



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

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

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

JENNIFER GEAREY AND MAJOR TYLER CURRIE

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

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

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

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

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

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

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

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

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

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

AI as a Strategic Challenge

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

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

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

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

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

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

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

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

Big Tech, Corporate Agency, and the Defence of Democracy

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

Photo: Canadian Armed Forces photo

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

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

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

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

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

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

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

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

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

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

Huawei, the Digital Silk Road, and the interoperability challenge

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

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

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

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

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

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

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

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

Procurement, market volatility, and the economics of speed

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

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

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

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

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

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

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

Implications for Canada and NATO: A contained Agenda

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

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

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



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

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

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

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

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

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

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

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

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

Conclusion

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

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

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

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

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

Notes

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

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