/11/information-resilience-countering-disinformation-and-its-threat-to-the-u-s-alliance-system/>.
- 18 Patrick Samaha, "Weaponized AI, The New Frontline in Global Disinformation Warfare," *NATO Association of Canada*, June 24, 2025. Originally found at: <https://natoassociation.ca/weaponized-ai-the-new-frontline-in-global-disinformation-warfare/>.
- 19 For current standards and ongoing initiatives, see Content Authenticity Initiative (CAI), which develops technical standards for content provenance (contentauthenticity.org), and the Coalition for Content Provenance and Authenticity (C2PA), which provides specifications for embedding cryptographic metadata in digital media (c2pa.org). NATO's Strategic Communications Centre of Excellence has also published guidance on countering disinformation in military contexts (stratcomcoe.org).
- 20 Department of National Defence, *Canadian Army Communication Strategy 2024-2026*, Government of Canada, July 15, 2025. Originally found at: <https://www.canada.ca/en/army/services/for-the-soldier/canadian-army-communication-strategy-2024-2026.html>.
- 21 Eric J.G. Storm, *Needing Unified Direction: Developing Capabilities for Operations in the Information Environment*, Canadian Forces College, 2025. Originally found at: <https://www.cfc.forces.gc.ca/259/290/950/305/StormSF50DL.pdf>.
- 22 George I. Back and George Raynor Thompson, "Military Communication," *Encyclopaedia Britannica*, accessed on September 29, 2025. Originally found at: <https://www.britannica.com/technology/military-communication>.
- 23 Di Cooke, Abigail Edwards, Alexis Day, Devi Nair, Sophia Barkoff, and Katie Kelly, *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*, Center for Strategic and International Studies, November 1, 2024. Originally found at: <https://www.csis.org/analysis/crossing-deepfake-rubicon>.
- 24 Daniel L. Byman, Chongyang Gao, Chris Meserole, and V. S. Subrahmanian, *Deepfakes and International Conflict*, Brookings Institution, January 2023. Originally found at: https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf.
- 25 Recent incidents show how Generative AI amplifies misinformation risks: during the 2025 Northwest Territories and British Columbia wildfires, AI-generated images exaggerated fire damage and spread widely on social media. See: *N.W.T. fire officials warn of AI-generated images, misinformation circulating online* | *CBC News*; *AI-generated wildfire images spreading misinformation in B.C., fire officials warn* | *CBC News*, and *AI-generated images exaggerated fire damage and spread widely on social media*. In 2022, a deepfake video of President Zelenskyy urging Ukrainian troops to surrender circulated online, aiming to erode morale during active combat. See: *A deepfake video showing Volodymyr Zelenskyy surrendering worries experts* : *NPR*.
- 26 Gen. Gary Brito, "Professionalism Is the Foundation of the Army and We Will Strengthen It," *War on the Rocks*, March 18, 2024. Originally found at: <https://warontherocks.com/2024/03/professionalism-is-the-foundation-of-the-army-and-we-will-strengthen-it/>.
- 27 While specific after-action reports remain classified, this observation is consistent with findings from NATO exercises on countering hybrid threats, where information verification was identified as an area requiring greater emphasis in training. See: *NATO Strategic Communications Centre of Excellence, Hybrid Threats: A Strategic Communications Perspective*, 2019.
- 28 *The Canadian Armed Forces Ethos: Trusted to Serve*, Department of National Defence, July 19, 2023. Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/CAF%20Ethos%20Trusted%20to%20Serve%20-%20English%20-%20FINAL.pdf>.
- 29 Department of National Defence, "CDS/DM Directive for CAF Force Posture and Readiness (FP&R) 2024/2025," Government of Canada, March 12, 2025. Originally found at: <https://www.canada.ca/en/departement-national-defence/corporate/policies-standards/dm-cds-directives/cds-dm-directive-caf-force-posture-readiness.html>.
- 30 Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734; and Grimmelikhuijsen, S., & Knies, E., 2017. Validating a scale for citizen trust in government organizations. *International Review of Administrative Sciences*, 83(3), 583-601.
- 31 Austin Coombs, "Persuade, Change, and Influence with AI: Leveraging Artificial Intelligence in the Information Environment," *Modern War Institute*, October 25, 2024. Originally found at: <https://mwi.westpoint.edu/persuade-change-and-influence-with-ai-leveraging-artificial-intelligence-in-the-information-environment/>.
- 32 *The Canadian Armed Forces Ethos: Trusted to Serve*, Department of National Defence, July 19, 2023. Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/CAF%20Ethos%20Trusted%20to%20Serve%20-%20English%20-%20FINAL.pdf>.



A pilot from 408 Tactical Helicopter Squadron does the last of his pre-flight checks before taking flight in a CH-146 Griffon helicopter, near the training area of Wainwright, Alberta during Exercise INTREPID BEAR 22 on May 4, 2022.

Photo: Master Sailor Dan Bard, Canadian Forces Combat Camera, Canadian Armed Forces photo

Cybersecurity and Air Power: Keeping Humans in the Loop

KRISTEN CSENKEY AND ALEXIS RAPIN

Dr. Kristen Csenkey is a Social Sciences and Humanities Research Council (SSHRC) postdoctoral fellow at the Brian Mulroney Institute of Government, St. Francis Xavier University. She is also a fellow with the Canadian Maritime Security Network, the Centre for Military, Security and Strategic Studies at the University of Calgary, and the North American and Arctic Defence and Security Network (NAADSN), among others. Dr. Csenkey has previously led multiple Department of National Defence-funded projects on the defence and security implications of quantum technologies, connected aviation systems, and cyber-resilient electric vehicles. She currently leads a SSHRC Partnership Engage Grant focused on responsible global quantum technology governance. She holds H.B.Sc., M.A., M.A.P., and Ph.D. degrees.

Alexis Rapin is an associate fellow with the Raoul-Dandurand Chair of Strategic and Diplomatic Studies (affiliated with the University of Quebec in Montreal). His research focuses on cybersecurity and on the international security implications of digital technologies. In 2023, he testified before the Standing Committee on National Defence of the House of Commons of Canada on issues related to Canadian cyber defence and strategy. He is also a member of the editorial committee for Le Rubicon, a francophone platform dedicated to the analysis of international and strategic affairs.

In their novel *2034* (published in 2021), authors Elliot Ackerman and former United States (US) Admiral James G. Stavridis imagine a major future conflict between the United States and China.¹ The first pages open with an incident in which an American F-35 fighter is suddenly captured by Iran, after a cyber attack has enabled them to remotely take control of the aircraft. Later in the book, faced with a desperate situation, the US Navy decides to retire its F-35 fleet and reactivate its old F-18s, which are stripped of most of their on-board electronics in the process. As its adversaries have managed to compromise its high-tech aircraft, the United States is forced to rely on its technological ancestors, assumed to be digitally safer.

Although an intriguing and fictional situation,² the scenario narrated in *2034* relates to an idea gaining traction in the strategic literature: namely, that the current approaches to technological superiority that have been the hallmark of Western militaries for almost 40 years may now represent a vulnerability.³ As cyber-warfare capabilities expand, it now seems possible for adversaries to take advantage of the emerging dependencies and possible vulnerabilities associated with highly connected technologies. Additionally, varying collective risk management practices, as well as legacy systems and an enlarged attack surface, increase exposure to sophisticated cyber attacks and potentially compromisable electronic components, systems, processes, technologies and people. We can observe this blending and complexity materializing in current geopolitical conflicts. For example, in the face of the ongoing Russian invasion, the Ukrainian military is reusing old field telephones along the frontline, fearing that its modern transmission systems may be compromised by its adversary.⁴

In this paper, we take an expansive view of cyber-warfare and connected technologies, encompassing both cyber and electronic warfare. Although operations in the cyber domain and electromagnetic sphere can have distinct characteristics (especially with regard to the units, capabilities and know-how involved), we focus on the implications of the associated human and technological vulnerabilities, capabilities and activities. Broadly, we contextualize this situation as part of a holistic cyber concept where electromagnetic tools, such as radio frequency jamming, and cyber tactics, such as hacking, comprise a dynamic space where humans and technologies interact in a digital-physical environment.⁵ This environment poses challenges for operations and activities in all domains, and we thus argue for solutions to both human and technical vulnerabilities.

The problem of interconnected technologies and threats proves especially meaningful to the aviation sector, in which aircraft, drones, helicopters,⁶ and the digital-physical infrastructure that supports them are now highly digitized and connected. In a scenario that may well have inspired Ackerman and Stavridis, in 2011, the United States lost an observation drone after Iran hacked into its GPS system to land the drone on an Iranian base.⁷ Drones are no longer considered part of a “poor man’s air force,”⁸ especially when paired with new cyber tactics,⁹ procedures,¹⁰ and increasingly available commercial technologies.¹¹ Others have also detailed how the F-35, which is deployed by a

growing number of Western armies, represents the epitome of a weapon system that is highly vulnerable to cyber threats.¹² Cyber threats are no longer a hypothetical danger: they are a reality for modern air forces to constantly be aware of, act upon, mitigate, and understand in terms of their connections in digital-physical spaces. The challenge before the forces is clear: identify how to deal with these threats, without renouncing their cutting-edge technologies.

“Cyber threats are no longer a hypothetical danger: they are a reality for modern air forces.”

One of the major issues is that the military “techno-solutionism,” inherited from the 1990-2000s,¹³ may be replaced by a “techno-pessimism,” in which armed forces in general (and air forces in particular) may have declining confidence in their high technologies and devices and end up discarding some of them, as in *2034*. Indeed, one of the great strengths of cyber capabilities is not only that they may undermine the availability and usability of military technologies, but also that they reduce the trust placed in them by a decision maker. By simply instilling doubt about the integrity of a system, cyber attacks may dissuade an actor from using a wider set of capabilities, thus producing a result disproportionate to their actual effects. Some, such as Christopher Coker,¹⁴ have surmised that this could be the future strategy of foreign powers like China. A state could attempt not to match a technologically superior competitor, but instead force a reduction in the use of certain technologies by persuading the adversary that these have been compromised or rendered inept.

Consequently, cultivating and securing the confidence of Western militaries in the technologies they employ, and in which they have invested considerable resources, appears to be a crucial issue of strategic importance.¹⁵ This may prove all the more important in a crisis context, where quick and difficult decisions may have to be made about the reliability of information technologies. The aim of this article is to present possible solutions to this challenge. We propose an approach that puts people at the heart of securing air power against cyber threats. This involves

cultivating the human capital and organizational structures needed to maintain a high degree of trust and technological resilience within an air force. As the Royal Canadian Air Force celebrates its centennial, adapts to defend and protect Canada, and continues to support the defence of North America with the United States, there is an opportunity to explore the increasing connectivity between domains, technologies, and the continued importance of people in a dynamic environment.

Boyd 2.0: Reinventing the Loop

To fully understand the issue at hand, we must first go back to the origins of the techno-solutionist paradigm and especially to one of its key concepts: the famous “OODA loop” (for Observe, Orient, Decide, Act), theorized by US Air Force Colonel John Boyd in the 1980s.¹⁶ Intended to describe the process by which an actor perceives a situation, analyzes it, deliberates, and acts accordingly, the OODA loop has since acquired much celebrity and—for better or worse—has been applied to a variety of non-military purposes, from business to sport. In the military domain, the OODA loop concept gradually gave rise to a full-fledged theory of victory, embraced by several major Western armed forces,¹⁷ such as the United States, the United Kingdom and France.¹⁸ In short, the core concept is that an actor who manages to complete the OODA cycle in the shortest possible time acquires an advantage over their adversary. Among other advantages, a rapid completion of the OODA loop is assumed to provide an actor with better situational awareness, ultimately enabling them to control the tempo of operations.¹⁹ Over the course of the 1990s, this logic led militaries to acquire increasingly sophisticated Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) technologies, to rapidly complete the OODA loop.

The OODA loop paradigm may now appear undermined by the increasing complexity and development of electronic and cyber-warfare capabilities. As cyber means have the potential to compromise the information technologies upon which the fluidity of the OODA loop heavily depends, they seem to threaten the viability of a way of war largely based on technological and information superiority.²⁰ Some approaches to contextualizing cyber operations demonstrate that an adversary can be restrained in the context of open warfare by hacking their information collection capabilities or communications systems.²¹ In this regard, cyber threats appear of particular importance in the air domain, where digital technologies are not only omnipresent and critical to mission completion, but also represent potential attack vectors. Indeed, air forces around the world must now contend with cyber-related threats, the risks enmeshed within the usage of and connection to complex technologies, and varying human actions, such as GPS spoofing,²² onboard software hacking,²³ or compromised data links,²⁴ in addition to threats relating to ground bases and physical installations. For instance, during the 2019 Gulf of

Oman crisis, the US military hacked a database operated by the Islamic Revolutionary Guards in order to cripple Iran’s targeting capabilities (including through the use of attack drones).²⁵ The above-mentioned vulnerabilities, if exploited, may considerably slow down or even paralyze the completion of the OODA loop.

In spite of its many uses and misuses throughout the years, the OODA loop remains a useful thinking framework for our purpose, as it helps emphasize two crucial aspects related to the management of cyber threats. First, the principle of the OODA loop is applicable to situations relating to cyber attacks, posture and planning. When faced with a cyber incident, for example, a military must ultimately be able to *Observe* the impact of hacking activities, *Orient* itself amidst the impacts caused by the attack, *Decide* with confidence which capabilities are compromised and which remain serviceable, and finally *Act* on the basis of this analysis. The OODA loop concept can thus be applied to understanding the impact of an attack and the appropriate resulting actions. To be sure, the OODA loop is not used for reacting to a cyber incident; however, it is a useful concept to develop confidence in both people and technologies, as we will further demonstrate.²⁶

Second, although information technologies appear to be important enablers and accelerators of the OODA loop, they are by no means its only components. The processes by which a military gathers and processes information include crucial human and organizational components, which are as important as the technologies themselves.²⁷ As others have shown, modern militaries may display a less-than-optimal use of cutting-edge technologies due to poor management of human and organizational issues.²⁸ Of course, an increase in the speed of completion of the OODA loop is not the only factor in achieving mission success in modern warfare. Nevertheless, human and organizational components are involved in the process and must be further developed to ensure its rapid completion. The challenge then becomes trying to determine how to make the best use of available human and organizational resources to maintain or re-establish the fluidity of the OODA loop in a context where technologies are (or appear to be) degraded.

In the sections that follow, we provide examples drawn from Canada’s international allies, as well as suggestions to further develop resilience in digital and physical contexts of conflict. We conclude by drawing together our discussion and recommendations in the context of NORAD modernization and cooperation, as emphasized in the recently released defence policy update, *Our North, Strong and Free: A Renewed Vision for Canada’s Defence*. In doing so, we make connections between cyber, air, and people power.

Train and Plan: Preparing for Crisis Scenarios

There are several measures that militaries can take to anticipate and prepare for major cyber attacks. These measures may include conducting exercises that simulate military systems being compromised. As early as 1997, the US Department of Defense (DoD) conducted their first such exercise, *Eligible Receiver 97*, in which a National Security Agency (NSA) red team attempted to infiltrate the US Indo-Pacific Command's networks.²⁹ Although the results proved catastrophic for the defenders, the exercise nevertheless helped identify various areas of cyber vulnerability within the DoD and demonstrated several ways to harden their defences. Such practices have since become increasingly common,³⁰ and take on a variety of forms.

These exercises are frequently practiced on an annual basis, and can include multinational cooperation, bring together mainly cyber specialists, and aim to simulate the active defence of a network against hypothetical hostile actors. Other types of exercises involve "traditional" forces who practice their ability to operate in the context of cyber attacks, with the goal of cultivating a conventional unit's digital resilience. France, for instance, is increasingly conducting such training in "digitally degraded conditions" to better prepare units to carry out a mission even when certain technologies are rendered unavailable or unusable.³¹

Exercises combining digital and traditional approaches can be particularly useful because they bring together cyber specialists and conventional forces personnel, and train units to synchronize their operations with cyber protection and remediation efforts. Several authors define this kind of synergy as "mission assurance," whereby an organization's mission capability is safeguarded by specific processes in the event of a system failure.³² For example, in early 2024, the French Air Force simulated a cyber attack (and the restoration) on a *Phénix* refueling and transport aircraft's onboard system,³³ bringing together aviators and cyber defence personnel as part of the major annual DEFNET exercise.³⁴ In such cases, the aim is not only to train a command to switch back to legacy technologies (in the manner of 2034), but also to practice confidently identifying the systems that remain trustworthy and those that seem compromised, and assessing the viability and speed of their restoration to operational status.³⁵ In other words, such exercises create opportunities to simulate and train in the *Observe* and *Orient* phases of the OODA loop in the context of cyber attacks.

Additionally, these types of exercises can help a military develop another important tool of resilience: contingency plans. Pre-established procedures can stipulate the appropriate actions in a crisis scenario where technological capabilities are degraded. In the air domain, the US Air Force is currently testing navigation methods based on the analysis of anomalies in the earth's magnetic field to help its pilots find their way even if their GPS is neutralized.³⁶ These are only a few examples of procedures that

“ Like a jigsaw puzzle, the coherence of a military organization depends not only on the presence of all the pieces, but also on their appropriate position within the ensemble.”

can be devised and deployed in the event of a cyber attack. These types of responses, however, should be a part of comprehensive contingency plans, including ensuring that personnel have a minimum level of training in using alternative or "low tech" methods. When properly designed and disseminated, such plans can facilitate the *Decide* and *Act* phases of the OODA loop. These plans can serve to provide tested and potentially viable options for commanders and ensure that tasked personnel have the necessary information for implementation.

Organize: Keeping Your Friends Close

Another set of measures that can increase an air force's resiliency to cyber threats relates to its organizational and bureaucratic structure: specifically, to the place occupied by cyber defence personnel within that structure. Like a jigsaw puzzle, the coherence of a military organization depends not only on the presence of all the pieces, but also on their appropriate position within the ensemble. The challenge in this case is to ensure that the "cyber pieces" of an air force are arranged in such a way as to be able to react effectively and efficiently in the event of a crisis.

As in many organizations, a major challenge lies in the fact that cyber defence specialists and units often remain a peripheral support element of military organizations, isolated from decision-making centres. Field commanders and cyber defence specialists do not often collaborate and may not really *know* each other professionally. To make matters more complicated, the two groups may have different educational backgrounds and ways of communicating about operational problems, and thus may not *understand* each other. As Michael Hayden, former US Air Force General and later NSA Director, laments: "After a few sentences, the cyber briefer often sounds vaguely like Rain Man to many of the seniors in the room. With a few more sentences, most are convinced that he is."³⁷ Speaking the same language and being able to switch between languages may prove useful in bridging gaps in strategic and operational planning.

This gap is especially problematic because cyber threats can produce major effects on the trust that militaries place in technologies without nuance about the interconnections



Tactical Air Control Party (TACP) personnel coordinates information between the aircrafts and Joint Terminal Attack Controller (JTAC) to make a successful air drop, taken on June 23, 2026 at Primrose lake, Alberta.

Photo: Corporal Connie Valin, Canadian Armed Forces photo

and complexities embedded within digital-physical systems. A component of this trust is based in part on the confidence that “traditional” military personnel place in the cyber specialists tasked with securing their systems.³⁸ To be sure, securing systems is not a function for cyber specialists alone – there is a broader role for commanders and their staff to play. In the military world, as in other contexts, it is easier to trust someone you know, and whose expertise you have already seen and experienced. More meaningful integration and interaction of an air force’s cyber personnel into its overall operations could be an organizational priority to consider, in addition to fostering mutually trusting relationships where commanders understand their dependence on cyberspace. Commanders would need to ensure that they and their staff (including the cyber specialists) play a role in the defence of systems. This cultivation of trust and expertise is especially important as many cyber attacks exploit human and technical vulnerabilities.

For instance, meaningful integration may involve setting up reciprocal learning mechanisms that enable personnel to better understand what cyber specialists do, how they think and work, and how this work fits into the strategic, operational, and organizational functioning of an air force. Other efforts may involve simply bringing cyber specialists physically closer to certain areas of operation. In the current war in Ukraine, for instance,

Ukrainian and Russian forces have reportedly started to position cyber teams closer to the frontline, to better coordinate with forward-deployed troops (this decision may be due in part to the importance of ensuring the effective operation of drones).³⁹ In addition to shortening the communication chain, bringing diverse teams together may help both cyber operators and traditional personnel to better understand each other’s needs and foster greater synergies.⁴⁰ Introducing this proximity or familiarity may thus contribute to streamlining the efficiency of the OODA loop process.

Inspire: Creating the Right Incentives

The isolation of cyber specialists is not only due to their position in the organizational chart, but is also rooted in organizational cultures that influence the way they are viewed by the military community. Whether army, navy or air force, military organizations maintain certain norms, ideas and traditions that they perpetuate over time.⁴¹ These specific cultures have a direct impact on the way organizations work; however, they can also contribute to issues relating to operational posture.

In an article, Rebecca Slayton explores how the persistence of the cult of the “warrior figure” directly contributes to the ostracization of cyber specialists in the US military.⁴² The warrior figure paradigm refers to an institutional reverence for

individuals from certain services, such as special forces or combat arms personnel, whose functions are perceived as more noble because they are closer to the martial ideal of the traditional soldier.⁴³ In the aviation domain, this logic applies particularly to the pilot figure, which is associated with an image of authority largely cultivated in popular culture.⁴⁴ As a result, these positions are often perceived to hold greater credibility in the military establishment to the detriment of branches seen as “less combative” and secondary, such as logistics or communications. There are practical implications of the cult of the warrior figure: for example, functions considered more prestigious are often guaranteed privileged access to certain positions or commands,⁴⁵ potentially making certain career choices more attractive than others.

Cyber specialists, who are not typically perceived as “real warriors,” may be negatively impacted by the perpetuation of the cult of the warrior figure. These negative impacts can include being more confined to menial roles, slowly climbing the institutional hierarchy, and being less likely to obtain certain prestigious commands.⁴⁶ Inevitably, this reality pushes many potential recruits towards other military functions or encourages experienced cyber specialists to join the civilian sector (where there are considerable opportunities in this domain).⁴⁷ In the United States, the US Air Force remains the service whose organizational culture has historically proved most welcoming to cyber specialists, perhaps due to a long standing “victory-through-technology” institutional mindset.⁴⁸ Yet, even in this seemingly successful case, the cyber-warrior status remains largely supplanted by the pilot as the ideal warrior figure. In a 2019 study, the RAND Corporation found that fighter pilots, followed by bomber pilots, remained by far the two most promising career paths for those wishing to climb the US Air Force hierarchy among the US military services.⁴⁹

If an air force aims to effectively deal with cyber threats in the future, then the status of cyber specialists needs to be elevated and paired with greater incentives to encourage members to embrace this vocation. This may involve reforming established recruitment, training, and retention mechanisms, or as Nicholas Romanow terms it, the “Cyber Talent Management Triad.”⁵⁰ Romanow argues that although military leaders understand the importance of cyber operations, there is a shortage of personnel to fill associated roles, and this may be because of workforce competition with the private sector and a military culture that is not attractive to the cyber community. One way to rectify this problem is to invest in developing strong cyber leaders and drawing on the military’s established service culture.⁵¹ The US Air Force recently launched a program aimed at accelerating the commissioning of cyber specialists.⁵² With a view to revising the traditional military career pipeline, one of the aims of this program is to reward cyber-related skills (relative to other conventional military experiences). Another is to make it easier for cyber professionals to attain a rank and pay that is comparable to related positions within the civilian sector.

As authors such as Max Smeets have shown, developing a military’s cyber capabilities requires properly combining a wide range of skills and people—and this goes beyond strictly technical personnel.⁵³ If human capital is important in maintaining the confidence of militaries in their technologies, and if human assets are deemed critical to the effective completion of the OODA loop process, then cyber personnel should feel encouraged and meaningfully engaged in this endeavour. In this case, the training and education of cyber personnel could be expanded to include cyber specialists, leaders and generalists. The bottom line is that all military personnel—particularly those in command positions—need to have the skills to understand their mission dependence on cyberspace and play their role in addressing cyber mission risk.

Conclusion

Maintaining confidence in digital technologies in the face of cyber threats must be paired with confidence in humans and their ability to work together. As we have shown, actively practicing cyber attack scenarios and developing contingency plans to deal with such situations help build and maintain confidence. Another approach is to focus on organizational structures with the aim of better integrating cyber specialists and establishing greater familiarity and synergy with other personnel. Shifts in organizational culture may also play an important role in confidence-building by creating greater incentives for individuals to embrace cyber-related functions.

“ Maintaining confidence in digital technologies in the face of cyber threats must be paired with confidence in humans and their ability to work together.”

In the recent defence policy update, the Department of National Defence details plans for implementing several technological innovations within NORAD, including in the domain of information and communication, stressing the need for command and control “to be digitalized to operate at machine speed.”⁵⁴ In this regard, Canada has begun adopting and integrating cloud-based command and control systems for Canada-based NORAD installations.⁵⁵ Although these new technologies provide opportunities for increased information flow, data collection, and analysis for enhanced situational awareness, they must be considered as a part of a system—or embedded within the loop with humans. Another important aspect to consider is that NORAD is a



Members of the Canadian Fleet Diving Unit (Atlantic) discuss with a member of the French Armed Forces about his explosive ordnance disposal (EOD) tool during the last day of EX NORTHERN CHALLENGE 2024, on October 9, 2024 in Keflavik Iceland.

Photo: Felix Chagnon

partnership based on interoperability and trusted cooperation. As such, confidence in information technologies is important; just as traditional personnel need to trust a cyber operator's capacity to secure their systems, the bi-national partners must promote and maintain trust in their ability to maintain the integrity of their

NORAD-related networks. Paying close attention to the human component of cyber may prove important in rectifying recruitment and retention issues within the Canadian Armed Forces.⁵⁶ Thus, the Canadian Armed Forces in general, and the Royal Canadian Air Force in particular, has a clear interest not only in ensuring that it remains an attractive employer for cyber professionals, but also in making the best possible use of the innovative people power it currently possesses in this domain.

While information technology is both a key component and a source of vulnerability for modern militaries, human and organizational factors represent critical safeguards for guaranteeing their operational capabilities. In this article, we sought to contextualize the problems associated with cyber within the air domain. The issues we raised are relevant for leadership in the Royal Canadian Air Force to consider both individually and jointly with the Canadian Army and Royal Canadian Navy. Long-term cybersecurity planning requires a whole-of-forces approach—not silos. We demonstrated that various instruments already exist, or are in development, and may be leveraged in a meaningful way. As the integration of emerging technologies becomes a priority area in continental defence and in other trusted cooperations,⁵⁷ allies will need to ensure that they are future-proofing technological and human capabilities to defend in unison. Faced with the risk of excessive techno-pessimism, air forces can therefore work towards maintaining confidence in their digital technologies by making sure they “keep humans in the loop.”

Notes

- 1 Elliot Ackerman, and USN Admiral James Stavridis (ret.), *2034: A Novel of the Next World War*. New York, Penguin, 2022.
- 2 For other examples of similar fictional scenarios, see P. W. Singer and August Cole, *Ghost Fleet: A Novel of the Next World War*, Houghton Mifflin Harcourt, 2015. For a critical perspective on the use of speculative fiction, see Col. Mark D. Jacobson, “The Uses and Limits of Speculative Fiction: Three Novels about a US-China War,” *Journal of Indo-Pacific Affairs*, August 2023, 1-10.
- 3 See Bruce Schneider and Tara Wheeler, “Hacked drones and busted logistics are the cyber future of warfare,” Brookings Institution, 4 June 2021. Originally found at: <https://www.brookings.edu/articles/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/>
- 4 Jonathan Beale, “Ukraine war: How old tech is helping Ukraine avoid detection,” *BBC World*, 3 May 2023. Originally found at: <https://www.bbc.com/news/world-europe-65458263>
- 5 For a discussion on the distinction and convergence of cyber and electronic warfare, see Ryan J. Worrell, *EW and Cyber Convergence: Beyond Information Warfare*, Air Force Fellows Program, 2020. Originally found at: <https://apps.dtic.mil/sti/pdfs/AD112357.pdf>
- 6 A note on terminology: in an aviation context, both drones and helicopters are examples of aircraft. There are different ways to classify drones based on national doctrine, such as unmanned/uncrewed/
- remotely piloted aircraft systems, and each comes with varying cyber vulnerabilities and characteristics. For more detailed distinctions between drone classification types, see Maj. Osman Aksu et al., *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, Joint Air Power Competence Centre, January 2021. Originally found at: <https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf>
- 7 Scott Peterson, Payam Faramarzi, “Iran hijacked US drone, says Iranian engineer,” *Christian Science Monitor*, 15 December 2011. Originally found at: <https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer>
- 8 Nick Waters, “The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria,” *Bellingcat*, 12 January 2018. Originally found at: https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_air_force/
- 9 Dan Black and Gabby Roncone, “The GRU's Disruptive Playbook,” *Mandiant Blog*, 12 July 2023 [updated: 3 April 2024]. Originally found at: <https://www.mandiant.com/resources/blog/gru-disruptive-playbook>
- 10 Mauro Gilli and Niklas Masuhr, “Drones enhance defences in the Ukraine war,” *Binding Hook*, 10 January 2024. Originally found at: <https://binding-hook.com/articles-hooked-on-trends/drones-enhance-defences-in-the-ukraine-war/>
- 11 See, for example, in Sam Skove, “Army puts drones front and center in unfunded wishlist,” *Defense One*, 22 March 2024; Sam Skove, “Army announces plan to help spread commercial drones across infantry units,” *Defense One*, 27 March 2024; Maxine Baen, “Army tests commercial satellite internet in pilot program,” *U.S. Army*, 28 February 2022. Originally found at: <https://www.defenseone.com/technology/2024/03/army-puts-drones-front-and-center-newly-obtained-budget-docs/395182/>, <https://www.defenseone.com/threats/2024/03/army-announces-plan-help-spread-commercial-drones-across-infantry-units/395260/>, and https://www.army.mil/article/254316/army_tests_commercial_satellite_internet_in_pilot_program
- 12 Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare*. Oxford University Press, 2022, 97-99.
- 13 For an overview of the military techno-solutionism paradigm, see Jon R. Lindsay, “The Technology Theory of Victory,” in *Information Technology and Military Power*. Cornell University Press, 2020, 13-31.
- 14 Christopher Coker, *Future War*, 2015, Polity Press, 171-172.
- 15 See Martin C. Libicki, “Cyberwar as a Confidence Game,” *Strategic Studies Quarterly* vol. 5, no. 1, 2011, 132-147.
- 16 For an overview of the work of John Boyd, see Robert Coram, Boyd: *The Fighter Pilot Who Changed the Art of War*, Little, Brown and Company, 2002.

- 17 Although the OODA loop's origins come from air power, the concept has increasingly become important across all traditional domains of warfare. For example, see Brian R. Price, "Colonel John Boyd's Thoughts on Disruption: A Useful Effects Spiral from Uncertainty to Chaos," *Journal of Advanced Military Studies*, vol. 14, no. 1, 2023, 98-117.
- 18 Pascal Venesson, "Fighting, Fast and Slow? Speed and Western Ways of War," in Sten Rynning, Olivier Schmitt, Amelie Theussen, *War Time: Temporality and the Decline of Western Military Power*, Brookings Institution Press, 2021, 211-229.
- 19 To be sure, the OODA cycle is not only about speed. As others such as Luft and Kollars argue, it is also about tempo and timing. See Alastair Luft, "The OODA Loop and the Half-Beat," *The Strategy Bridge*, 17 March 2020 and Nina A. Kollars, "War at Information Speed: Multi-Domain Warfighting Visions," in Sten Rynning, Olivier Schmitt, Amelie Theussen, *op. cit.*, 230-252. Originally found at: <https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat>
- 20 Joseph Henrotin and Stéphane Taillat, "Military Operations: What If Digital Technologies Fail on the Battlefield?," in Sten Rynning, Olivier Schmitt, Amelie Theussen, *op. cit.*, 275-291.
- 21 Daniel Moore, *op. cit.*, 186-200.
- 22 Shah Zahid Khan, Mujahid Mohsin, and Waseem Iqbal, "On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science*, no. 7, 2021, e507.
- 23 Eduard Kovacs, "BAE Releases New Cybersecurity System for F-16 Fighter Aircraft," *Security Week*, 14 October 2022. Originally found at: <https://www.securityweek.com/bae-releases-new-cybersecurity-system-f-16-fighter-aircraft/>
- 24 Kim Hartmann and Keir Giles, "UAV Exploitation: A New Domain for Cyber Power," *8th International Conference on Cyber Conflict: Cyber Power*, NATO Cooperative Cyber Defence Centre of Excellence, 2016, 205-221.
- 25 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say," *The New York Times*, 28 August 2019. Originally found at: <https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>
- 26 The US National Institute of Standards and Technology (NIST)'s Cybersecurity Framework is generally used to react to cyber incidents. The NIST Cybersecurity Framework includes Identify, Protect, Detect, Respond, and Recover, and the linkages between the framework and human-centric cybersecurity and organizational culture are further explored in forthcoming work by Csenkey and Furlong.
- 27 Jon R. Lindsay, *op. cit.*, 32-70.
- 28 Jon Lindsay, *op. cit.*
- 29 Fred Kaplan, *Dark territory: The secret history of cyber war*, New York, Simon & Schuster, 2016, 68-71.
- 30 For a more in-depth history of early cyber conflict, including and beyond ELIGIBLE RECIEVER, see Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013.
- 31 Comité d'éthique de la défense, *Avis sur l'environnement numérique des combattants*, ministère des armées, 13 April 2022. Originally found at: https://www.defense.gouv.fr/sites/default/files/tronc_commun/20220413_Comit%C3%A9_d%C3%A9thique_de_la_d%C3%A9fense_-_Avis_sur_l%27environnement_num%C3%A9rique_des_combattants.pdf
- 32 Brad Bigelow, "Mission Assurance: Shifting the Focus of Cyber Defence," *2017 9th International Conference on Cyber Conflict (CyCon)*, NATO CCD COE, 2017, pp. 1-12, <https://doi.org/10.23919/CYCON.2017.8240327>.
- 33 Airbus Defence and Space A330-200 Phénix Multi-Role Tanker Transport.
- 34 Commandement de la Cyberdéfense, *DEFNET 2024 : une cyberattaque simulée sur le plan de vol du Phénix*, Ministère des Armées, 29 March 2024. Originally found at: <https://www.defense.gouv.fr/comcyber/actualites/defnet-2024-cyberattaque-simulee-plan-vol-du-phenix>
- 35 Daniel T. Sullivan, Edward J.M. Colbert, Blaine E. Hoffman, Alexander Kott, "Best practices for designing and conducting cyber-physical-system war games," *Journal of Information Warfare*, vol. 17, no. 3, 2018, 92-105.
- 36 David Roza, "C-17 Tests Magnetic Navigation System That Works When GPS Doesn't," *Air & Space Forces Magazine*, 7 June 2023. Originally found at: <https://www.airandspaceforces.com/air-force-magnetic-navigation-gps/>
- 37 Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, Penguin Press, 2016, 147.
- 38 Diane Henshel, M. G. Cains, Blaine Hoffman & al., "Trust as a human factor in holistic cyber security risk assessment," *Procedia Manufacturing*, vol. 3, 2015, 1117-1124.
- 39 Gordon Corera, "Ukraine war: Cyber-teams fight a high-tech war on front lines," *BBC*, 5 September 2023.
- 40 *Ibid.* Originally found at: <https://www.bbc.com/news/world-europe-66686584>
- 41 Joseph Soeters, "Organizational Cultures in the Military," *Handbook of the Sociology of the Military*, Springer, 2018, 251-272.
- 42 Rebecca Slayton, "What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967-2018," *Texas National Security Review*, vol. 4, no 1, 2021.
- 43 *Ibid.*
- 44 See Michael Wayne Hankins, *The Cult of the Lightweight Fighter: Culture and Technology in the U.S. Air Force, 1964-1991*, doctoral dissertation, Kansas State University, 2018.
- 45 For a discussion of this dynamic in the aerial domain, see Michael R. Worden, *Rise of the fighter generals: the problem of air force leadership, 1945-1982*, Air University Press, 1998.
- 46 Josh Lospinoso, "Fish Out of Water: How the Military Is an Impossible Place for Hackers, and What to Do About It," *War on the Rocks*, 12 July 2018. Originally found at: <https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/>
- 47 Lee Lunn, "Cyber Operator: Are you sure you want to do that?," *The Blue Knight Review*, 2021. Originally found at: <https://www.cmrsj-rmcscj.forces.gc.ca/cb-bk/art-art/2021/art-art-2021-7-eng.asp>
- 48 Sarah P. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, doctoral dissertation, Harvard University, Graduate School of Arts & Sciences, 2019.
- 49 S. Rebecca Zimmerman, Kimberly Jackson, Natasha Lander, Colin Roberts, Dan Madden, Rebeca Orrie, *Movement and Maneuver: Culture and the Competition for Influence Among the U.S. Military Services*, RAND Corporation, 25 February 2019.
- 50 Nicholas Romanow, "Leadership, Culture, and the Military Cyber Workforce," *War on the Rocks*, 11 April 2024. Originally found at: <https://warontherocks.com/2024/04/leadership-culture-and-the-military-cyber-workforce/>
- 51 *Ibid.*
- 52 Air Force Recruiting Public Affairs, "Cyber Direct Commissioning Program enhancement to onboard future cyber officers," US Air Force, 19 April 2023. Originally found at: <https://www.af.mil/News/Article-Display/Article/3368057/cyber-direct-commissioning-program-enhancement-to-onboard-future-cyber-officers/>
- 53 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, Oxford University Press, 2022, 75-79.
- 54 Department of National Defence, *Our North, Strong and Free: A Renewed Vision for Canada's Defence*, 9 April 2024. Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html>
- 55 Maxime Cliché, *Canadian Air Defence Sector introduces new cloud-based command-and-control system*, North American Aerospace Defense Command, 26 January 2024. Originally found at: <https://www.norad.mil/Newsroom/Article/3657967/canadian-air-defence-sector-introduces-new-cloud-based-command-and-control-syst/>
- 56 Aaron D'Andrea, "Canada's military facing 'death spiral' on recruitment, minister says," *Global News*, March 7, 2024. Originally found at: <https://globalnews.ca/news/10341588/canadian-forces-recruitment-death-spiral/>
- 57 Kristen Csenkey and Nina Bindel, "Post-Quantum Cryptographic Assemblages and the Governance of the Quantum Threat," *Journal of Cybersecurity* vol. 9, no. 1, 2023, 1-14, <https://doi.org/10.1093/cybsec/tyad001>.



A sailor downloads data from a REMUS autonomous underwater vehicle for analysis while deployed on Operation OPEN SPIRIT with Fleet Dive Unit (Atlantic) in Lithuania, on May 14, 2025.

Photo: Master Corporal Mark Wanzel

Autonomous Weapons and Cognitive Extension

MAJOR ANDREW G. HOLT

Major Andrew G. Holt is currently Commandant of the 5^e regiment d'artillerie légère du Canada. He holds an M.A. in History and Philosophy of Science and Technology from the University of Toronto and a Master of Military Studies from Deakin University.

Countries are fast developing and fielding Lethal Autonomous Weapons System (LAWS). These weapons are debated in academic, legal, and policy realms where many raise ethical objections due to a perceived “accountability gap.” Such a gap could hinder prosecution of war criminals, threaten the moral conduct of war, and reduce respect for the Law of Armed Conflict.¹ Many focus on keeping LAWS under human control, but with no consensus on how this control is defined and how it can be exercised. The HEC, an increasingly popular view in contemporary cognitive science, provides a useful way to understand human control of LAWS. I first explore the ongoing LAWS debate and its failure to define human control. I then summarize the HEC and its application to human control of LAWS, looking at how humans interact with cognitive technologies generally, considering LAWS as cognitive artifacts, and comparing control of LAWS and human subordinates. I conclude that LAWS can extend cognition and be under human control even without immediate, conscious human intervention. Therefore, military processes such as training and issuing orders might allow commanders to exercise control of LAWS in ways that parallel control of human subordinates.

Vague Notions of Control

Academics have debated the ethical implications of LAWS for over a decade. Surveying this debate, most of them take positions that are skeptical of LAWS, if not outright opposed to their use. A common concern is the lack of human accountability for LAWS.² A minority of authors, such as Simpson and Muller, take a different view.³ They argue that responsibility rests with the commanders who armed and deployed the LAWS, and LAWS behaving unpredictably does not preclude their use. The debate is not merely academic but leads to calls for bans or limitations on LAWS based on a lack of human control.⁴

Various non-governmental organizations have taken strong positions on LAWS. The International Committee for Robot Arms Control advocates that we must act against the “pressing dangers that [LAWS] pose to peace and international security and to civilians in war.”⁵ The International Committee of the Red Cross (ICRC) made a submission to a meeting of the High Contracting Parties and Signatories to the Convention on Certain Conventional Weapons (CCW) focused on human control of LAWS stating that “it is essential that States develop common understandings on the elements and criteria of human control.”⁶ Even organizations peripherally interested in LAWS such as the Institute of Electrical and Electronics Engineers (IEEE) recommend that measures be taken to “help ensure there is meaningful human control of weapons systems.”⁷

States too have commented on the legal and ethical implications of LAWS, although stated positions may not be comprehensive nor aligned with actual state actions.⁸ Many of the articulated positions focus on human control of LAWS, but there is no consensus on what human control really means.⁹ The Chair of the Group of Governmental Experts proposed a working characterization of LAWS in 2025, but the ensuing debate shows that the issue of human control remains unresolved. Some parties still sought the qualification of “human control” with phrases such as “contextappropriate” or “meaningful,” but there was no agreement as “delegations reiterated their diverse positions shared during the [previous] exchanges.”¹⁰

Discussions of human control often reference a decision-action cycle or “loop.” Canada uses the “loop” terminology in official documents on LAWS, saying in the Canadian Army modernization strategy that “the requirement for a human in or on ‘the loop’ will remain for any application of lethal force.”¹¹ In 2013, Human Rights Watch articulated the following definitions:

- Human-in-the-Loop Weapons: Robots that can select targets and deliver force only with a human command;
- Human-on-the-Loop Weapons: Robots that can select targets and deliver force under the oversight of a human operator who can override the robots’ actions; and
- Human-out-of-the-Loop Weapons: Robots that are capable of selecting targets and delivering force without any human input or interaction.¹²

What constitutes “human command” or “oversight” in terms of time, space, and specificity? What about an autonomous weapon “commanded” to seek and destroy the largest target in a given area? Must human oversight be constant and real-time? Attempting to define human control by appealing to concepts such as “command” and “oversight” merely pushes the explanatory burden onto new terms. Some technical experts contend that the debate around LAWS remains “filled with a lack of technical literacy and emotional rhetoric.”¹³ Additionally, human oversight risks producing “automation bias” that Cummings argues can lead to new errors if human cognitive abilities are not considered.¹⁴

The ill-defined notion of human control frustrates progress in legal and ethical debates over LAWS. The ICRC notes that “there is general agreement among States that human control—be it qualified as ‘meaningful,’ ‘substantive,’ ‘appropriate,’ ‘sufficient’ or ‘effective,’ or ‘appropriate levels of human judgement,’ or ‘human involvement’—must be retained over weapon systems and the use of force.”¹⁵ This proliferation of adjectives reveals a lack of consensus and clarity. Bode and Heulss make the point that “[m]ultiple understandings of what meaningful human control implies present a complication.”¹⁶ Nations favourable to the development of LAWS thus question whether and how human control can be usefully defined, arguing that “it is doubtful whether criteria to determine a due level of ‘significance’ of human control over the machine could be developed.”¹⁷ Regulatory measures would seem impossible to implement based on a vague notion of control, let alone ones that can practically be applied in military operations.

To further complicate human control, LAWS can be autonomous in different ways and to different degrees.¹⁸ Retired U.S. Army officer Brian Cox proposes that we understand LAWS in terms of the degree of autonomy, what contribution that autonomy makes to their overall function, and their method of programming.¹⁹ Even in 2012, before many advancements in AI, the US DoD noted that “system autonomy is a continuum from complete human control of all decisions to situations where many functions are delegated to the computer.”²⁰ A 2017 report explores definitions of autonomy and describes weapon autonomy in terms of the capability accomplished autonomously.²¹ They find that a variety of systems (air defence, active protection, loitering munitions, etc.) can be autonomous in a variety of functions (mobility, targeting, health management, etc.).²²

It is useful, in light of the wide variety of LAWS, to focus my analysis on a particular type. Unpiloted aerial systems (UAS) or “drones” that are autonomous in the selection and prosecution of targets are the archetypal “killer robots” at the centre of LAWS debate. Discussion of such systems is not just hypothetical—a United Nations report indicates a possible first use of such LAWS in Libya in March 2020.²³ Ukraine has used UASs extensively in their ongoing war with Russia.²⁴ Some are carrying out attacks autonomously.²⁵ It is this type of system, with this high degree of autonomy in targeting, that I will consider in exploring how human control of LAWS might be understood through the HEC.

The Hypothesis of Extended Cognition (HEC)

Cognitive science and the philosophy of cognition offer a useful way to understand meaningful human control of LAWS. Examining how LAWS might extend cognition intersects an existing body of thought about AI, cognitive artifacts, and the HEC. LAWS make for a particularly interesting and ethically charged example of extended cognition that seems yet unexplored. None of the extant LAWS literature considers LAWS through the HEC. Suchman and Weber make a tantalizing reference to Knorr-Cetina's seminal *Epistemic Cultures*, and its implications for subject/object relations,²⁶ but go no further in exploring how LAWS and soldiers might be part of a cognitive system.²⁷ This is the gap I attempt to resolve. Before looking at LAWS specifically, it will help to give an overview of the HEC.

The HEC has an intellectual heritage going back decades. Clark and Chalmers argue that the human mind can and does extend into the physical, material world.²⁸ Their theory rests on functional parity between the roles of internal (neural) and external processes in cognition. They argue against attempts to bound the human mind based purely on where a cognitive process takes place. An alternative argument for the extended mind claim is that our tools often complement, rather than mimic or replicate, the cognitive processes of the biological brain.²⁹ Both arguments reach the same conclusion: that the mind resides not just in the brain. The physical machinery that realizes our cognitive processes and, indeed, our *minds*, includes more than just our neural processes. Our minds can and do sometimes extend into the tools we use, our notebooks, telescopes, hammers, laptops and so on. Although the HEC remains controversial, it is gaining popularity in cognitive science. As Heersmink notes, "The paradigm shift from conceptualizing the mind as a purely internal affair to seeing it as

embodied and shaped by and strongly connected to the environment is well under way."³⁰ I do not attempt to enter fully into the debate on the HEC; it is sufficient to have established that the HEC is a credible theory.

Under the HEC paradigm, LAWS could be understood as artifacts that can extend human cognition, or cognitive artifacts. Heersmink calls cognitive artifacts "human-made, material objects or structures that functionally contribute to performing a cognitive task."³¹ Authors such as Sienknecht have considered the integration of cognitive artifacts into war where these artifacts provide inputs to biological cognitive processes (such as an AI system that analyzes enemy movements and recommends to a human commander a pre-emptive strike).³² A LAWS would instead extend biological cognition into action. If the mind extends into LAWS, as the HEC allows, perhaps this extension remains under human control.

LAWS Extending Cognition

LAWS, as cognitive artifacts, can take on some of the cognitive tasks required to effect the intentions of their designers and operators. To understand how, we need to consider intentions in more detail. Intentions can be hierarchical, existing at various levels of abstraction. A human commander might deploy LAWS with the more abstract, or higher order, intention to disrupt enemy communications. A LAWS could analyze enemy radio traffic, construct a representation of the enemy communications network, and locate and destroy key nodes in it. It might do this by targeting the radios themselves, re-broadcast antennas, or perhaps the fuel that supplies their generators. While operating autonomously in terms of the selection and prosecution of particular targets, such a LAWS is still effecting a human intention. LAWS merely allow humans to focus their conscious intentions and thought at a higher level of abstraction. This is exactly the kind of complementary delegation of cognitive tasks that Heersmink argues characterizes an extended cognitive system: "The human brain develops in an information-rich environment and has to learn how to complement its shortcomings by using the functionalities of artifacts to perform cognitive tasks in such a way that it does not waste expensive internal resources."³³ Hernandez-Orallo and Vold speak of technologies that act as AI extenders, which exist "in a continuum between fully externalized systems, loosely coupled with humans, and fully internalized processes."³⁴ LAWS seem to fall on this spectrum, even without a human in or on "the loop."

An interesting property of advanced LAWS would be their transparency³⁵ to the commander employing them. This lack of conscious awareness may even make a case for understanding LAWS as cognitive extenders. Heersmink comments: "The use of artifacts can be conceptualized along a spectrum of expertise. The first time we use an artifact, it requires a lot of conscious, cognitive effort, but over time, we become better at using an artifact



HMCS VILLE DE QUÉBEC's CH-148 Cyclone, Avalanche, launches flares over the Atlantic Ocean while deployed on Op HORIZON, November 6, 2025.

Photo: Sailor First Class Kyle Maguire, MARPAC Imaging Services, CFB Esquimalt

and its use becomes more proceduralized.”³⁶ Philosopher Michael Wheeler argues that such transparency can be an indication of cognitive extension, but also a cause for concern.³⁷ If systems that extend our cognition become sufficiently transparent to us, we may no longer realize the ways in which their categorizations of the world do not match our own.³⁸ Wheeler writes:

“If a deep neural network application to which I am transparently coupled qualifies as part of my cognitive architecture and thus as part of me, then the classifications in question—classifications that unconsciously guide my behaviour—will be part of what I unconsciously believe to be the case, and thus presumably will have the same status as my more familiar, internally realized unconscious beliefs.”³⁹

His objection is that these machines “may routinely classify the world in ways at potentially damaging epistemic variance with our technologically unaugmented practices.”⁴⁰ This is especially concerning for LAWS employing AI that function as “black boxes” whose inner workings are unknowable to the user. He thus recommends that cognitive technologies be made deliberately non-transparent, similar to calls for keeping a human on the loop for LAWS.

Concerns about cognitive technologies are not new. Socrates worried that writing, as a cognitive technology, acts outside of meaningful human control, claiming: “And once a thing is put in writing, the composition, whatever it may be, drifts all over the place, getting into the hands of not only those who understand it, but equally of those who have no business with it; it doesn’t know how to address the right people, and not to address the wrong.”⁴¹ These words echo modern objections to LAWS interacting with the wrong people in unintended ways. If we accept that the intentions of an author are sufficiently embedded in a written composition that it does not need active human control as it propagates unsupervised into the world, there should be some parity in the degree and type of control we demand over LAWS. While the potential deadly effects of LAWS might limit direct comparison to civilian technology, LAWS are not the only technology whose failure poses a risk of death (i.e. bridges and automobiles).

The HEC, by allowing that the mind might extend into LAWS, calls into question any insistence that a biological brain must be “on the loop” for control. Increasingly, machine learning and AI will permit LAWS to effect not only a specific human intent, taking on a tiny share of cognition, but to effect a general or more abstracted human intent by taking on much more cognitive burden. Thinking of control merely in terms of immediate and active involvement of a biological human brain ignores how we routinely extend cognition into physical artifacts without surrendering control. The ICRC argues that “a weapon system with autonomy in its critical functions prevents the human commander or operator from making the judgements required by IHL [international



A member of The Royal Canadian Dragoons participates in an urban village attack scenario as part of the Basic Tactical Aviation Course (BTAC) at CFB Petawawa on April 4, 2022.

Photo: MCpl Laura Landry, Canadian Armed Forces

humanitarian law] [emphasis added].”⁴² The HEC allows, however, that the mind making these judgements *extends* into LAWS. Under the HEC, a military force could instantiate cognitive processes either in a biological human brain or the physical world, or some mix of the two.

Whether a LAWS carries out human intent may be more important than whether it is under direct and immediate human supervision. The United States 2018 submission to the CCW advances that idea by stating the following: “The key issue for human-machine interaction in the development, deployment, and use of emerging technologies in the area of lethal autonomous weapons systems is ensuring that, when it is necessary to use force, such force is used to effectuate the intentions of commanders and operators.”⁴³ Australia takes a similar view, stating that “the phrase ‘human control’ as used by some in the [Group of Governmental Experts] discussions does not adequately cover the plethora of practical controls or systems utilised by states and their militaries.”⁴⁴ Rather than mandating a human on the loop, Australia instead articulates their own nine-stage system of control applicable to all weapons, human-operated and autonomous.

Implications for Commanders

The autonomy of human subordinates does not entail that they are beyond the control of their commanders. Militaries do not require a commander on the loop watching a human subordinate and authorizing every specific action. James Kraska, of the US Naval War college, argues that there is no responsibility gap with LAWS, as commanders remain ultimately responsible for all the means of warfare that they employ in achievement of their military objectives.⁴⁵ Granted, LAWS and human subordinates are not identical, with human subordinates having accountability and moral agency that LAWS do not.⁴⁶ Despite that disparity, control

of human subordinates might still inform control of LAWS in at least two respects: orders and training.

Commanders give orders that direct the actions of their human subordinates. These orders can include both a task and a purpose. Orders typically refer to the higher commander's intent, including contextual information that allows human subordinates to act in accordance with these intentions, even if the situation changes so drastically that their assigned task is no longer appropriate. A commander's intentions can be effectuated in ways that are opaque to that commander without a loss of control. Even in modern, professional armies with advanced communication, there are examples where subordinates have acted unexpectedly, with no oversight by superiors, to achieve a higher intention.⁴⁷ Such military units are not considered out of control, so why should LAWS be? When appropriate, orders can contain a variety of formal constraints (rules of engagement, boundaries, timings, and reporting requirements) that could have direct analogies for LAWS. There is a growing body of literature that seeks to "assess the trustworthiness of humans and automated systems to decide whether to rely on a respective trustee to perform a certain task."⁴⁸ A human commander might have adequate instrumental trust in LAWS to apply a form of mission command and accept unpredicted actions that still achieve the intent.

The analogy to training humans provides a way to look at human-LAWS interaction and control of LAWS employing AI or machine learning. LAWS using generative models are "trained" on a sample of inputs simulating what they might encounter in operations. This training would provide opportunities for confirmation and validation of LAWS very similar to what is done for (human) military units prior to deployment. Although Verbruggen argues that "there are no techniques in existence that can validate and

verify AI, to ensure that the systems will function as specified and avoid unpredictable behaviour."⁴⁹ This understanding of validation, seeking full predictability, is much stricter than what is applied to human organizations. The Canadian Army (CA) defines confirmation as "an assessment of how well a tactical organization has mastered a particular [battle task standard]."⁵⁰ Validation serves to "verify that a [collective training] program has adequately prepared units or formations to perform the operational tasks to meet specified CA goals."⁵¹ Both are a responsibility of commanders.

A well-trained LAWS might be under control even if it operates outside of human conscious awareness and decision-making similar to the unconscious human execution of drills. In certain military disciplines, reactions and behaviours requiring immediate response are drilled and trained to a point of near unconsciousness. With sufficient practice, this manipulation of a weapon for potentially lethal ends becomes almost transparent. Wheeler describes this as transparency of tool use, writing:

"When we skillfully manipulate equipment in a hitch-free manner, we have no conscious apprehension of the items of equipment in use as independent objects, that is, as something like identifiable bearers of determinate states and properties. Thus, to use Heidegger's most-quoted example, while engaged in trouble-free hammering, the skilled carpenter has no conscious recognition of the hammer, the nails, or the work-bench, in the way that one would if one stood back and thought about them."⁵²

A weapon could be similar to the skilled carpenter's hammer. Being freed from the need to focus consciously on *how* to manipulate the weapon, the human consciousness can focus on more abstract cognitive tasks like what effect this manipulation aims to achieve (i.e. suppression of an enemy sniper). If the training of a human to respond unconsciously does not entail an abdication of meaningful control over lethal force, could the programming or training of an artificially intelligent LAWS also provide control, even if the LAWS operates outside human conscious awareness? Removed from individual decisions about the selection and prosecution of targets, a military commander is not divorced from the application of force, nor from responsibility, but rather is liberated to consider it at a higher level.



Members of HMCS Charlottetown conduct a proficiency flight of the ships Sparrow Uncrewed Aerial System (UAS) during operational patrols in the Mediterranean Sea as Flagship of Standing NATO Maritime Group Two (SNMG2) while deployed on Operation REASSURANCE on July 8, 2024.

Photo: Aviator Gregory Cole, Canadian Armed Forces Photo

Conclusion

The notion of human control of LAWS is complex, and examining it through the HEC can lead to useful ideas and policy. Treating LAWS as cognitive artifacts opens new ways of understanding and exercising human control of LAWS. LAWS that extend human cognition may be under control even without immediate, conscious intervention by a biological human brain. Openness to experimentation and training with LAWS might produce unpredicted benefits for the CAF. Carter and Nielsen argue that generative models can enable artificial intelligence augmentation, writing:

“[Generative models] can be used to explore and discover, to provide new representations and operations, which can be internalized as part of the user’s own thinking. And while these examples are in their early stages, they suggest AI is not just about cognitive outsourcing. A different view of AI is possible, one where it helps us invent new cognitive technologies which transform the way we think.”⁵³

If LAWS are trained in conjunction with their human counterparts, the solutions LAWS employ may in fact provide novel ideas and new cognitive tools that expand the range of human thought. This promise should not be ignored.



Commodore Matthew Coates, Commander of Standing NATO Maritime Group Two (SNMG2), discusses capabilities with drone operators from HMCS Charlottetown upon completion of flying operations with the “Sparrow” Uncrewed Aerial System (UAS) while conducting operational patrols in the Mediterranean Sea while deployed on Operation REASSURANCE on July 9, 2024.

Photo: Aviator Gregory Cole, Canadian Armed Forces Photo

Notes

- Mariarosaria Taddeo, *The Ethics of Artificial Intelligence in Defence* (New York: Oxford University Press, 2024), 181.
- Robert Sparrow, “Killer Robots,” *Journal of Applied Philosophy* 24, No. 1 (2007): 62-77.
- Thomas Simpson and Vincent Müller, “Just War and Robots’ Killings,” *Philosophical Quarterly* 66, No. 263 (2016): 302-322.
- Ingvild Bode and Hendrik Huelss, *Autonomous Weapons Systems and International Norms* (Kingston: McGill-Queen’s University Press, 2022), 9.
- International Committee for Robot Arms Control. Originally found at: <https://www.icrac.net/about-icrac/> (accessed 3 November 2025).
- International Committee of the Red Cross, “The Element of Human Control,” *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (2018): 1. Originally found at: https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/hcp-meeting/documents/ICRC_WP3.pdf (accessed 3 November 2025).
- IEEE, “Reframing Autonomous Weapons Systems,” *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*, 113. Originally found at: https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/lead_reframing_autonomous_weapons_v2.pdf (accessed 3 November 2025).
- Michael Schmitt and Sean Watts, “The Decline of International Humanitarian Law Opinion Juris and the Law of Cyber Warfare,” *Texas International Law Journal* 50, No. 2-3 (2015): 191.
- Australia, “Australia’s System of Control and Applications for Autonomous Weapon Systems,” *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (2018). Originally found at: <https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2019/gge/Documents/GGE.2-WP2.pdf> (accessed 3 November 2025).
- Group of Governmental Experts on Emerging Technologies, “Chair’s summary - First 2025 session of the GGE on LAWS,” *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (2025): 7. Originally found at: [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2025\)/CCW-GGE.1-2025-WP1_-_Chair's_summary.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2025)/CCW-GGE.1-2025-WP1_-_Chair's_summary.pdf) (accessed 6 October 2025).
- Canadian Army Headquarters, *Advancing with Purpose: The Canadian Army Modernization Strategy*, (2020): 52. Originally found at: https://publications.gc.ca/collections/collection_2021/mdn-dnd/D2-438-2021-eng.pdf (accessed 3 November 2025).
- Human Rights Watch, *Losing Humanity: The Case Against Killer Robots*, (2012). Originally found at: <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots> (accessed 3 November 2025). Although dated, this typology remains influential and was used by Vincent Boulanin and Maakie Verbruggen in *Mapping the Development of Autonomy in Weapon Systems* (Stockholm: Stockholm International Peace Research Institute, 2017), 26, to characterize systems in their dataset.
- Mary Cummings, “Lethal Autonomous Weapons: Meaningful Human Control or Meaningful Human Certification? [Opinion],” *IEEE Technology and Society Magazine* 38, No. 4 (1 December 2019): 20-26. Originally found at: https://publications.gc.ca/collections/collection_2021/mdn-dnd/D2-438-2021-eng.pdf (accessed 28 Feb 2025).
- Missy Cummings, “Automation Bias in Intelligent Time Critical Decision Support Systems,” *American Institute of Aeronautics and Astronautics 1st Intelligent Systems Technical Conference* (20-22 September 2004). Originally found at: <https://arc.aiaa.org/doi/10.2514/6.2004-6313> (accessed 9 July 2025).
- International Committee of the Red Cross, “The Element of Human Control,” *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (2018): 1.

- Originally found at: https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/hcp-meeting/documents/ICRC_WP3.pdf (accessed 6 October 2025).
- 16 Ingvild Bode and Hendrik Huelss, *Autonomous Weapons Systems and International Norms* (Kingston: McGill-Queen's University Press, 2022), 159.
 - 17 The Russian Federation, "Russia's Approaches to the Elaboration of a Working Definition and Basic Functions of Lethal Autonomous Weapons Systems in the Context of the Purposes and Objectives of the Convention," *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (2018): 3. Originally found at: <https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/documents/GGE.1-WP6-English.pdf> (accessed 6 October 2025).
 - 18 Noel Sharkey, "Staying in the Loop: Human Supervisory Control of Weapons." In *Autonomous Weapons Systems: Law, Ethics Policy*, edited by N. Bhuta, S. Beck, R. Geiß, H.Y. Liu and C. Kreß, (Cambridge: Cambridge University Press, 2016), 27.
 - 19 Brian Cox, "Why Binding Limitations on Autonomous Weapons Will Remain Elusive," *Articles of War*, (2022). Originally found at: <https://lieber.westpoint.edu/binding-limitations-autonomous-weapons-elusive> (accessed 6 April 2022), further articulated by the author at a presentation to The Canadian National Group of the International Society for Military Law and the Law of War on 24 Feb 2022, Ottawa (broadcast virtually on MS Teams).
 - 20 DoD Defense Science Board, *The Role of Autonomy in DoD Systems*, (2012): 4. Originally found at: <https://apps.dtic.mil/sti/pdfs/ADA566864.pdf> (accessed 28 Feb 2025).
 - 21 Vincent Boulanin and Maakie Verbruggen, *Mapping the Development of Autonomy in Weapon Systems* (Stockholm: Stockholm International Peace Research Institute, 2017), 20.
 - 22 Vincent Boulanin and Maakie Verbruggen, *Mapping the Development of Autonomy in Weapon Systems* (Stockholm: Stockholm International Peace Research Institute, 2017), 36.
 - 23 United Nations, *Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council*, (2021): 17. Originally found at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/037/72/PDF/N2103772.pdf?OpenElement> (accessed 25 October 2025).
 - 24 Jon-Wyatt Matlack, Sebastian Schwartz, and Oliver Gill, *Ukraine's Drone Ecosystem and the Defence of Europe: Lessons Lost Can't Be Learned* (London: LSE, 2025). Originally found at: <https://www.lse.ac.uk/ideas/Assets/Documents/2025-04-05-DRONES-MatlackSchwartzGill-FINAL-WEB-03.pdf> (accessed 7 October 2025).
 - 25 David Hambling, "Ukraine's AI Drones Seek and Attack Russian Forces Without Human Oversight," *Forbes* (17 Oct 2023). Originally found at: <https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/> (accessed 21 September 2024).
 - 26 Lucy Suchman and Jutta Weber, "Human-Machine Autonomies," in *Autonomous Weapons Systems: Law, Ethics Policy*, edited by N. Bhuta, S. Beck, R. Geiß, H.Y. Liu and C. Kreß, (Cambridge: Cambridge University Press, 2016), 98.
 - 27 Karin Knorr-Cetina, *Epistemic Cultures: How the Sciences Make Knowledge* (Cambridge: Harvard University Press, 1999).
 - 28 Andy Clark and David Chalmers, "The Extended Mind," *Analysis* 58, (1998): 7-19.
 - 29 Richard Heersmink, "Dimensions of Integration in Embedded and Extended Cognitive Systems," *Phenomenology and the Cognitive Sciences* 14 (2015): 577-598.
 - 30 Richard Heersmink, "Varieties of Artifacts: Embodied, Perceptual, Cognitive, and Affective," *Topics in Cognitive Science* 13 (2021): 574.
 - 31 Heersmink, "Varieties of Artifacts," 580.
 - 32 Dennis Muller, Maurice Chiodo, and Mitja Sienknecht, "Integrators at War: Mediating in AI-assisted Resort-to-Force Decisions," (12 January 2025): 7. Originally found at: https://www.researchgate.net/publication/387976034_Integrators_at_War_Mediating_in_AI-assisted_Resort-to-Force_Decisions (accessed 7 October 2025).
 - 33 Heersmink, "Dimensions of Integration," 582.
 - 34 Karina Vold and José Hernández-Orallo, "AI Extenders: The Ethical and Societal Implications of Humans Cognitively Extended by AI," *AIES '19 Session 9: Human and Machine Interaction*, (2019): 507.
 - 35 Note that "transparency" as used by Wheeler refers to a tool being outside the user's conscious awareness. This differs from the use of transparency in the AI literature where it refers to the ability to understand the interior workings of an AI.
 - 36 Heersmink, "Varieties of Artifacts," 577.
 - 37 Michael Wheeler, "The Reappearing Tool: Transparency, Smart Technology, and the Extended Mind," *AI & Society* 34 (2019): 857-866.
 - 38 Wheeler, "The Reappearing Tool," 857-866.
 - 39 Wheeler, "The Reappearing Tool," 864.
 - 40 Wheeler, "The Reappearing Tool," 864.
 - 41 H. Fowler, *Plato: Phaedrus*, (Loeb Classical Library, 1971): 275e.
 - 42 International Committee of the Red Cross, "The Element of Human Control," *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (2018): 2. Originally found at: https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/hcp-meeting/documents/ICRC_WP3.pdf (accessed 6 October 2025).
 - 43 U.S.A., "Human-Machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems," *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (2018): 7. Originally found at: <https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/documents/GGE.2-WP4.pdf> (accessed 6 October 2025).
 - 44 Australia, "Australia's System of Control and Applications for Autonomous Weapon Systems," *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (2018): 5. Originally found at: <https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2019/gge/Documents/GGE.2-WP2.pdf> (accessed 6 October 2025).
 - 45 James Kraska, "Command Accountability for AI Weapon Systems in the Law of Armed Conflict," *International Law Study* 97 (2021): 408-445.
 - 46 Daniele Amoroso and Guglielmo Tamburrini, "Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues," *Current Roboethics Report* 1 (2020): 189.
 - 47 Douglas MacGregor, *Warrior's Rage: The Great Tank Battle of 73 Easting* (Annapolis: Naval Institute Press, 2009).
 - 48 Markus Langer, Cornelius J. König, Caroline Back, and Caroline Hensing, "Trust in Artificial Intelligence: Comparing Trust Processes Between Human and Automated Trustees in Light of Unfair Bias," *Journal of Business and Psychology* 38 (2023): 493.
 - 49 Maaike Verbruggen, "No, Not That Verification: Challenges Posed by Testing, Evaluation, Validation and Verification of Artificial Intelligence in Weapon Systems," in *Armament, Arms Control and Artificial Intelligence: The Janus-Faced Nature of Machine Learning in the Military Realm*, edited by Thomas Reinhold, and Niklas Schörnig, Springer International Publishing AG, 2022, *ProQuest Ebook Central*. Originally found at: <http://ebookcentral.proquest.com/lib/cvlibrary-ebooks/detail.action?docId=7108384>. Created from cvlibrary-ebooks on 2025-07-09 18:36:43, p. 242.
 - 50 Commander Canadian Army, *TRAINING FOR LAND OPERATIONS*, (2014): 6-3-11.
 - 51 Commander Canadian Army, *TRAINING FOR LAND OPERATIONS*, 6-3-12.
 - 52 Wheeler, "The Reappearing Tool," 859.
 - 53 Shan Carter and Michael Nielsen, "Using Artificial Intelligence to Augment Human Intelligence," *Distill* (2017). Originally found at: <https://distill.pub/2017/aia> (accessed 3 November 2025).