National Defence / Défense nationale

CANADIAN ARMED FORCES

#SALMANQADIR

THE DEPARTMENT OF NATIONAL DEFENCE
AND CANADIAN ARMED FORCES

ARTIFICIAL INTELLIGENCE STRATEGY

Canada

FOREWORD

Foreword from the Deputy Minister and the Chief of the Defence Staff

We live in an artificial intelligence (AI)-enabled world. When we unlock our smartphones using facial recognition, search the internet, accept suggestions provided by autocorrect, or interact with a chatbot or virtual assistant, we are engaging with AI. These technologies are now so ubiquitous that we forget they are AI—and that none of them existed a mere twenty-five years ago.

Just as it has rapidly transformed the activities of our daily lives, AI is also transforming the defence environment. It has enabled new operational and corporate capabilities to help us continue to meet our obligations to protect and defend Canada and Canadians, but also new risks against which we must protect them. Furthermore, AI is not a standalone technology, but part of a broader and even more transformative technological revolution brought about by the convergence of data and digital with AI.

The DND/CAF Artificial Intelligence Strategy (AI Strategy) commits the Defence Team to becoming AI enabled by 2030, in line with our goals for an overall digital transformation by that date. This is an ambitious objective, but one that we must meet. We stand at a technological inflection point. Our allies are moving ahead rapidly in their commitments to AI and its adoption. We must move now to ensure that we can continue to share a common operating picture with them, sensing, deciding, and acting at a pace enabled by AI, so that we do not lose our credibility and relevance as a fighting force.

The technology will not wait for us to act. With every day that passes, it is becoming more accessible to our competitors and potential adversaries at a lower cost, and the convergence of quantum and AI is rapidly approaching. Falling behind now in our adoption of AI will risk the loss of our operational advantage.

Becoming AI-enabled also offers us the opportunity to meet the call for modernization and reconstitution: to become better stewards of the resources with which Canadians have entrusted us, while delivering improved results. It offers the opportunity to meet the expectation of our personnel that they will work and fight in the same digital, AI-enabled world in which they live. At the same time, we must ensure that our use of AI lives up to what Canadians and our people expect of us. We must ensure that it meets their expectations for safe, responsible, and ethical implementation while upholding an inclusive and diverse culture.

The AI Strategy provides a vision and direction for the development and integration of AI and automated decision systems in the Defence Team. The operational capabilities and requirements of the Department of National Defence and the Canadian Armed Forces (DND/CAF) in the modern security environment are at the heart of this approach, guiding the prioritization and need for this Strategy. The Strategy conveys our intent and direction to our people, to our partners in the Government of Canada, academia, and industry, and to our allies.

Today, we face a world more insecure and dangerous than at any time since the end of the Cold War. We must expect that demand on the Canadian Armed Forces both domestically and internationally will only increase. We must modernize rapidly in order to meet the challenges of tomorrow. The imperative is clear, and the urgency is real—but we are equal to it. We must move—and move now—to become an AI-enabled organization.

General Wayne Eyre

Chief of the Defence Staff
Canadian Armed Forces

Bill Matthews

Deputy Minister
Department of National Defence

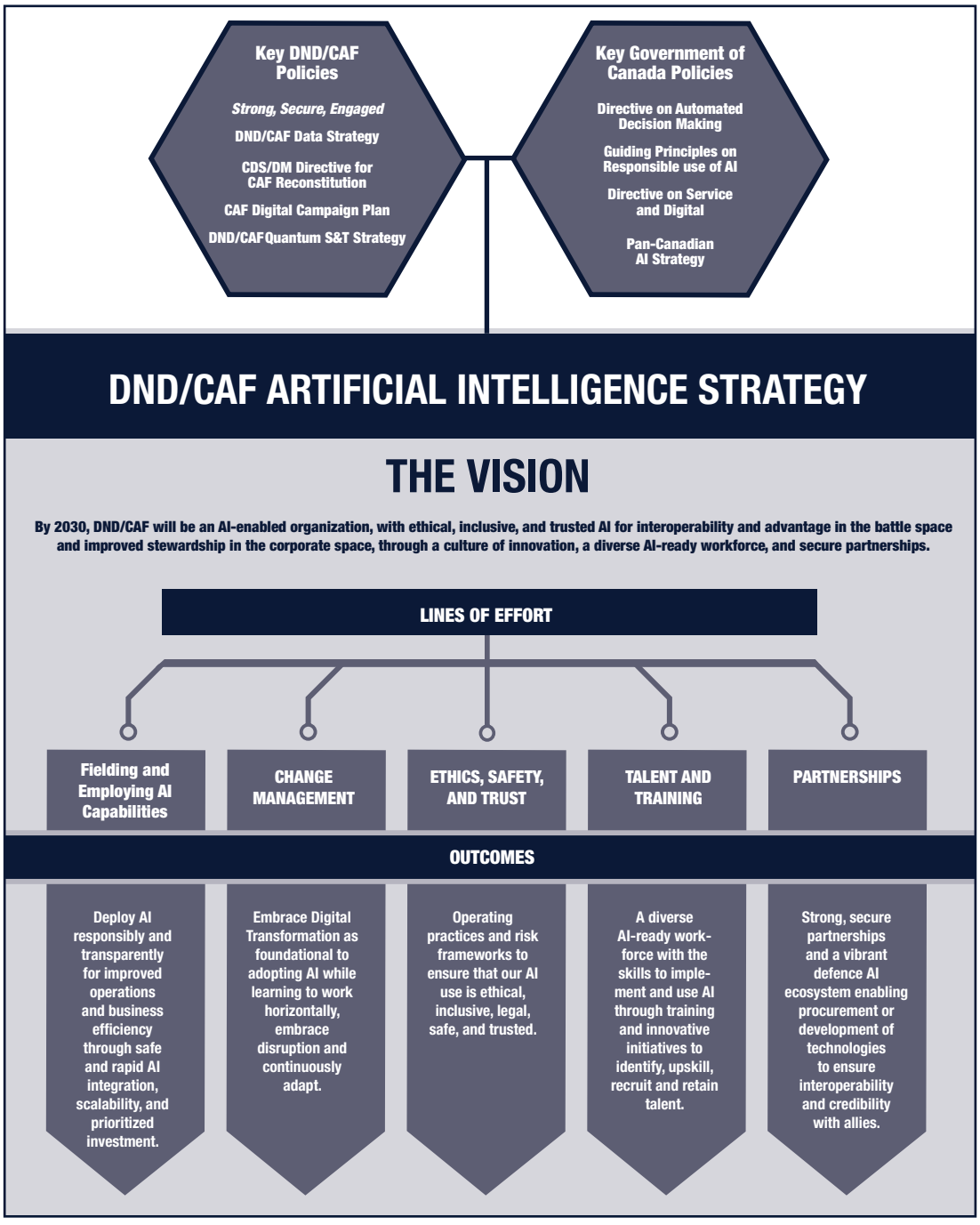
TABLE OF CONTENTS

INTRODUCTION

STRATEGIC ALIGNMENT

The AI Strategy aligns with the Department of National Defence and Canadian Armed Forces (DND/CAF) policies and strategies on modernization and digital transformation, and with its commitment to apply Gender-Based Analysis Plus (GBA Plus) in the development and execution of its operations, policies, and programs.

In particular, the AI Strategy is to be read and implemented in conjunction with the Data Strategy and the Data Strategy Implementation Plan (DSIP) to ensure that a strong data management foundation will underpin AI implementation. This Strategy also aligns with applicable Canadian and international law, and with Government of Canada policies and guidelines for the use of digital and AI.



CONTEXT

AI is a powerful tool that has the potential to disrupt and transform both the conduct of military operations and the management of corporate functions. At all levels of command, algorithmic technologies are enabling new capabilities which are faster and more powerful than those deliverable by human agents alone. Enabled by ever-growing volumes of data, these technologies can enhance situational awareness and decision support across all domains. At the operational level, AI and the use of machine learning (ML) tools can augment human capabilities to monitor, predict, target, and accelerate the capacity to detect and respond to an adversary. AI can also be used to automate logistics and predict the need for repairs, improving operational readiness. At the organizational level, advanced analytics allow organizations to see and understand themselves and their processes better, identifying potential efficiencies of cost and time. AI-augmented automation can take over repetitive tasks, freeing personnel to take on more complex and demanding activities.

Leveraging AI is central to the priorities of DND/CAF, and its allies and adversaries. Canada's defence policy, Strong, Secure, Engaged, and the DND/CAF Data Strategy describe a desired end state in which data is leveraged to provide increased efficiency and an information advantage in military operations and corporate applications. Analyzing and interpreting large volumes of data is now well beyond the capacity of human agents alone and achieving this end state will require assistance from AI and other automated decision systems. Defence priority areas such as NORAD modernization, National Defence Operations and Intelligence Centre (NDOIC), and Joint Intelligence, Surveillance, and Reconnaissance (JISR) envisage the incorporation of AI and related technologies in the development of a modernized Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) spine. Canada's defence partners are rapidly defining their own approaches to AI; while China has announced plans to achieve global AI dominance by 2030.

But DND/CAF is not yet positioned to adopt and take advantage of AI. At present, AI initiatives within DND/CAF are fragmented, with each command and environment addressing AI independently. AI maturity varies across DND/CAF, with pockets of significant expertise and lower levels of skills and capacity elsewhere. No roadmap exists to move the organization towards leveraging AI effectively to ensure that investments are coordinated and appropriately governed, or to develop the capabilities, attitude, and skills to implement AI effectively, safely, and responsibly. Without such an approach, DND/CAF risks missing many appropriate opportunities to responsibly employ AI in the conduct of CAF operations, thus failing to realise its many benefits, including operational advantage over potential adversaries. Equally, it risks creating or perpetuating harms through algorithmic or data biases and unanticipated system effects, and the loss of opportunities to improve the business of defence and our corporate stewardship through the capabilities enabled by AI.

To move forward on AI, DND/CAF requires an AI Strategy to guide and cohere efforts towards enabling operations and defence business with AI. This AI Strategy lays out five lines of effort to accelerate the adoption of responsible AI within DND/CAF. The lines of effort described within this document have associated activities to advance implementation in the near term, including the creation of a DND/CAF AI Centre (DCAIC) as a centre of excellence for DND/CAF. This AI Strategy will be followed by an implementation directive laying out responsibilities and timelines for Strategy implementation.

MACHINE LEARNING CAN PREDICT SYSTEM FAILURES ON ROYAL CANADIAN NAVY SHIPS

AI capability needed: Identify impending failure in ship systems using sensor data

AI techniques used: Supervised and unsupervised machine learning, predictive analytics

Value added by AI: Prediction of system failures using Integrated Platform Management System (IPMS) sensor data

Failures in machines can lead to tragic events on board ships, putting sailors in danger and the success of sea operations at risk. Therefore, being able to predict failures in marine systems and to replace equipment before failure occurs offers major user benefits for the Royal Canadian Navy (RCN).

For that reason, in 2018, the RCN reached out to the Defence Research and Development Canada Centre for Operational Research and Analysis (CORA) to explore whether data from IPMS could be used to predict failures on board RCN ships. IPMS was installed during a mid-life refit to help monitor propulsion, electrical, and damage control machinery. Its network of sensors on each ship records data every 0.5 seconds, giving trillions of data points on the ship's condition and performance.

CORA took three years of data from four systems aboard select RCN ships—the propulsion diesel engine, the diesel generator, the shaft-line and controllable reverse pitch propellers, and the gear box. It aggregated the data on a five-minute scale and categorized the data as being either normal or preceding a failure. CORA then used corrective maintenance logs and operational deficiency reports to corroborate the failure events.

CORA used this data to train autoencoder neural network algorithms to pinpoint system anomalies associated with failure events. The initial results showed that the algorithms could predict the need for corrective maintenance up to a week in advance 75 percent of the time.

The system's performance was not perfect, with false positives also produced, but the initial results were promising enough to warrant further testing.

WHAT IS AI?

Defining AI is challenging and there is no single accepted definition. The technologies included within the term are constantly shifting and expanding as the science of AI advances while many older technologies once included are no longer considered AI at all.

For DND/CAF, AI is considered the capability of a computer to do things that are normally associated with human cognition, such as reasoning, learning, and self-improvement.

Even the most advanced AI today is narrow AI: tools focused on specific tasks such as pattern recognition, classification, task optimization, and anomaly detection. Experts disagree on when or even if general AI, which can perform any cognitive task as well as or better than a human, will ever be developed. General AI systems are therefore outside the scope of this Strategy. Augmented Intelligence is also a subset of AI in which AI and ML technologies, such as virtual assistants, which will assist humans by analyzing queries and providing relatable data to assist the requestor in making better decisions.

ML is currently the dominant technique in AI, both in terms of widespread application and effectiveness. Rather than defining rules to obtain a result as conventional software does, ML uses past data to identify patterns which allow it to optimize for a predefined goal. When functioning properly, ML tools can help anticipate future needs, events, trends, and risks, allowing users to yield significant efficiencies in areas such as maintenance, logistics and inventory management. However, the effectiveness of ML depends on access to sufficient, relevant and high-quality data, without which the tool's outputs will be unreliable. As a result, the quantity and quality of the data used for ML applications is a key priority for DND/CAF.

Generative AI is a subset of ML which can produce a wide variety of novel content, such as images, videos, audio, text, code, and 3D models, in response to user prompts. It does this by identifying the structure and patterns of vast quantities of existing data, and then using these patterns to generate novel outputs with similar

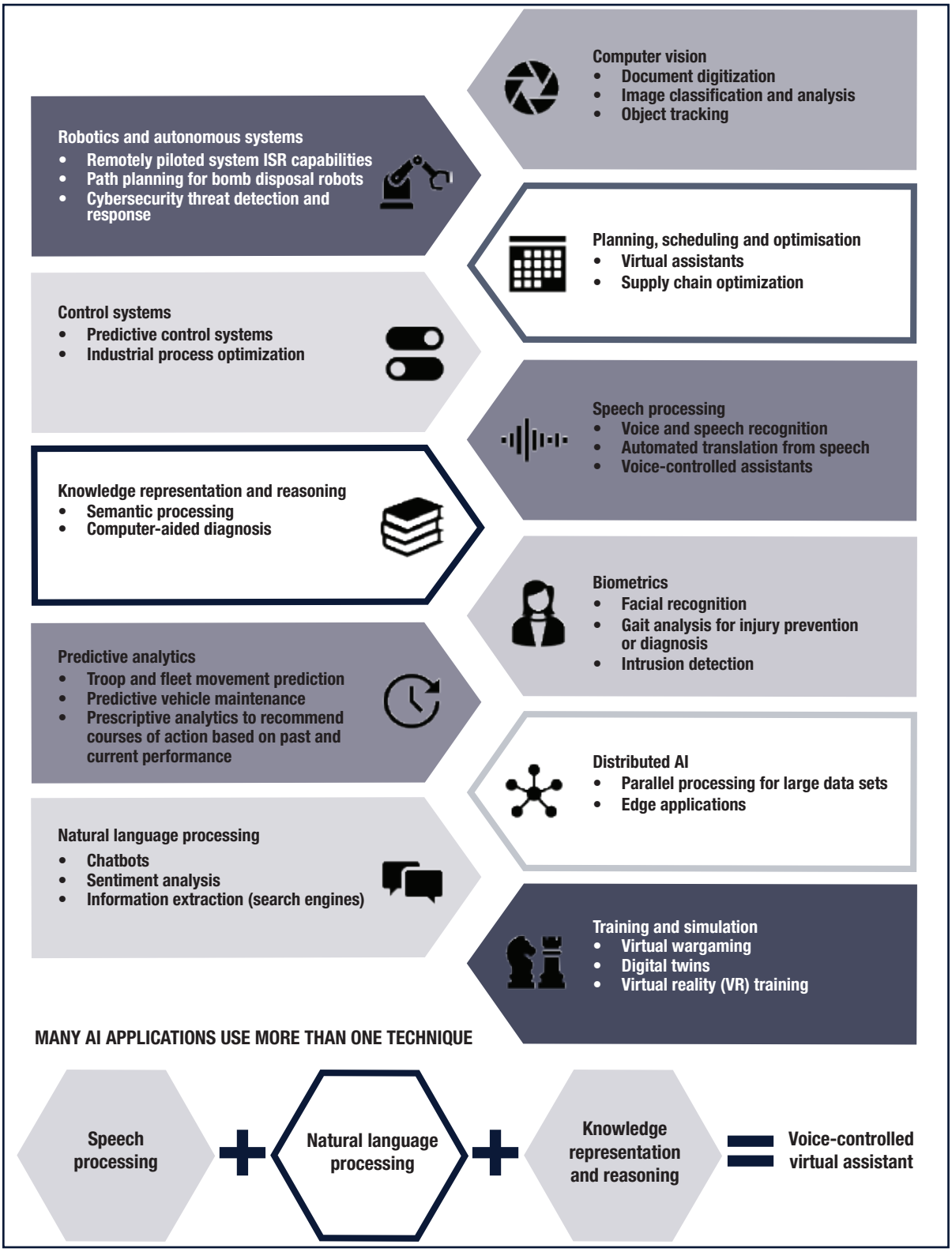
characteristics. Generative AI outputs can be complex, highly realistic, and at times, indistinguishable from human-authored content. Recent breakthroughs in the field, particularly in large language models and image generation, have significantly advanced the capabilities of generative AI, opening new possibilities to use the technology to solve complex problems, including assisting in scientific research.

In popular culture, AI is often characterized as a competitor to human intelligence; however in practice, the two types of intelligence are highly complementary. In many domains, human intelligence supported by AI can deliver results that are superior to those achieved separately. For example, AI can undertake tasks that are repetitive or require high levels of precision and sustained attention. This leaves human personnel free to undertake the tasks at which they excel, especially those requiring judgement, creativity, initiative, and a grasp of the strategic landscape.

	HUMAN INTELLIGENCE	ARTIFICIAL INTELLIGENCE
Strengths	• Can innovate, imagine, and create without data • Understands conversation, emotion and humour • Can draw conclusions with little data • Can anticipate possible but uncertain outcomes and understand the implications of a decision • Can quickly incorporate new data sources and adapt actions • Highly energy efficient	• Almost unlimited computational capacity • Almost unlimited sensor inputs, with signal speed close to speed of light • Can be networked with other AI/computers for direct communication • Can be updated and scaled • Excels at tasks requiring sustained attention • No biological limitations of fatigue, hunger, or mortality • Learning can be transferred at end of system life
Weaknesses	• Limited working and long-term memory and computational capacity • Limited sensory inputs and slow signal speed • Cannot be reconfigured, updated, upgraded, or scaled • Communicates indirectly through language and cannot be networked to other humans or machines • Struggles to maintain attention and accuracy in monotonous conditions • Cognitive biases affect rationality and decision quality • Error prone: performance degrades when tired, hungry, or stressed • No transfer of knowledge at end of life	• Cannot learn across problems • Can be trained to recognize but not understand language, emotion • Requires data to learn, and currently learns poorly with limited data • Cannot incorporate facts outside the training data into decision making • Cannot understand the implications of decisions • Unable to judge the importance or significance of the problem it is asked to solve • Subject to data and algorithmic bias • Highly energy inefficient

Along with its promise, AI and its use of data brings about challenges and responsibilities. If an AI model is trained on biased data, the resulting prediction may reflect and perpetuate those biases, leading to real world harms. Further, AI predictions based on past data may not represent the future, failing to foresee low-probability but high-impact events. Finally, AI's data usage can also pose privacy and security risks, especially when it involves personally identifiable or otherwise sensitive government information. Consequently, the outputs of AI must always be analyzed against expert human judgement and the constraints and expectations of the organization, with an awareness of AI's limitations. On the road to AI enablement, it is critical for the Defence Team to establish and uphold ethical, equity, and security requirements for the use of AI.

AI CAPABILITIES



GUIDING PRINCIPLES

To successfully implement this Strategy by 2030, DND/CAF will be guided by the following principles:

- ***We must put in place the data and technical enablers of AI***. DND/CAF must implement the ***DND/CAF Data Strategy*** to support access to the high-quality, well-governed, well-architected, and appropriately classified data on which AI depends. DND/CAF must also create the secure and interoperable digital infrastructure required to support the application layer, including investments in the cloud infrastructure and security required to scale AI. This must be done with full consideration of Data Centric Security, an essential aspect of data and cyber security. DND/CAF must allocate financial and human resources to defining, implementing, and managing a secure space for AI application development.

- ***We must embrace and actively manage change.*** We must overcome resistance to change and institutional skepticism by demonstrating the value proposition of AI. We must build on the lessons, results, and momentum of existing initiatives, learning from best practice and our own experience. Although leveraging AI is a process rather than an end, involving ongoing experimentation with emerging techniques and applications, we must also commit to fund projects to scale so that we reap the full benefits of our innovation.

- ***We must recognize that AI is a means to solve a problem, not an end in itself***. DND/CAF must maintain informed and realistic expectations of what AI can deliver, avoiding an inappropriate reliance on automated decision systems. We must create the conditions for success by ensuring that problems are appropriately defined and that the necessary data, technical and human foundations are present. We must approach AI wisely, choosing it where there is a reasonable expectation that its results will be superior to existing methods, with a clear understanding of its risks. Finally, we must view AI as a catalyst for a broader and more fundamental digital transformation of the business of defence, and an opportunity to imagine and design systems that are more transparent, equitable, and just.

- ***We must deploy AI to augment, not replace, human action and decision making.*** Regardless of the tools, defence will always be a fundamentally human endeavour. We must ensure appropriate human involvement in AI systems, calibrated to their risk and impact. While this involvement may be minimal for low-risk applications, applications involving lethal force must always retain the human in the loop. Where possible, decisions and outcomes should be explainable and transparent, with appropriate accountability mechanisms in place.

- ***We must not adopt AI without the processes demanded by AI.*** Advances in technology have compressed innovation cycles from decades to months. To succeed with AI, DND/CAF must be prepared to move at that pace. We must evolve our systems and processes to enable us to procure, develop, test, and field AI safely, securely and at the speed of relevance while working horizontally to achieve our AI goals. This will require that we incorporate agile project management, recognize software as a military capability as much as hardware, and integrate software agility and upgrades into our process to enable capability improvement. It will require that we solve critical process and capacity constraints for infrastructure and data. In short, we must be willing to accept fundamental disruption to benefit from AI.

- ***We must calibrate our AI investments and ensure alignment to government priorities.*** DND/CAF must identify and prioritize areas for strategic investment in AI that will enable the development or amplification of key capabilities for priority missions, especially where AI can be a combat multiplier. Wherever possible, these should build on DND/CAF and Canada's existing strengths in AI and defence to maximise the return on our investment and ensure sovereign AI foundations and capabilities. In calculating the return on investment; however, we must factor in the hidden costs of AI, including the costs of data and computation, and the impact on wider Canadian Government priorities and goals.

LINES OF EFFORT

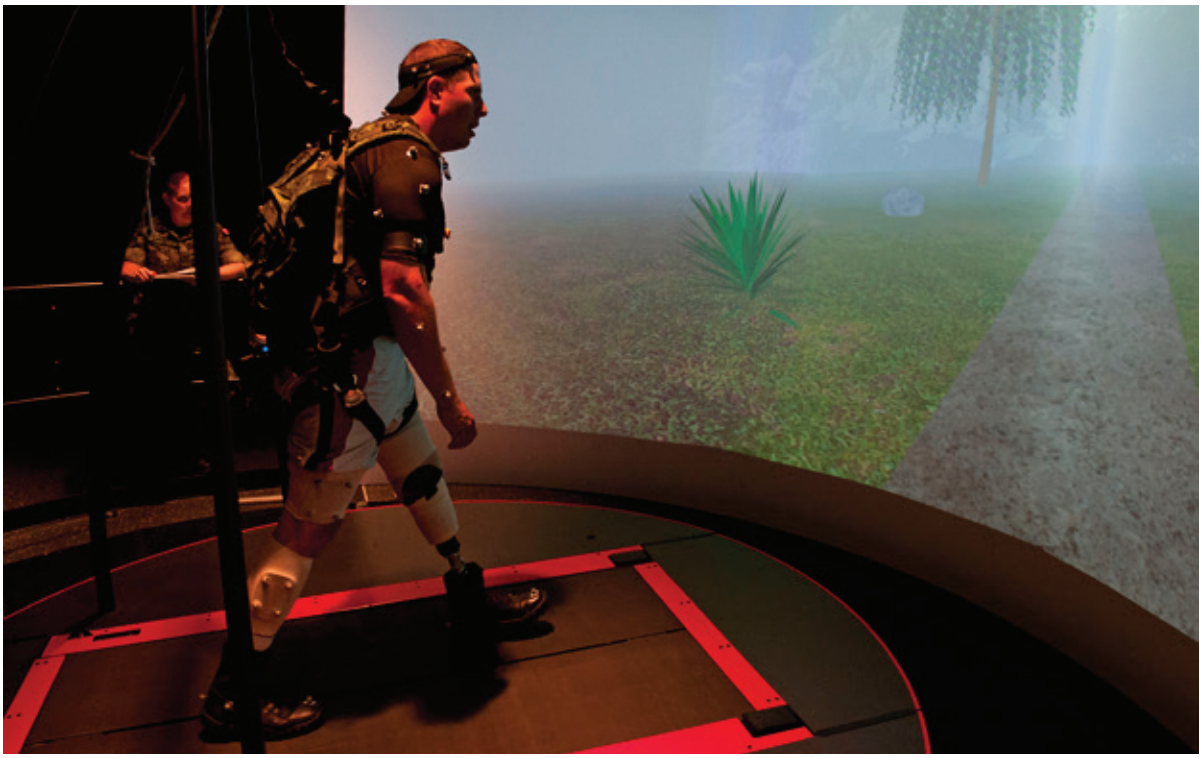
LINE OF EFFORT 1: FIELDING AND EMPLOYING AI CAPABILITIES

The challenge

AI will be foundational to Defence modernization. The fusion of AI, networking, predictive and prescriptive analytics, ML, and robotics will be critical to equip DND/CAF and digitally transform defence. This will provide the capabilities needed to ensure operational superiority over our adversaries and technological parity and interoperability with our allies. The sheer volume, diversity and complexity of data produced by modern sensors has already overwhelmed the capacity of human analysts to process and interpret it. This problem will only increase as legacy systems are upgraded and replaced.

Despite this, we are only beginning to identify the AI-enabled capabilities we need and how to achieve them. Although DND/CAF possesses areas of AI expertise, its maturity, integration, and implementation are still at an early stage of development. Our current efforts are divided across environments and commands, with each element approaching AI enablement and capabilities separately, and hampered by data quality issues. Effectively fielding and employing AI capabilities will require a concerted, collaborative effort until DND/CAF is more digitally advanced and technologically proficient.

AI is beginning to proliferate into many facets of operations and the business of Defence. DND/CAF needs to be fully aware of the benefits and challenges of AI to aid in the responsible, transparent use of this powerful tool while minimizing the potential risks. Any AI that is employed by the CAF on operations, including AI and AI-enabled information obtained from allies or partners, will likely receive scrutiny and this requires additional attention by operational authorities to ensure they are aligned with Canadian law and policies.



The accountability and responsibility of AI systems may crosscut existing structures within and outside DND/CAF. Further, because of their application to national defence, some DND/CAF use cases may fall outside the policy provided by the Treasury Board of Canada Secretariat, and the gap between the development of AI and legislative and policy coverage will widen further. Where laws and policies do not apply, or have not yet been developed, L1s must work collaboratively to develop appropriate guidance to ensure the responsible and transparent use of AI. We must balance testing, validation and risk mitigation with the agility required to adopt AI technology at the speed of relevance.

What we must do

We must responsibly and transparently use AI to provide capabilities for operations and to solve key business problems. We must quickly build the internal expertise and experience to assess, advise, field, and manage AI tools and applications for operations and the business of defence. We must also provide collaborative mechanisms to support the use of AI during operations, whether the technology originates within DND/CAF or is shared with us by our allies or partners.

We must align our investments in AI with existing priorities. Fielding and employing AI capabilities will not happen all at once. DND/CAF will therefore prioritize the fielding of AI systems that support commitments within the Departmental Plan to augment decision-making and processes, and to improve the capabilities and performance of our personnel by freeing them from repetitive or dangerous tasks. Initially, efforts will be focused on enabling CAF operational capabilities as well as efforts that support the business of defence, particularly those that support CAF reconstitution and readiness. These capability areas can be directly linked to Departmental Plan priorities to overcome existing DND/CAF challenges. Although these efforts will need to be collaborative and horizontally executed at the lowest level, effective governance will be required to ensure they are coordinated, prioritized, and implemented within DND/CAF plans and priorities. Regular assessments will be required to monitor and report on progress.

We will identify or develop tools to support the rapid and safe design, procurement, integration, and scaling of AI. The initial focus will be on tools to support the evaluation of AI for operations but will also include problem definition tools to help identify when problems are amenable to an AI solution, guidelines to assist project teams and support staff in procuring them, and both quantitative and qualitative risk assessment tools to identify and mitigate risks to privacy, security, safety, human rights, and GBA Plus considerations.

HOW WE WILL DO THIS

1. ***Establish an internal DND/CAF AI Centre (DCAIC).*** Like those of our defence partners (below) the DCAIC will act as a hub of AI expertise and an accelerator for experimentation, testing, evaluation, and fielding AI. This Centre will establish AI adoption processes for developing and onboarding AI technologies in collaboration with key stakeholders and provide support and advice to all to enable safe and responsible AI adoption and use.

2. ***Conduct an AI maturity assessment and develop metrics for measuring our progress and performance.*** An assessment of current levels of AI implementation and capacity will establish a baseline against which the success of the AI Strategy and our own AI enablement can be measured using key performance indicators (KPI).

3. ***Develop supporting mechanisms and tools to support AI growth.*** DND/CAF will need standards, guardrails, checklists and internal processes to enable the rapid and safe use, design, procurement, integration, risk management and scaling of AI. The DCAIC will lead this effort in collaboration with all stakeholders.

4. ***Develop governance for AI to align resources and goals.*** Options for effective governance of AI will be developed and considered as part of the overall governance structure within DND/CAF. This governance will ensure that efforts remain aligned to existing priorities, policy and capacity.

A DND/CAF AI CENTRE (DCAIC)

Within the last five years, three of Canada's closest defence partners have established centres of excellence to accelerate AI experimentation and scaling across the Defence enterprise. In 2018, the U.S. Department of Defense (DoD) established the Joint AI Center to accelerate AI development and deployment, and to support the implementation of the DoD AI Strategy. The Australian Defence AI Centre was established in the same year, and the U.K. Ministry of Defence launched its own Defence AI Centre in April 2022 to serve as an accelerator of concepts to operationalize and scale across defence, with key pillars focusing on robotics, digital, and responsible AI. In addition, AI accelerators for defence were endorsed as best practice by the U.S. National Security Commission on Artificial Intelligence in its final report in 2021.

To reach its AI goals, DND/CAF needs an AI Centre of its own. Working cross-functionally with teams currently exploiting or experimenting with AI, the Centre would serve as a hub of AI expertise for the Defence Team. It would identify and support the integration of capabilities developed by industry, academia, or allies, facilitate the creation of a common repository of AI applications, techniques, and data, develop common AI applications to meet shared challenges across the organization, and support local AI development within the commands and environments. It would also provide guidance on related issues required for successful AI implementation, such as policy, ethics, GBA Plus, procurement, and training. The DCAIC would work with stakeholders and users from the Warfare Centres, DRDC research centres, Joint Operations Fusion Lab, Innovation for Defence Excellence and Security (IDEaS), and other Defence Team branches (L1s), to coordinate the setting of organizational priorities for AI, ensure internal interoperability and economies of effort and scale, and help to ensure that successful initiatives were able to be appropriately scaled. It would also collaborate with Five Eyes partners and NATO allies on standards and guidelines for interoperability and responsible use. It would also have an outreach role with academia, industry and civil society, and with other government departments and review bodies. In this role, it would help foster the growth of the Canadian defence AI ecosystem, identify and promote the uptake of promising solutions within DND/CAF, and provide an environment in which defence and security challenges could be discussed.

LINE OF EFFORT 2: CHANGE MANAGEMENT

The challenge

Leveraging AI broadly across the enterprise will require change and that change will need to be supported, monitored, and managed. The transformative and rapidly advancing nature of AI requires that DND/CAF actively fosters the expansion of AI across the enterprise by being more agile, innovative, inclusive, solution driven, and risk tolerant. These changes are needed not only to fully leverage AI, but they are also being demanded of the organization through its commitment to digital transformation, and by the rapid and often disruptive security, technical, industrial, and social changes currently taking place worldwide.

Our current structure, processes and incentives do not fully support the required change. Our focus and spending have been directed towards military hardware, and our structures and processes reflect that. Our processes limit our capacity to procure or collaborate with others to develop AI, hampering experimentation and innovation. Data and information are often disparate and unavailable, and business owners are unwilling to share it because of security concerns. Traditional styles of leadership have tended to vest authority at the top and reward conformity rather than innovation. This must change if we are to successfully implement AI.

What we must do

We must embrace digital transformation as foundational to adopting AI. Digital transformation and adopting AI will require our organization to accept a greater tolerance for risk and failure. AI research and development is high risk and often involves trial and error before success is achieved. We will need to embrace experimentation and appropriate risk-taking and provide protected environments in which this can be done safely. We will need to be tolerant of failing forward and early in the pursuit of experimentation and discovering what is possible.

We must learn to work horizontally. Working within commands or organizational silos will not yield the results we are seeking. Instead, we must learn to work collaboratively across the enterprise. Wherever possible, we should seek

joint capacity and capability to reduce domain-specific stovepipes. Given the complexity of the technology, we must take an intersectional, multidisciplinary, and cross-functional approach to project design and problem solving. This horizontal, cross-functional approach will enable senior leadership to empower decision-makers at all levels with the authority required to identify and implement AI initiatives while embracing a diversity of perspectives as a strength rather than a weakness.

We must embrace disruption. AI is disruptive, and we must be prepared for the fact that adopting AI will bring changes—sometimes profound ones—to our structures and ways of working. We must embrace this. We must be willing to challenge orthodoxies and embrace novel methods of achieving objectives, making use of the innovation, diversity, agility, and excellence present within the Defence Team.

We must adapt continuously. In the past, changes to technology brought about episodic disruptions to culture, processes, and roles followed by periods of stasis. With the advent of AI and related technologies, innovation cycles have been dramatically compressed. We will need to be prepared to move to a state of continuous adaptation, alert for new developments and ready to integrate them into our corporate and battle space. In particular, the cost of experimentation, development, fielding and sustainment of AI will need to be built into defence capability development plans. DND/CAF will require greater nimbleness and agility in our supporting processes in both military and civilian branches, including the necessity of continual reviewing and updating of training and delegated authorities to maximize horizontal action of thought and purpose. Finally, our training system needs to fully incorporate AI whenever possible to enable quicker, more adaptive, individual, and collective force generation systems.

HOW WE WILL DO THIS

1. ***Vest decision authorities for AI at the lowest appropriate level to encourage innovation.*** Although centres of excellence will be critical to AI success, local development is equally vital to encourage the development of solutions to meet specific needs. Consequently, leaders must be empowered with the authority to experiment and innovate within a horizontal, cross-functional environment while selecting and respecting the AI adoption processes, developed by the DCAIC, best suited to their specific circumstances.

2. ***Identify and change incentives.*** We must identify the ways in which incentives such as promotions, recognition or career structures can be used effectively to encourage the kinds of behaviours required for AI adoption at scale. We will need to increase incentives to innovate and lower the costs and risks of failure by providing protected environments for early failure and adopting a no-blame approach.

3. ***Include AI as a defence capability enabler that requires funding.*** If it is to realize its AI aspirations, DND/CAF must commit to fund the technical, digital, and data enablers and the research, engagement, and staff AI requires. These enablers must be costed and those costs built into program and project planning and development from the inception. New programs, projects, and initiatives will be required to assess the potential implementation of AI, and existing capabilities will be assessed to determine the need to integrate AI enhancements into legacy systems.

4. ***Identify, prioritize, and address key impediments to responsibly procuring, developing, testing, validating and certifying, fielding and decommissioning AI.*** In addition to funding and supporting AI enablers, we must also ensure that key AI governance bodies have the authority and resources to minimize policy and process barriers to development, implementation, and adoption.

POLICIES AND STANDARDS CHATBOT

AI capability needed: AI chatbot which can provide answers to questions on military dress policy

AI techniques required: Natural language processing

Value proposition: Improved policy comprehension and compliance among CAF members

Policy documents contain vital information, but they can be long and difficult to navigate for personnel looking for answers to specific questions. In response to this challenge, the Digital Transformation Office's Data Science team has produced a working prototype which could help CAF members find answers to questions about military dress policy.

Built from scratch by the Data Science team using industry-standard open-source technologies, the chatbot enables users to input questions in natural language and receive references to the passage the system believes contains an answer to their question, with links to relevant policies. The prototype also contains features allowing users to provide input on the relevance of the response to improve the accuracy of the tool and send feedback to the team on their experience. According to its developers, the chatbot is over 90 percent accurate in its responses to questions. This chatbot has only been deployed in test environments as a proof of concept. This class of AI tool holds promise to answer questions on other types of policies.

LINE OF EFFORT 3: ETHICS, SAFETY AND TRUST

The challenge

Canadians expect us to procure, develop and implement AI that is legal, inclusive, ethical and safe. The use of AI within Defence, particularly in applications related to the use of force, will be closely scrutinized to ensure it is in line with our shared values and Canadian and international law. Our legitimacy in the use of military force comes from the consent of the people we serve, and we must ensure we retain this legitimacy in the use of AI. Failing to do so may risk loss of public trust, reputational damage, the perpetuation of discrimination and bias, and poor morale among personnel.

AI may involve risks to human rights, privacy, and safety. While DND/CAF faces real risks if it fails to keep pace with adversaries in AI, it must also remain cognisant of the potential human rights risks of this technology. AI is a human product, with human biases and flaws embedded in its data, algorithms, models, and accompanying processes. A growing body of incidents demonstrate that AI can fail or cause harm through these flaws, producing discriminatory decisions that cannot be explained or audited. AI can also cause harms through a lack of testing, evaluation, and oversight, and can create new data protection and privacy risks. In a national defence context involving highly classified information, the risks from AI also include leaks, cyber-attacks, inadvertent exposure of intelligence equities, manipulation, and bias.

Ethical, safe AI will be central to ensuring our people trust and use it. The willingness of members and employees to use AI applications, especially in the battle space, will depend on their having confidence in the safety and ethics of these technologies and their effects and decisions. Consequently, widespread adoption will require that we demonstrate that safety to our people. AI decisions, behaviours, and performance must be as consistent, reliable, and trustworthy as possible.

What we must do

We must accord equal billing to ethical, security, and technical concerns. Identifying, mitigating, and addressing sources of both unintended harm and malicious activities must be part of the lifecycle for AI systems, and should be accorded equal importance with the resolution of technical problems.

We must embed ethical, equity, and security requirements into every stage of project and system lifecycles, from design, development, validation and certification, procurement, and deployment of AI systems to their eventual decommissioning. Decisions to augment human decision-making or human judgement-based tasks must be justified and documented, with mechanisms in place to ensure the ultimate decisions are traceable and explainable, and with appropriate accountability measures in place. All personnel involved in developing, procuring, and using AI must clearly understand their role, level of responsibility and authority with respect to these projects and systems. Projects must also incorporate GBA Plus throughout the AI lifecycle to ensure solutions respond to the needs of diverse groups and experiences, contribute to positive outcomes, and do not create harms resulting from algorithmic or data bias.

We must make AI ethics clear, consistent, and actionable. Many organizations have created AI ethics principles, but most have failed to communicate how to put them into practice. Those involved in AI system design, development, and delivery need clear steps to follow to integrate ethical approaches into their process. We must create tools to enable AI project teams to identify risks and mitigation strategies and adopt sound ethical operating practices at every stage of the project life cycle.

HOW WE WILL DO THIS

1. ***Ensure that any new AI or AI-enabled technology is developed and implemented in accordance with applicable laws, policies and guidelines.*** These include Canadian and international law, applicable regulation, and Government of Canada policies such as the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems, Guide on the use of Generative AI, and Directive on Automated Decision-Making. It will also include DND/CAF commitments to integrate GBA Plus into operations, policies, and programs, risk management, and other related DND/CAF instruments such as the targeting cycle, rules of engagement, and security and information management policies and guidelines. DND/CAF will also respond to guidance from external review bodies such as the National Security and Intelligence Committee of Parliamentarians (NSICOP), the National Security and Intelligence Review Agency (NSIRA) and the Office of the Privacy Commissioner (OPC).

2. ***Develop AI ethics principles, risk frameworks and operating practices for the AI life cycle***. Drawing on federal and international best practice, DND/CAF, led by the DCAIC will develop a set of ethics principles, operating practices, and a risk framework for AI to embed best practice into the entire AI lifecycle. This framework will identify risks and impacts so they can be mitigated and ensure a level of transparency, comprehension, and human involvement appropriate to the risk and impact involved. In alignment with the ***Directive on Automated Decision Making*** and Algorithmic Impact Assessments, it will consider risks to the rights, health or well-being, and economic interests of individuals or communities affected by the system, including discriminatory effects arising from data or algorithmic bias, and any risks to the ongoing sustainability of an ecosystem. As technology and best practice develops, we will continue to update this framework and these practices to ensure they remain evergreen.

3. ***Integrate standards and develop requirements for ethical, safe, inclusive, and trustworthy AI systems in defence and security.*** These include existing international and domestic ethical standards as well as applicable standards on, data, digital trust, and identity management. We must also encourage adoption and operationalization of AI principles in third party vendors and collaborate with key allies and partners to continue to develop and integrate national and international standards for data and AI ethics, such as the NATO Principles of Responsible Use of Artificial Intelligence in Defence.

4. ***Collaborate with internal and external partners on ethical, safe, and trusted AI.*** DND/CAF will leverage Canada's public sector and civil society leadership in AI ethics, and internal expertise from the Defence Ethics Programme, Director Gender Equality and Intersection Analysis (DGEIA) and others to support the responsible, safe and inclusive use of AI technologies. We will work with other Government of Canada agencies and departments and our security partners to continue to advance military AI ethics, safety, and trust, and with other nations to develop standards, norms and confidence-building measures for AI, open channels for communication about accidents, unexpected system behaviour, cyber-attacks, and emergent effects as a result of system interaction, and encourage responsible AI development and use by other nations.

LINE OF EFFORT 4: TALENT AND TRAINING

The challenge

Effective implementation of AI will require the right people with the right training in the right place at the right time. The future DND/CAF workforce will require diverse personnel with a broad range of both technical and non-technical skills. These include multidisciplinary specialists with advanced skills, such as machine learning engineers, data engineers, data scientists, cyber security specialists, and AI product managers. It will also require those with soft skills including ethical reasoning, systems thinking, creativity, problem solving, communications, and human-centred design. In addition, it will also need personnel in the fields of IT, law, policy, human resources, procurement, and finance with the skills and knowledge to support AI initiatives and a diversity of identities, backgrounds, and perspectives. This talent must be identified, cultivated, and used to its fullest potential when and where it is needed.

DND/CAF recruitment, retention, training and deployment are not yet equal to this challenge. Overall levels of data literacy are low, AI skills are scarce, and personnel with AI knowledge are in short supply. While the CAF recognizes its own need for AI skills, it often struggles to make use of those specialized personnel it already has. Members have described their specialization in AI and related fields as career limiting and speak of having to choose between remaining within their technical field and a career path that would lead to promotion. Unsurprisingly, the frustration this produces leads members to release, or transfer to the reserves.

What we must do

We must identify and plan for our workforce needs. DND/CAF must identify the skills, perspectives, and competencies its personnel, both military and civilian, will need to ensure they can understand new technologies, absorb them into the battle space and corporate space, and develop the new operating concepts, organizations, and strategies to use them effectively and ethically. This process will require identifying what must be cultivated within the organization and what can both safely and effectively be contracted out. It should also consider the adequacy of recognized competencies and existing trades, classifications, and occupations, and how the trades, career management, and staffing may need to be revised

to make them able to accommodate AI. Given the rapid pace of technological development, this cannot be a one-time exercise but must be ongoing to ensure that we have the balance of skills required by these technologies, and that our training equips our people to procure, sustain, and use it effectively and safely. Once these needs are identified, they must inform robust planning for military recruitment and civilian human resources. This must give consideration for the impact of such changes on organizational inclusion and diversity.

We must cultivate AI readiness among our existing people. This must begin with ensuring adequate data and digital literacy: without these skills, achieving AI implementation will be impossible. We must be ready to invest in continuous development of the skills of our existing and future workforce to help them keep pace with AI development outside the enterprise, accelerate the acquisition of expertise, and enable them to progress within their career and adapt to new roles in the future. Comprehensive and high-quality AI training is widely available, often free or at minimal cost from software providers, but DND/CAF will need to allow personnel to take training within working hours. It will also need to offer opportunities to learn by doing and to use the skills learned so they are not lost. More specific training to address the skills to support AI use may need to be developed in-house or co-created with the Canada School of Public Service (CSPS) or private providers. These include training for leaders and decision makers in the opportunities, risks, and limitations of AI and how to assess and maintain appropriate human involvement in system decisions. They also include the soft skills needed for communication, ethics, ideation, and design, and the administrative skills to procure, staff and sustain AI tools. Moreover, these skills must be regularly reviewed and adapted as strategic circumstances, capabilities, and technology change. Existing professional military education programs must be reviewed and adapted to incorporate these skills, and to address issues such as the ethics and military implications of data and advanced technology. As we automate repetitive tasks too, we must plan to upskill and redeploy those personnel who previously performed them to more challenging and rewarding tasks that require human judgement.

We must find new ways to bring critical skills into the enterprise–and to retain and use them. AI and data skills are in high demand in the private sector, and we will need to compete with the private sector to recruit and retain personnel with these skills. Militaries worldwide are experimenting with new ways of identifying and recruiting talent to the regular, reserve, and civilian workforce, and as embedded contractors, and we should learn from them. We must explore flexible, streamlined, and non-traditional pathways to bring world-class AI talent into the organization and expand access to outside expertise, including short-term exchanges with industry and academia. Career pathways, development and management of CAF members will need to be reviewed and adapted to support attraction and retention of AI-related talent and provide pathways for its professional advancement. Finally, we must consider ways to make use of the depth of skills present among current and potential members of the Reserve Force. This could include the creation of technical reserves and routes to identify and reward technical talent outside traditional ranks. We must offer Canadians ways to bring their skills to DND/CAF on a part-time basis in roles that offer opportunities to make an impact using leading AI technologies to solve consequential problems.

HOW WE WILL DO THIS

1. ***Review DND/CAF workforce needs for AI***. DND/CAF must review its AI workforce requirements to identify the skills, competencies, and personnel required to implement AI successfully. This must include not only subject matter experts in AI, but also staff whose roles support the AI lifecycle, including civilian and military leadership. Such a review must include GBA Plus to assess the impact of these changes on workforce inclusivity and diversity.

2. ***Identify priority AI workforce training requirements and develop or procure curricula to meet them***. DND/CAF must identify and plan to meet its priority needs through in-house curriculum development, external procurement, and academic partnerships. This review should consider training needs at all levels and new options for both academic and professional training to ensure a talent pipeline catered to future needs.

3. ***Explore and identify processes to recruit and retain AI talent, and to use it where it is needed***. DND/CAF must explore non-traditional routes and processes to identify and place talent, such as short-term exchanges, the creation of technical reserves, and more flexible career pathways allowing for talent attraction above entry level.

LINE OF EFFORT 5: PARTNERSHIPS

The challenge

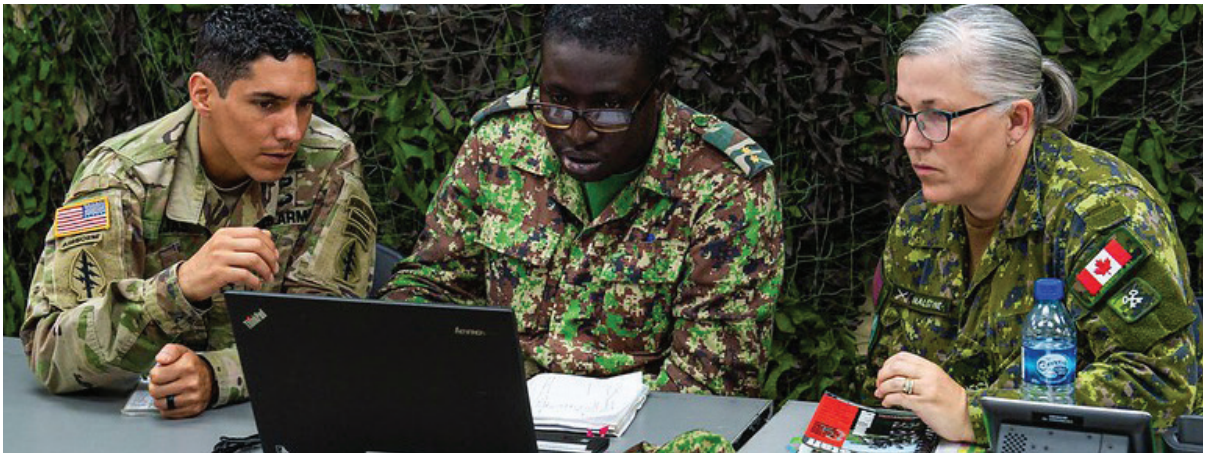
The state of the art in AI is collaborative—and often outside defence. Internally, implementing and leveraging AI will take the collaboration of many within the Defence Team, however, that is only the beginning. Globally, although defence research once claimed the technological leading edge, the most advanced AI techniques and applications are now typically found in industry, academia, and the open-source community. Consequently, DND/CAF must be open to procure, co-design, co-develop, test and validate with trusted partners. Adopting AI-enabled technologies will also require international cooperation between nations sharing the same values to develop and agree upon principles, policies and standards to build and protect a secured digital infrastructure and supply chain with the right analytics.

At present, AI in DND/CAF needs the coordination that would come from partnerships. DND/CAF must continue to actively pursue opportunities for defence, safety and security collaboration with partners from other government departments and agencies, industry, academia, and international allies to maximize the strategic advantages of Canada's innovation ecosystem and to secure it against adversaries and threats. Engagement activities must span the entire innovation spectrum, including scientific and technical information and personnel exchange, shared data, jointly developed frameworks, trials, experiments, advanced concept technology demonstrations, and consultation with communities of practice.

What we must do

We must ensure that innovation is adaptable and interoperable. Developing a strategic AI vision that aligns with Canada's defence allies, including the Five Eyes partnership, the Technical Cooperation Program (TTCP), and our NATO Allies, will allow DND/CAF to prioritize and further develop AI research on interoperable capabilities, while sharing current best practice on building a military AI capability and educating personnel in its use. It will also afford opportunities to invest strategically in technologies that complement those of our defence partners.

We must work to build and leverage a defence and security AI ecosystem. Both Canada and DND/CAF benefit from the growth of talent and competition in AI. It is in DND/CAF's interest to nurture a vibrant, diverse, agile, and responsive defence innovation ecosystem drawing on that already created by the Pan-Canadian AI Strategy and administered by the Canadian Institute for Advanced Research (CIFAR). The experience of CIFAR proves clearly that this can be done. However, this will require innovative tools for engagement with industry, academia, and non-traditional partners to maximise the identification and leveraging of joint capabilities, speed up procurement, and facilitate access to experts for short-term engagements. It will require that we identify dual use and defence-specific opportunities, and partner with small and medium enterprises to field limited-use and scalable capabilities. It will



also require efforts to overcome the obstacles to engaging industry effectively, to aligning digital infrastructure that supports external collaboration, and to protecting intellectual property. Finally, it will require a long-term commitment to invest beyond experimentation to scale.

We must continue to innovate in partnership with external sectors. Strong partnerships with the private sector and academic institutions at the leading edge of AI advances will be vital at every stage in the AI life cycle, from research, validation, certification, deployment, sustainment, and decommissioning. DND/CAF must increase partnerships with academia and industry to identify, fund, and enable breakthroughs in AI. This collaboration should include traditional funding models and existing initiatives such as Mobilizing Insights in Defence and Security (MINDS) and Innovation for Defence Excellence and Security (IDEaS), but also increased use of innovative approaches such as grand challenges, hackathons, and creative design sessions with start-ups and integrators to co-design and co-develop AI-enabled solutions at the leading edge of the technology. We must also explore non-traditional partnerships. Defence has much to learn from non-traditional partners such as civil society, non-technical branches of academia, and the open-source community.

We must deepen collaboration with other government departments to yield efficiencies and a common approach. For economy of effort and interoperability, DND/CAF must work towards co-developing and sharing AI capabilities with other government departments, particularly with those departments and agencies with whom we share responsibilities for national security. A whole-of-government approach will enable transfer of technology, better external relationship-building and partnerships, and the acquisition of AI technology that can benefit all areas.

We must establish guidelines to ensure that our partnerships are trusted and secure. We know that our allies, industry and academia are constantly targeted by potential adversaries, making our reliance on AI partners a potential source of strategic vulnerability. This is particularly true for dual-use technologies. Academic researchers often work in global networks whose boundaries and membership can be hard to secure, while Canadian companies continue to be subject to industrial espionage and can experience supply chain vulnerabilities. We must therefore invest in research and the development of guidelines to ensure that our partnerships are appropriately secured against external threats.

HOW WE WILL DO THIS

1. ***Reinforce strategic partnerships and cooperation with allies on new capabilities, best practices, and lesson learned.*** This should include furthering our strategic collaboration with the Five Eyes, TTCP, and NATO, but also deepening bilateral cooperation with trusted nations on specific areas of common interest.

2. ***Contribute to improving the procurement process to support development and acquisition of AI that balances security, safety, and ethics with the imperative to maintain flexibility and agility.*** We must continue to work with Public Services and Procurement Canada (PSPC) to identify the specific requirements and opportunities to simplify and accelerate procurement processes. This will lower administrative barriers for Canadian innovators to onboard, increase supplier diversity, and enhance economic and social opportunities for underrepresented groups. Procurement changes should also encourage organizations to identify AI and its technical foundations such as data and digital infrastructure within capability requirements.

3. ***Contribute to activities that encourage secure and reliable data infrastructures and sharing with partners and allies***, working on common datasets to develop interoperable solutions.

4. ***Enhance connections with academia to encourage skill development in support of defence requirements.*** We must encourage innovative partnerships through personnel exchanges, such as the Mobility initiative to enable personnel exchange between IDEaS partners. We must also look for opportunities for new training paths to develop a talent pipeline for defence.

5. ***Further develop and foster the innovation ecosystem for defence and security in partnership with the Pan-Canadian Innovation Ecosystem in AI.*** We must explore avenues for skill-sharing and assignments to deploy talent flexibly across sectors. We will also need to expand linkages and support for innovative solutions to defence challenges and foster processes to scale these initiatives across the Defence Team. This could include existing vehicles such as the DRDC research centres, and the MINDS and IDEaS programs, but should also extend to new funding lines to support priority military capabilities and mechanisms to provide challenges to industry. In doing so we must be strategic about research and development areas where we can build on Canada's existing strengths.

6. ***Work with government partners to ensure defence and security interests are included in the design of the Canadian innovation ecosystem.*** The innovation ecosystem must be secured against adversarial actions and supported to build linkages to the defence environment. This should include attention to the security of the supply chain and the need for export controls on sensitive Canadian technology. We must also ensure cohesion and coherence in the regulatory space, reducing the administrative burdens of compliance for non-experts.

CONCLUSION

AI holds enormous potential for defence. AI-enabled capabilities can allow us to improve the accuracy of our intelligence, targeting, situational awareness, and decision making, while enabling logistic and corporate efficiencies and improving services. To achieve these gains, however, we must put in place the necessary environments, data management practices and guardrails to ensure that AI is safe, ethical, inclusive, legal, and trusted. We must manage change so as to support innovation, and ensure that our personnel, both now and in the future, have the training and skills that they need to implement AI initiatives successfully. We must also forge partnerships outside the organization to take advantage of promising innovations, and to ensure that our AI-enabled capabilities complement and interoperate with those of our defence partners.

The AI Strategy lays out the vision for the adoption and implementation of AI and related algorithmic technologies within the Defence Team, and five lines of effort to achieve that vision. These goals are needed to set the forward direction, to align expectations for DND/CAF at the enterprise level, and cohere thought, effort, and purpose towards this common goal. However, these alone will not be enough to achieve our purpose. To make this vision and these lines of effort a reality, the Digital Transformation Office will develop a staged implementation plan with timelines, milestones, and performance indicators, leveraging the cross-functional approach adopted in the development of this Strategy. It will also develop a governance model and accountabilities and responsibilities framework for AI to ensure that the implementation itself is successful and well-governed.