



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.

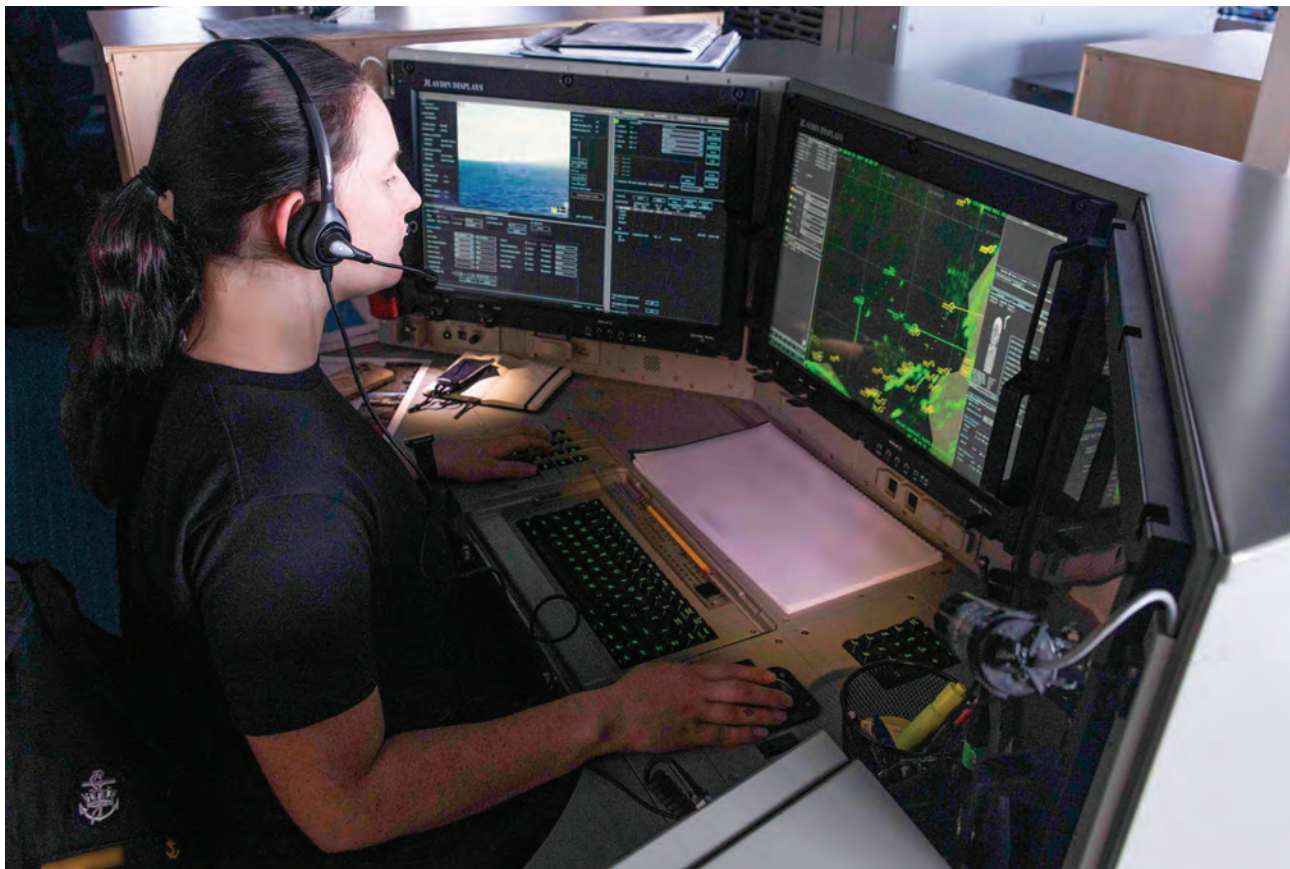
The U.S. Department of Defense's cloud modernization illustrates this vulnerability. First announced in 2017, the Joint Enterprise Defense Infrastructure (JEDI) aimed to consolidate cloud services under a single \$10 billion contract with one company.⁹ Years of legal challenges followed, and by 2021 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>.