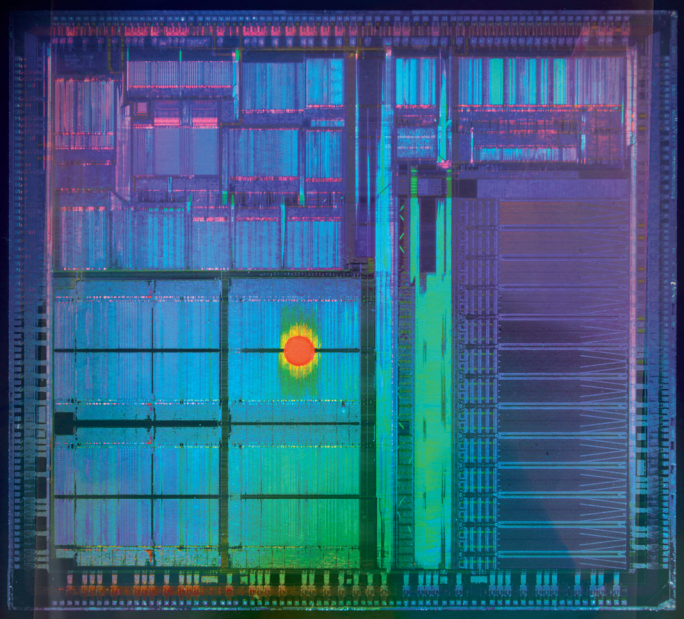
Centre for International
Governance Innovation

SPECIAL REPORT

Artificial Intelligence for Defence and Security

Daniel Araya



Centre for International
Governance Innovation

SPECIAL REPORT

Artificial Intelligence for Defence and Security

Daniel Araya

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Manager, Government Affairs and Partnerships Liliana Araujo
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Sami Chouhdary

This work was carried out with the aid of a grant from the Department of National Defence's Defence Research and Development Canada.

For publications enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Daniel Araya is a CIGI senior fellow, a senior partner with the World Legal Summit, and a consultant and an adviser with a special interest in artificial intelligence, technology policy and governance. At CIGI, his work contributes to research on autonomous systems in global governance and looks specifically at the best ways to mitigate the negative effects of the widespread deployment of new technologies.

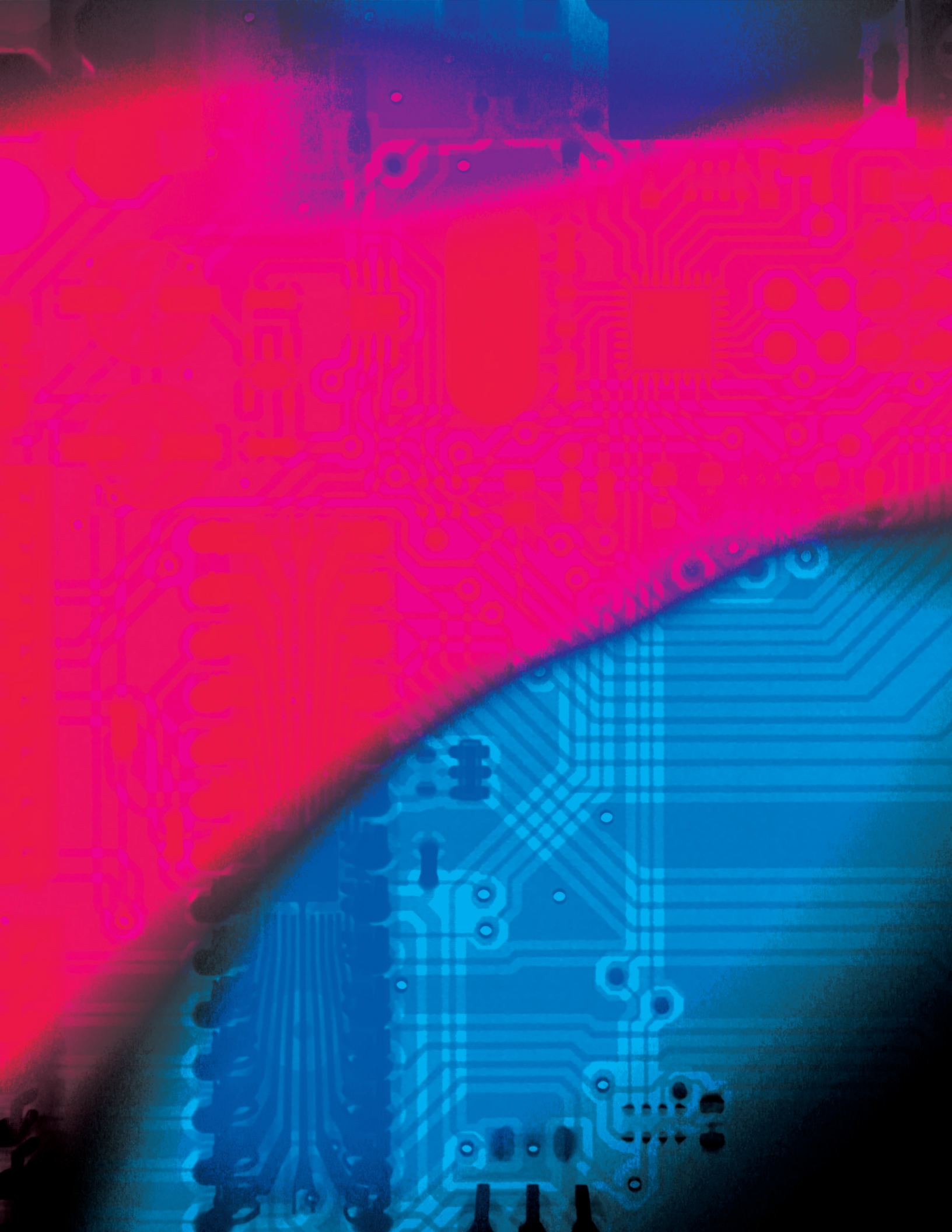
Daniel is a regular contributor to various media outlets and organizations such as Forbes, the Brookings Institution, Futurism and Singularity Hub. He has been invited to speak at a number of universities and research centres, including the US Naval Postgraduate School; Harvard University; the American Enterprise Institute; the Center for Global Policy Solutions; Stanford University; the University of Toronto; the University of California, Santa Cruz; and Microsoft Research. His most recent books include *Augmented Intelligence: Smart Systems and the Future of Work and Learning* (2018) and *Smart Cities as Democratic Ecologies* (2015). Daniel has a doctorate from the University of Illinois at Urbana-Champaign.

About the Workshop Series

The Centre for International Governance Innovation (CIGI) and Defence Research and Development Canada (DRDC) hosted a series of interactive virtual workshops on using artificial intelligence (AI) to address defence and security challenges and opportunities. The aim of this workshop series was to bring together experts from the Canadian innovation ecosystem in AI, the Department of National Defence (DND) and the Canadian Armed Forces (CAF) to exchange perspectives on the impact of the development and adoption of AI for defence and security, to inform DRDC's strategic science and technology and innovation programs, and to contribute to the development of DND and CAF's AI strategy. This workshop series was divided into three thematic areas: AI and semi-autonomous systems, AI and cybersecurity, and enabling pan-domain command and control. These sessions were interactive and used an ideation approach, meaning they were designed to generate both ideas and potential solutions, and to equip participants with the necessary information to make decisions about the shape and direction of the future usage of AI within the military and national defence and security spheres. This special report serves as a summary of these discussions, while also drawing on the policy, regulation, diversity and ethical dimensions of adopting AI in this field of application.

Acronyms and Abbreviations

5G	fifth-generation
AI	artificial intelligence
C2	command-and-control
CAF	Canadian Armed Forces
CIGI	Centre for International Governance Innovation
DLTs	distributed ledger technologies
DND	Department of National Defence
DoD	Department of Defense
DRDC	Defence Research and Development Canada
EDTs	emerging and disruptive technologies
GPT	general purpose technology
IoT	Internet of Things
JWCC	Joint Warfighting Cloud Capability
LAWS	lethal autonomous weapons systems
NATO	North Atlantic Treaty Organization
NORAD	North American Aerospace Defense Command
NSI	National System of Innovation
OODA	observe, orient, decide, act
OSINT	open-source intelligence
UAVs	unmanned aerial vehicles



Executive Summary

Technology is fundamentally changing the nature of national defence. From revolutionary advancements in artificial intelligence (AI) and machine learning to rapid innovation in quantum computing, robotics and space-based telecommunications, military defence planning is evolving. Harnessing science and technology to advance command-and-control (C2) systems across the Department of National Defence (DND) and the Canadian Armed Forces (CAF) is critical to maintaining the defence of North America.[1]

The defence of North America remains a key priority for Canada and the United States as highlighted in *Strong, Secure, Engaged: Canada's Defence Policy* (National Defence 2017) and the US National Defense Strategy (US Department of Defense [DoD] 2018) and by the US National Security Commission on Artificial Intelligence (2021). Notwithstanding the fact that our current systems and approach to the defence of North America have kept Canada and the United States safe for many years, they are increasingly outdated in the face of new and emerging threats.

As a recent report prepared for the DoD explains, technological change is reinforcing time compression between an operational commander's identification of a need or opportunity and the delivery of a solution to warfighters (Modigliani et al. 2020). In the digital age, militaries are now challenged to move faster and make better decisions even as the timescale between idea and initial operational capability begins to shrink.

Today's security threats continue to blur the traditional distinctions between land, sea, air, cyber, space and information domains — even as technology erodes the advantage that geography once provided. The application of AI and autonomous systems to battlefield situational awareness and precision-guided weapons systems represents a paradigm shift in the evolution of military technologies.[2]

Notwithstanding the fact that technological innovation has always shaped the nature of war, the scale and velocity of contemporary technological change are unprecedented. Together, autonomous drones, augmented human-machine teaming and satellite-mediated telecommunications are increasingly becoming the basis for modern military systems. Together, the rise of a multipolar order and a growing market in digitally augmented weapons (Public-Private Analytic Exchange Program 2019) have begun to strategically reconfigure the nature of national security.

Beyond the era of Western predominance, Asia is returning to the patterns of commerce and cultural exchange that thrived long before the age of modernity (Romei and Reed 2019). The growing rivalry between the United States and China overlaps a shift in the world's geopolitical centre of gravity as changes in the global economy increasingly favour Asian markets. If the nineteenth century belonged to Europe and the twentieth century to the United States, then the twenty-first century now belongs to Asia and especially China.

Indeed, the events unfolding in Ukraine signal a turning point in the history of great power competition. Russia's invasion of Ukraine underscores a changing geopolitical landscape as a polycentric system begins to take shape. Together, Russia's regional ambitions and China's economic ascendance are upending the strategic architecture of Eurasia in reconfiguring the global order.

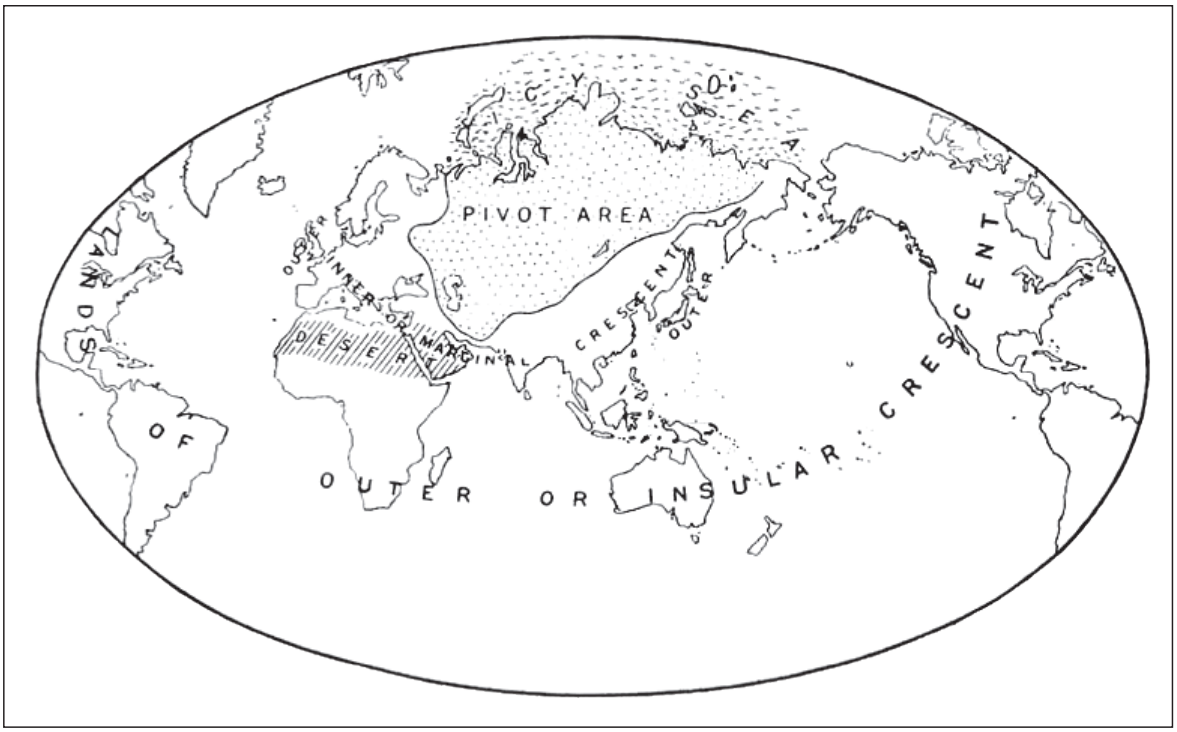
What we may be witnessing is a new geopolitical configuration. China's ambitious Belt and Road Initiative has the potential to unify what geopolitical strategist Halford Mackinder described in 1904 as the "World-Island" (Afro-Eurasia or Africa, Europe and Asia) (see Figure 1). As Mackinder observed, the rise of every global hegemon over the past 500 years has been possible because of a dominance over Eurasia (McCoy 2021).

We face a new historical moment as great power rivalry and accelerating technological change combine to reshape the global order. Together, the convergence of geopolitical frictions in global trade and a protracted conflict between the North Atlantic Treaty Organization (NATO) and Russia suggest a new and different risk environment. The application of commercial

1 See www.ourcommons.ca/Committees/en/NDDN/StudyActivity?studyActivityId=8818485.

2 Significantly difficult to detect and defend against, hypersonic weapons and their high-speed manoeuvring severely shorten the time it takes to reach their target, negatively impacting the overall ability to predict target behaviour when compared to current cruise and ballistic missiles.

Figure 1: The World-Island



Source: https://en.wikipedia.org/wiki/The_Geographical_Pivot_of_History#/media/File:Heartland.png.

algorithms and off-the-shelf software ensures that technologies that build on autonomous systems and AI raise the spectre of protracted cyberwar even as cybercriminals and state-sponsored actors leverage data and communication networks to attack nonconventional targets.

DND/CAF recognizes that a new technological era marked by shifting innovation and a changing geopolitical landscape is now taking shape. In June 2017, DND/CAF released its defence policy, *Strong, Secure, Engaged*, with the understanding that much of Canada's tactical advantage is due to "agile information management and technology tools."[3] With a strategic focus on advancing a range of information technologies including data analytics, deep learning and autonomous systems, *Strong, Secure, Engaged* outlines a number of priorities and defines key pillars[4] supporting Canada's strategic vision on national defence.

Consistent with *Strong, Secure, Engaged*, Defence Research and Development Canada (DRDC) and the Centre for International Governance Innovation (CIGI) co-organized a nationwide workshop series to examine Artificial Intelligence for Defence and Security in the context of Canadian national security. This initiative was specifically aligned with the growing focus on data across the Government of Canada as seen in the *Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service* (Government of Canada 2018).

The workshop series hosted a variety of speakers to advance a better understanding of the resources and expertise needed to manage next-generation military operations across three broad themes:

3 See www.canada.ca/en/department-national-defence/corporate/reports-publications/data-strategy/introduction.html.

4 The three pillars are: "strong at home, its sovereignty well-defended by a Canadian Armed Forces also ready to assist in times of natural disaster, other emergencies, and search and rescue; secure in North America, active in a renewed defence partnership in NORAD and with the United States; [and] engaged in the world, with the Canadian Armed Forces doing its part in Canada's contributions to a more stable, peaceful world, including through peace support operations and peacekeeping" (National Defence 2017, 14).

- AI and semi-autonomous systems,
- AI and cybersecurity, and
- enabling pan-domain C2.

Aimed at strategically engaging the Canadian innovation ecosystem, the workshop provided a space for experts to engage in a discussion on the challenges presented by AI to Canadian national defence. Initiated by the DRDC Directorate of Partnership Strategies, the workshop program was managed by CIGI over the course of fall 2021 and winter 2022. Participants included key stakeholders from DND/CAF, the Government of Canada and leading institutions supporting research on AI.

Focused on understanding the requirements involved in developing and implementing a trusted, explainable AI for military operations, the workshop examined a host of issues, including data quality assessment, data format, data sharing, bias mitigation, human-machine teaming and the ethics of autonomous systems. This special report builds on the workshop series and offers specific recommendations for advancing Canadian military planning. It is designed to provide an analytical framework for understanding the impact of AI on national defence over the coming decade.

Introduction

Strategic prospects for sustaining military preparedness are now directly tied to the development and application of emerging and disruptive technologies (EDTs). From AI and robotics to fifth-generation (5G) telecommunication networks and the Internet of Things (IoT), many of the key innovations now set to catalyze military development have a science and technology nexus. Taken as a whole, these frontier technologies represent an enormous economic and security transformation that is reshaping the commanding heights of the global economy.

While our current military systems and approach to the defence of North America have kept Canadians safe from harm, many of these systems are now outmoded in the face of new and emerging threats. Technology is eroding the advantage that geography once provided for the security and defence of Canada from adversaries overseas. Indeed, where nuclear warheads remain a singular application of technology, AI is capable of underwriting many different types of weapons and systems.

While we often understand EDTs in terms of linear development, the reality is that innovation across a global market now follows an exponential curve (National Intelligence Council 2021). Together, neuroscience, quantum computing and biotechnology are advancing quickly and represent uncharted territory in the long-term evolution of military technologies. This transition portends a dramatic shift away from rudimentary machines and toward data-driven technologies and precision electronics. Given this accelerating innovation, DND/CAF now faces a transformation in military technologies that is difficult to overstate.

At the centre of this enormous transformation are AI and machine learning. As the DND/CAF data strategy observes,[5] traditional military platforms (ships, tanks and planes) are now data platforms for capturing, creating and using large volumes of data. AI is essentially a "learning engine" that relies on the constant feed of massive amounts of data in support of machine-learning algorithms. As these learning engines proliferate, the digital ecosystems they depend on are becoming critical to reorganizing mass industrial systems and personnel.

In response to the need for military transformation, Prime Minister Justin Trudeau has directed the minister of national defence to "continue Canada's strong contributions to the North Atlantic Treaty Organization (NATO) and work with the United States to ensure that the North American Aerospace Defense Command (NORAD) is modernized to meet existing and future challenges, as outlined in *Strong, Secure, Engaged*" (Office of the Prime Minister 2019). More recently, in the "Roadmap for a Renewed U.S.-Canada Partnership" (February 2021), Prime Minister Trudeau and US President Joe Biden agreed to expand cooperation on continental defence and in the Arctic, including the modernization of NORAD.[6]

What is clear is that a changing technological landscape signals the need for close collaboration between Canada and its NATO allies. Fortunately, Canada has many strengths with regard to AI. A recent study by Global Advantage Consulting Group (2021) contained the following conclusions:

- Canada has a strong AI talent pipeline, including 47 major higher-education institutions offering AI-specific programs and/or courses, and world-class AI institutes serving as anchors for future development.
- As of January 2022, $1.1 billion in government grants and contributions have been awarded across Canada.
- In 2021, Canada ranked seventh in terms of AI publications globally (however, it ranked only fifteenth in patent outputs).
- Of the identified 543 AI firms in Canada, 47 are already involved in AI for defence and security, including supplying the Government of Canada, while the products and services of another 54 can potentially find defence application.
- Canada has the foundations and fundamentals to be a significant player in AI for defence and security; however, since 2018, 187 AI

5 See www.canada.ca/en/department-national-defence/corporate/reports-publications/data-strategy/data-strategy.html.

6 NORAD is a binational military command responsible for aerospace warning, aerospace control and maritime warning. As a binational command, the NORAD commander is appointed by and responsible to the heads of government of both Canada and the United States.

companies have permanently closed or have been acquired by foreign firms.

The Defence of North America

Technological innovation enables ever-more powerful innovation to emerge on top of previous generations of science and technology, much like sedimentary layers. And as each new substrate of innovation builds on the last, new disruptive technologies take root. Today, a vast creative explosion in commercial applications overlapping robotics, autonomous systems, renewable energy infrastructure, space-based telecommunications and commercial AI is reshaping the global order. As these technology building blocks continue to underwrite the convergence of human and machine intelligence, they are beginning to reshape the fabric of modern militaries as well.

In response to this changing threat environment, DND/CAF has begun a long-term process of integrating frontier technologies into Canadian military operations. This process includes expanding and evolving DND/CAF by incorporating next-generation surveillance aircraft, remotely piloted systems and space-based assets in the integration of new military platforms (National Defence 2017, 77).

NORAD remains the cornerstone of Canadian national defence, providing both the United States and Canada with a broad mandate on continental security (see Figure 2). As the "Joint Statement on Norad Modernization" (National Defence 2021) explains, a changing security landscape necessitates a shared commitment to modernizing, improving and better integrating the capabilities required for NORAD to maintain persistent awareness in understanding new potential threats to North America.

Canada continues to be a technology leader, but global markets in frontier technologies are shifting. In fact, the pace of innovation itself now demonstrates a rate of change that is not constant but accelerating. Part of the explanation for this acceleration is the capacity of digital technologies to support lateral scaling networks across a global telecommunication infrastructure. Extensive global cooperation among academic researchers, leading commercial enterprises and industry clusters means that advancements in AI and machine learning now diffuse globally.

Figure 2: The NORAD and US Northern Command Strategy

All-domain awareness: This is created through a layered sensing grid (network of all-domain sensors and systems) that provides persistent and complete situational awareness, from subsurface to space and cyberspace.
Information dominance: Effective information dominance systems must ingest, aggregate, process, display and disseminate data quickly and reliably by leveraging the potential of AI and machine learning. The data needs to be shared across domains, across classification, with partners and allies and brought into a cloud-based computing environment to enable decision superiority. Experiments such as the Global Information Dominance series are useful to test and validate pan-domain situational awareness and identify what is possible and what needs to be improved.
Decision superiority: This aims to give senior leaders the options they need for deterrence and de-escalation. Efforts should be made to identify early indications and warnings, pattern of life and weak signals. Relying on endgame, kinetic defeat mechanisms is a losing strategy and must be avoided using all levers of influence.
Global integration: Potential adversaries' actions are global in nature and require global and all-domain awareness, options, actions and effects. Global options, strategies and plans need to be developed to achieve integrated deterrence.

Source: Author.

Science and Technology in a Changing Multipolar Order

Beyond purely extractive systems of production (coal, oil, gas, livestock, raw materials), we are now moving into a world that is increasingly focused on leveraging building blocks for creative innovation (protons, electrons, quantum bits, DNA and new materials). Where industry leaders in the twentieth century (for example, Chevron, ExxonMobil, General Motors, IBM) oversaw the rise of a mass industrial society, so industry leaders of the twenty-first century (Alphabet, Amazon, Google, Baidu, Tesla) are now catalyzing an economy and society driven by AI and robotics.

Militaries around the world are investing enormous sums in the development and adoption of AI-enabled capabilities. Against the backdrop of great power rivalry and a changing multipolar order, AI has emerged as a particular focus of competition. Indeed, strategic planning around AI (see Figure 3.1 in Berryhill et al. 2019, 74) now defines contemporary efforts at security modernization (Congressional Research Service 2020).

Competition across a changing multipolar order is accelerating the pace at which governments invest in AI research — particularly machine learning. In the past, the convergence of steel, rubber and the internal combustion engine combined to remake transportation and the design of cities; today, AI and robotics promise to reshape the nature of national defence and security. China, Russia, the United States and other state and non-state actors are aggressively pursuing the military application of AI and robotics.

China, in particular, hopes to lead the world in AI by 2030 and expects to widen its lead in the industrialization of AI by harnessing the country's massive abundance of data (Lucas and Feng 2017; Lee 2018). Given the seemingly unlimited scale and scope of Chinese data, the rapid rise and trajectory of Chinese AI will be critical to the evolution of Chinese military technologies (Kania 2017). To be sure, China's national agenda for military-civil fusion (军民融合) portends a new era in military innovation.

Semi-autonomous Systems and AI

AI might be best defined as tasks performed by machines that are designed to mirror human intelligence.[7] The field of AI research began in the 1940s, but the explosion of interest in AI only gathered pace as increases in computer processing power and improvements in software algorithms began to converge. As a subset of AI, machine learning represents the most prominent application of AI (see Figure 3). Machine learning uses statistical techniques to enable machines to "learn" without explicit instruction, generating many applications and services that improve automation across a range of analytical and physical tasks.

The application of AI to military planning has become a major priority for the vast majority of states today. In fact, the application of technology to war is rooted in a long history of military innovation. Horses and armour powered feudal kingdoms, and steel and gunpowder galvanized the rise of nation-states. Now, AI and robotics represent a new phase in the evolution of a multipolar order. Data-driven technologies that build on AI are now ubiquitous, transformational and omnipresent in modern societies and our everyday lives.

In the military domain, three centres of AI leadership have emerged across the global security landscape: China, Russia and the United States. In fact, all three countries are competing to capitalize on AI for relative advantage given its potential military application — from cyber defence, intelligence, surveillance and reconnaissance to logistics and medicine. Annual global investments in AI are expected to jump from US$85 billion in 2021 to more than US$204 billion by 2025.

7 AI systems are made possible by research and innovation in machine vision, natural language processing, robotics, autonomous and multi-agent systems, knowledge representation and reasoning, machine learning, deep learning, mathematics and statistics, neural networks and neuroscience. This field overlaps academic disciplines that include computer vision, natural language processing, robotics, autonomous and multi-agent systems, knowledge representation and reasoning, machine learning/mathematics, neuroscience and computer science.

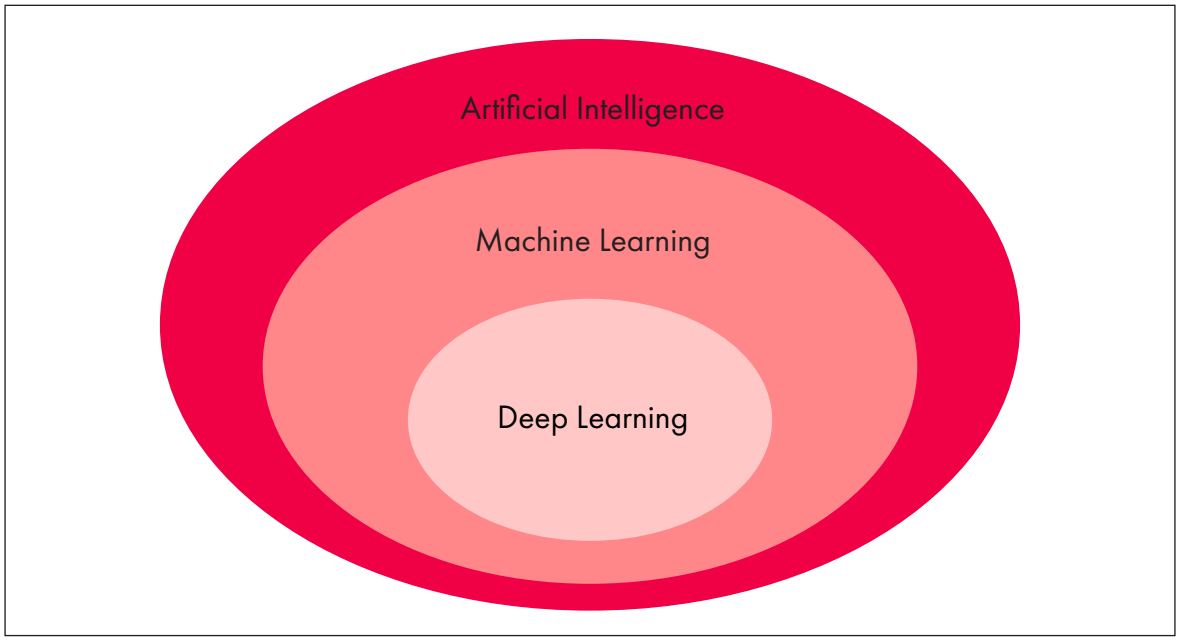
AI is expected to improve military capabilities across a range of fields and domains, including:

- image and pattern recognition (for example, threat identification);
- event and anomalous behaviour detection;
- data fusion and classification;
- cybersecurity (defensive and mitigation measures);
- autonomous system control (single platform or swarms);
- autonomous convoy and resupply (self-driving vehicles);
- human systems performance (gait learning, personalized training);
- natural language processing and text classification;
- automated reasoning/inference for intelligence;
- recommender systems (risk assessments);
- smart virtual personal assistants;
- cognitive electronic warfare; and
- medical diagnostics.

As a "general purpose technology" (GPT) (Jovanovic and Rousseau 2005), AI represents a force multiplier with a capacity to transform not only national defence systems but also agriculture, communications, transportation and health-care systems. Indeed, GPTs have a capacity to reconfigure the shape and contours of societies as a whole, dramatically altering their pace and organization. The term itself refers to innovations that trigger widespread technological development beyond their initial application (Bresnahan and Trajtenberg 1995).

The impact of AI and machine learning on the speed, scale and scope of war should not be underestimated. Much like other GPTs (electricity, fossil fuels and the steam engine), AI has a capacity to profoundly reshape the nature of conflict. Unlike a human army, a computer provides a direct application of human demands, providing a perfect tool for nation-states, rogue states and terrorists alike to weaponize. Software can work at much faster timescales across virtually unlimited networks and, for

Figure 3: The Layers of AI



Source: Author.

this reason, strategic planning will need to be highly calibrated to data-driven systems.

Platform Digitalization and the Value of Coordination

Beginning with network-centric US military operations in the 1990s, digital technologies have become the basis for advanced weapons, tactics and strategy. From battlefield situational awareness and autonomous weapons to precision-guided munitions and machine-driven psychological operations, cyber is moving war into the network era.

Much as in the private sector, software is transforming government and the military as well (Andreessen 2011). Data is now the lifeblood of all operational domains. In a digitized battlespace, every soldier, platform and resource is now a node within a complex military network. Where layers of human bureaucracy once coordinated the industrial era, digital platforms and data-driven applications are now central to a rising multipolar order.

Building on satellite applications, 5G telecommunications and cloud computing, information systems now easily and efficiently collect, transmit and process massive amounts of data, providing real-time analytics in support of both advanced and mundane military operations. As states rush to develop secure platforms and operating systems to reduce the threat of cyberattack, governments are now focused on a new era of military modernization.

In the United States, DoD has already begun the comprehensive process of integrating the US military across a commercial cloud platform. Working with the country's largest cloud service providers (Amazon, Microsoft, Google), DoD has begun developing what it calls the Joint Warfighting Cloud Capability (JWCC). Replacing the previously planned Joint Enterprise Defense Infrastructure system, JWCC is envisioned as a multi-cloud architecture supporting the entire US military. Spanning the full scope of DoD operations at all security levels, JWCC is expected to modernize the US military, including its procurement systems.

NATO itself has selected the French multinational Thales[8] to provide its first defence cloud infrastructure. Supporting a fully certified solution for end-to-end connectivity, the Nexium Defence Cloud is expected to analyze and share data in real time from a command centre to the theatre of operations, both accelerating the decision cycle and accommodating various levels of classification.

Networked platforms are now critical to multi-domain operations across NATO countries. The increasing dimensionality of war means that the large number of actors involved, the vast quantities of data to be acquired and digested, the number of lines of authority to work across, and the considerable number of actions and effects to consider, requires extensive algorithm-driven augmentation.

Unfortunately, Canada has no enterprise-wide architecture for managing military digitalization across DND/CAF. Nor does it have a strategic model for managing investments in the application of technology at an enterprise level. From strategy to communications to logistics to intelligence, digital platforms are now fundamental to orchestrating complex military operations. This includes coordinating air strikes, piloting drones, digesting real-time video of the battle space and managing highly complex supply chains.

A national cloud platform to modernize DND/CAF will be critical to integrating DND/CAF with its US and NATO partners. Digital platforms now underwrite communication, data processing and information sharing on a global basis. Enterprise-scale networks make it possible to visualize and coordinate highly varied resources across complex organizational environments. In the context of data, for example, the data needed to fuel AI and other digital technologies will remain siloed and inaccessible without the development of a national cloud infrastructure.

Challenges confronting DND/CAF include:

- → inadequate data standards and a fractured and siloed governance framework;
- → high volumes of data, and compressed analysis and decision cycles; and

8 See Thales (2021).

→ a lack of interoperability between government departments and allied networks, representing real and significant impediments to modernizing DND/CAF.

Given the size and scope of the Canadian defence enterprise, a strategic approach to modernizing DND/CAF will mean leveraging the enormous resources that digital technologies provide. Compressing timescales across contracting, acquisition, task orders and funding is critical to contemporary military modernization. Any DND/CAF strategy that seeks to leverage AI should endeavour to develop a national cloud ecosystem.

This includes platforms that bridge cross-sectional networks in order to support lateral scaling and working environments that:

→ improve data architecture;

→ augment data governance;

→ accelerate sensor networks;

→ promote better information technology;

→ ensure more advanced interoperability; and

→ implement advanced security measures.

Augmenting the CAF: Semi-autonomous Systems and AI

Together, the combination of great power competition and accelerating technological change means that military modernization efforts today must be data-driven and strategic. Unlike past technological development (for example, atomic weapons or stealth aircraft), no country will have a monopoly on military AI. Indeed, given the fact that most technological progress in the development of AI is now driven by industry rather than by government, future military technologies will be adaptations of commercial technologies.

Militaries around the world are developing or procuring autonomous and semi-autonomous systems, including unmanned aerial vehicles (UAVs)[9] that build on commercial algorithms (see Table 1). Using swarm techniques, for example, hundreds of unarmed drones can collect information from the field while guiding thousands more armed with various weapons (for example, firearms, artillery and/or munitions).[10] In fact, the process of systematizing targeting cycles (finding, fixing, tracking, selecting and engaging a target) is becoming entirely commodified in the form of "fire-and-forget" technology.[11]

Taken as a whole, the various drone programs that criss-cross Britain,[12] the United States,[13] Turkey, Israel,[14] Russia and China represent the early stages of a robotics revolution in military AI that is highly dependent on corporate research. Loitering munitions, for example, are not new, but recent innovations in machine learning are enabling the application of lethal autonomous weapons systems (LAWS) on a much larger scale. Unlike industrial-era military technologies (munitions, armoured vehicles, aircraft), drones can be acquired at low cost and require relatively little technical skill (Bergen, Salyk-Virk and Sterman 2020) even as they generate equal if not greater kinetic force.

Alongside large global technology companies, a wide range of commercial and academic research clusters are incubating a new generation of commercial AI (Li and Pauwels 2018). Fortunately, Canada has been a leader at the forefront of AI research and continues to nurture a strong AI ecosystem through several programs under the Pan-Canadian AI Strategy.[15] Canada's 2021 federal budget earmarked $444 million over 10 years to advance research and development, foster talent and promote leadership in AI. At the same time, Canada has struggled in the application

9 See https://en.wikipedia.org/wiki/Unmanned_combat_aerial_vehicle.

10 Drone swarm technologies can involve groups of micro/mini drones or UAVs, leveraging autonomous decision-making based on shared information. Indeed, contemporary military drones can already be designed to locate, identify and attack targets without a human in/on the loop.

11 See www.iai.co.il/p/harpy.

12 See https://dronewars.net/british-drones-an-overview/.

13 See https://dod.defense.gov/UAS/.

14 See https://drones.rusi.org/countries/israel/.

15 See https://cifar.ca/ai/.

Table 1: Militaries Using Autonomous and Semi-autonomous Systems

Platform	Countries
Harpy/Harop	Azerbaijan, China, Germany, India, Israel, Kazakhstan, South Korea, Turkey, Uzbekistan
Orbiter 1K	Azerbaijan
CH-901, WS-43	China
Devil Killer	South Korea
Coyote, Switchblade	United States

Source: Author.

of AI. The number of Canadian AI patents, for example, has been dropping steadily over the past 10 years (see Figure 4). In fact, since 2018, the number of AI patents published in Canada has halved. This trend will need to be reversed.

Notwithstanding the fact that Canada has a vibrant innovation ecosystem, there is a general lack of understanding about the nature of military procurement systems within Canadian commercial industry. This may partly explain the reluctance to invest and work in this area, but regardless of the reasons, the twentieth-century procurement processes designed for the acquisition of tanks and aircraft are simply no longer fit for purpose. The scale of change accompanying AI and other EDTs means that DND/CAF will need to redesign its procurement systems.

Canada now faces a generational challenge that is rooted in technological change. Building on the country's robust technology sector, Canadian security and defence strategy should be refocused to leverage the country's considerable technological prowess (Carson and Mersereau 2022). This includes autonomous space-based and subsea surveillance as well as a broad investment in Canada's digital infrastructure and technology industries. Indeed, even as we harness Canada's technological capabilities, we will need to safeguard Canadian intellectual property (Balsillie and Georgaras 2021).

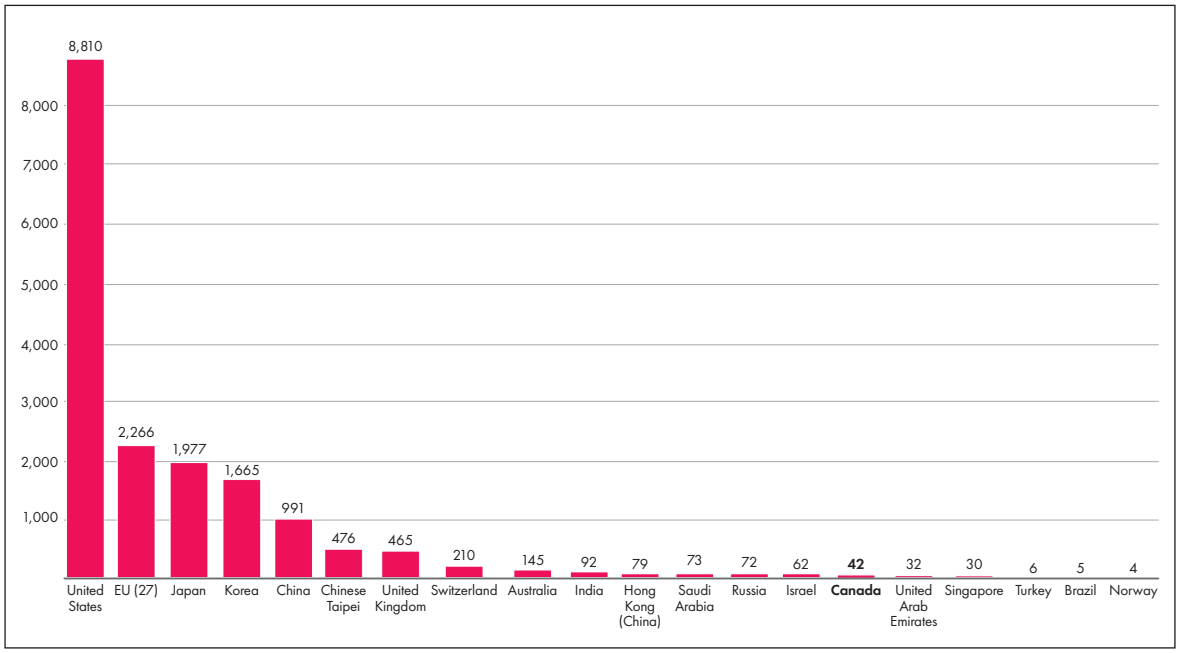
Augmenting Canadian Intelligence

Given the scope of AI in fomenting changes in military technologies, it would be wrong to assume that we can simply maintain the systems and practices inherited from a previous generation. Digitization is now so pervasive that cyber (Adams 2016) has become indispensable to Canadian transportation systems, water and power systems, electrical transmission grids, weapons systems, C2 systems and routine everyday communications.

As Greg Fyffe (2021) observes, the rise of AI as a tool of war overlaps a growing need to upgrade Canada's national security architecture — particularly Canadian intelligence. In the digital age, war is knowledge based. Given the commercial nature of Canada's digital ecosystem, the distinction between military and civilian infrastructure is now much less clear. Cyber continues to be a key target for potential adversaries, state proxies, criminal organizations and non-state actors alike. This includes surveillance (Stanley 2012) and reconnaissance of communications, intelligence and sensitive information.

As conflict expands into the information domain, Canadian military planning will need to significantly augment Canada's intelligence capabilities. This includes defence against information/disinformation operations, cyber

Figure 4: Canada's Ranking in AI Patents (2021–2022)



Source: https://oecd.ai/en/data?selectedArea=ai-research&selectedVisualization=ai-publications-by-country-over-time.

operations, espionage, covert intelligence operations, and political or economic influence operations. Compounding cycles of technological change and the explosion of data, new skill sets and new data strategies are now critical to the evolution of military modernization.

As Amy Zegart (2021) explains, technology is democratizing the nature of intelligence by dramatically expanding access to data and information. In fact, the majority of information driving strategic intelligence today is actually open-source intelligence (OSINT) or in the public domain. Canada's continued role in traditional alliances (NORAD, NATO and the Five Eyes[16] community) remains the basis for national security. However, AI and other EDTs are fundamentally changing the nature of conflict. Modern militaries are now critically dependent on secure, timely and accurate data. But as data expands exponentially, digesting it becomes impossible. The explosion of a data-driven economy has stimulated the need for new modes of analysis and new kinds of cyber tools.

In the digital age, security and intelligence personnel require new platforms, new tools and new OSINT agencies that work across domains. AI can be particularly helpful in this regard. As data grows in importance, so does adversarial competition across a vast digital landscape. AI and machine learning can dramatically improve Canada's national intelligence capabilities by sifting through enormous troves of data. AI is not a silver bullet, but it will dramatically augment Canadian intelligence capabilities in terms of information management, data analytics and evidence-based decision making.

Recommendations

- → Developing new platforms, new tools and new OSINT agencies that enable security and intelligence personnel to work across domains will be critical to pan-domain C2 in the digital era.
- → Redesigning DND/CAF procurement systems is critical to leveraging AI and other frontier technologies.
- → AI must be seen as a tool in modernizing Canada's national security architecture, particularly Canadian intelligence.

16 The Five Eyes security alliance consists of Australia, Canada, New Zealand, the United Kingdom and the United States.

Cybersecurity and AI

Conventional forecasts on technological change often assume that innovation replaces old technologies on a one-to-one basis. The reality is that general-use technologies such as AI and machine learning tend to disproportionately replace old systems with dramatically new architectures, boundaries and capabilities (Canadian Association of Defence and Security Industries 2019). AI is now fundamental to military modernization, particularly in terms of cybersecurity. Data has become the basis for a highly charged arms race that overlaps a range of commercial industries and platforms.

In the commercial domain, data has moved to the epicentre of global trade. With the rollout of 5G edge networks, it is anticipated that there will be an explosion of data created, collected, processed and stored. Where IoT encompassed 10 billion devices in 2018, it is projected to reach 64 billion by 2025 and possibly many trillions by 2040 (National Intelligence Council 2021). Measured by bandwidth, cross-border data flows grew roughly 112 times over from 2008 to 2020 (Slaughter and McCormick 2021). In 2018 alone, 330 million people made online purchases from other countries — each transaction involving the transmission of data driving US$25.6 trillion in cross-border sales — even though only 60 percent of the world is online.

This data-driven economy has ushered in a confluence of technological breakthroughs, from stacked neural nets that now consume zettabytes of big data to the application of massive cloud computing infrastructure in conjunction with smart mobile devices. Data is used for training AI algorithms, which, in turn, drive advanced machine-learning and autonomous systems. When applied to augmenting decision systems, the potential for serious and credible threats to Canadian defence and security will grow exponentially.

Adversarial AI: Attacking the Data, Attacking the Model

In addition to the slow pace of change across highly bureaucratized organizations, the centralized nature of C2 systems means that single points of failure provide vulnerable points of attack. Authorities and machine-driven systems responsible for managing C2 are particularly prone to adversarial techniques that leverage bad or deceptive information.

Just as cyber operations (whether espionage or attack) can instruct computer networks or machines to operate in ways they were not intended, adversaries can also use the same tactic against AI systems. Known as adversarial machine learning, this process seeks to identify weaknesses in machine-learning models and exploit them. Attacks can occur in the development or deployment stages, including misleading models by supplying deceptive input (for example, "poisoning" data) or targeting the model itself.

These methods are especially dangerous in national security settings because, in many cases, they are subtle and imperceptible to humans. Additionally problematic is the fact that adversaries do not necessarily need specific knowledge of a target model or direct access to its training data to impact it. As AI systems become more pervasive and more accessible to more people, the attractiveness and opportunity for attack grows.

Decentralization: Federated Data Governance

The weaponization of data is catalyzing new methods for countering AI systems. Securing commercially developed cloud platforms will be key to reducing the overall vulnerability of militaries in the digital age. Given the growing number of cyberattacks and the many commercial and government networks that have been penetrated over the past two decades — as well as the ever-increasing frequency of sophisticated cyberattacks — the need to build security into every level and feature of a military system is clear. Data security is pivotal to Canadian national security.

In this decade, Canada is at risk of falling behind both our allies and our adversaries in the data economy. Given the changing nature of national security in a digital era, DND/CAF has begun the process of elevating data to the level of a strategic asset. This matters both for economic growth and for national security planning.

One European country that stands out as a model for data security is Estonia. The country is perhaps the best example of advanced data governance

anywhere in the world. Most of Estonia's public services are digitally enabled and anchored to citizen digital identification cards. Often described as the first "digital republic" (Khan and Shahaab 2020), Estonia has even created "digital embassies" (Rice 2019) that provide a digital backup in the event of any loss of autonomy or sovereignty. Having constructed its own sovereign cloud infrastructure and data systems, Estonia's government remains largely immune to potential cyberattacks against commercial providers such as AWS or Google Cloud.

Developing federated data systems is the best method for managing cybersecurity in the digital age. Like the financial sector, DND/CAF should look to distributed ledger technologies (DLTs) such as blockchain to accelerate digital transformation. By distributing data laterally across decentralized networks, a CAF blockchain could help reduce the limitations and vulnerabilities inherent to highly bureaucratized systems. DLTs provide a decentralized validation system that can ensure all communication and data transfers are accurate, immutable and protected from adversaries while eliminating the potential failure of centralized networks.

Data as a Strategic Asset

Data is the key to unlocking EDTs for DND/CAF. Data, much like our natural resources, fuels immense economic growth for Canada. Canadian data must be appropriately secured through a proper digital trust infrastructure. This next decade will be fuelled by data and will itself fuel the creation of ever-more data-driven technologies. This reinforces the need for Canada to prioritize Canadian data across domains.

Given the fact that Canada's cyber infrastructure is almost exclusively owned by private firms, the threat of attacks in the cyber domain must be addressed using new data strategies and methods. In addition to defending Canada against foreign armies, Canadian national security now also means leveraging data as a strategic national asset. This means:

- Canadian data should be harnessed for the benefit of national defence and security.
- Certain data sharing/access should be restricted for national security purposes.
- Certain data/digital infrastructure should be classified as critical infrastructure having national security implications.
- Economic prosperity is directly linked to data governance and is critical to Canadian sovereignty and Canadian security.

Even as contemporary AI systems are limited to the narrow capacities of machine-learning algorithms, this limitation will not likely be true of future generations of AI. Optimizing the application of AI and other EDTs to DND/CAF will require an AI strategy that leverages data and especially platform computing for augmenting Canadian military capabilities.

Recommendations

- Protect and harness data as a strategic asset in rethinking the large centralized digital infrastructure that constitutes our current data architectures.
- Establish a secure data infrastructure that is interoperable, flexible, modular and resilient, and builds on the federated capacities of blockchain and other DLTs.

Enabling Pan-Domain C2

Together, AI and the proliferation of EDTs will almost certainly advantage "smart" states and non-state actors by capitalizing on the scaling effects of AI and autonomous systems. At the same time, modern non-linear and/or hybrid approaches to warfare and the actors that use them will make warfighting much less predictable. Responding to non-linearity in an increasingly networked environment requires context awareness and adaptation to allow pan-domain C2 to be more responsive, agile and resilient.

The growing scale and scope of data used in warfighting is undermining the human-centric

data-processing that once anchored industrial-era bureaucracies. Beyond vertically integrated systems, C2 is now increasingly dependent upon laterally scaling networks that drive decision making. Indeed, the accelerating pace of machine autonomy and other AI-driven applications suggests that conventional models of pan-domain C2 are becoming obsolete.[17]

The increasing computer-based execution of tasks demanded of military commanders will mean a dramatically tightened observe, orient, decide, act (OODA) loop[18] (see Figure 5). Taken together, the delegation of decision authority within mixed teams of humans and machines, the trust placed in machines, and experiments in optimization of human-machine teaming will be increasingly central to C2. Given the inherent risks in deploying new technology-mediated methods and systems, military personnel will need to understand the ramifications of AI in accelerating the OODA loop to speeds that potentially exceed human capabilities.

Applications of AI to the military domain will prove challenging to conventional C2 systems. Nonetheless, changes in the methodologies and resources underlying war in the twenty-first century do not alter the goals of pan-domain C2 (see Figure 6). Indeed, the goals remain the same: domain awareness, information dominance, decision superiority and global integration.

In response to this changing threat environment, the Defense Advanced Research Projects Agency has developed the concept of mosaic warfare to adapt conventional methods of C2. With the purpose of leveraging technology to support a more modular military ecosystem, mosaic warfare envisions a military that leverages resources that are cheap, flexible and highly scalable. Like the ceramic tiles in mosaics, individual warfighting platforms can be designed to be configurable. Formations leverage decentralized agents reconfigured across a "kill web" with the goal of avoiding the structural rigidity of "monolithic systems."

Like complex systems in nature, kill webs can leverage algorithms to eliminate single points of failure, accelerating response time through the application of modular design. Moving away from dominance (forecasting) and toward accelerating reaction (adaptation), mosaic warfare is designed to support hybrid military units that leverage lateral networks up and down a "decision-making stack."

Unlike the complex chess moves required in conventional warfighting, mosaic warfare leverages digital networks to accelerate dynamic response time using modular flexibility and augmented decision making (time compression). Together, AI, drones, sensors, data and personnel are combined to support operational commanders on the ground, making intelligence, resources and logistics assets available to small formations at an accelerated pace.

Complex Systems: Leveraging Exponential Growth

Taken as a whole, the data-driven algorithms and off-the-shelf software applications are reshaping the nature of C2. As AI-driven technologies become cheaper and more widespread, they will provide a broad range of state and non-state actors with platforms and tools to leverage algorithmic-learning engines in new and disruptive ways.

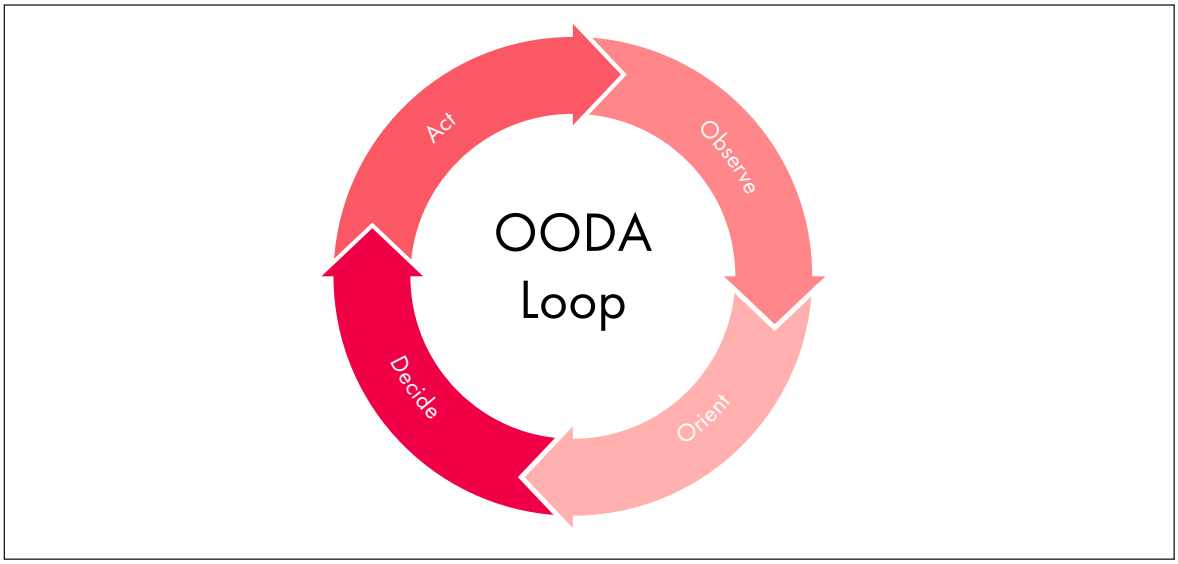
Given the fact that the manufacturing costs associated with drones and other digital technologies follow Moore's law (Singer 2012), we can assume that many of these technologies will enter the arsenals of sophisticated non-state actors. Affordable drones can be fitted with off-the-shelf weapons, and their sensors tethered to homegrown remote AI systems to identify and target human-like forms.

In the current technology environment, disruptions that build on data-driven networks will not follow linear rates of change but instead build on complex systems. Feedback loops that build on disruptive innovation and the decline of older technologies will drive exponential acceleration and the mass adoption of new technologies. In fact, this pattern holds for dozens

17 In the United States, for example, the Pentagon's first chief software officer resigned in protest at the slow pace of military transformation. As Nicolas Chaillan told the *Financial Times*, the failure of the United States to respond to technological change had put the country's future at risk (Manson 2021).

18 Note that virtually all the processes used by the different services and organizations, regardless of the name they take (kill chain, detect-to-engage sequence, joint engagement sequence and so forth) are just variations of this OODA loop.

Figure 5: The OODA Loop



Source: https://en.wikipedia.org/wiki/John_Boyd_(military_strategist).

Figure 6: Pan-domain C2

Domain awareness is now increasingly dependent on a network of sensors and systems to provide persistent and complete battlespace awareness from subsurface to space and cyberspace. Seabed surveillance systems (undersea), for example, enable ships to pull the radars and counter unmanned aircraft systems.
Information dominance increasingly means connecting data from all domain awareness sensors to flexible and responsible decision superiority. Ingesting aggregate processes means using AI and machine learning. Improving data gathering will mean bringing disparate and fragmented data into a cloud-based computing environment.
Decision superiority means giving senior leaders options that go beyond the kinetic kill into all levers of influence, including non-kinetic solutions. AI can assist with accelerating decision cycles.
Global integration is important for keeping the CAF relevant. Leveraging Canadian AI can provide a unique opportunity to support partners, in particular the United States (NORAD) and NATO.

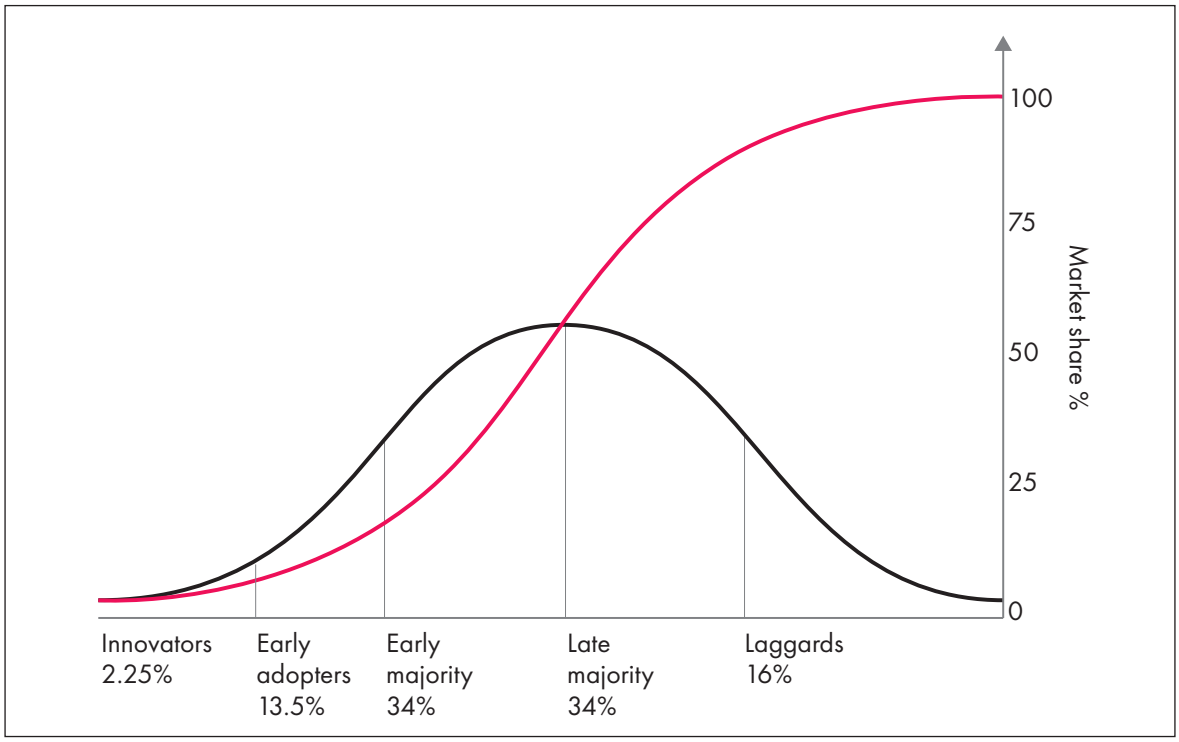
Source: Author.

of historical examples of disruption (Nagy et al. 2013) across all sectors and industries.[19]

These periods of disruption follow an S-curve (see Figure 7). Adoption of innovation is relatively slow at first but begins to accelerate dramatically at the knee of the curve. In a market economy, disruptions occur when incumbents heading toward the top of an old S-curve confront a new business model

19 For Austrian economist Joseph Schumpeter, this "creative destruction" (Kopp 2021) reflects the natural cycles of social transformation that evolve within market economies. Long periods of stability are often punctuated by abrupt technological and economic change that builds on GPTs triggering rapid economic and social transformation. Disruption occurs when a new technology of equal or greater capability (for example, the steam engine and the printing press) becomes available at a significantly lower cost than existing alternatives.

Figure 7: The S-Curve



Source: https://commons.wikimedia.org/wiki/File:Diffusionofideas.PNG.

at the bottom of a new S-curve.[20] New entrants entering a non-linear hypergrowth phase move up the curve before accelerating toward market saturation.[21] Underlying this innovation curve is the capacity of commercial firms to leverage "collective intelligence" (Bradley and O'Toole 2016) to quickly build new markets around a product or service.[22]

Closing the Gap: Harnessing the Canadian Technology Ecosystem

One of the most difficult challenges facing DND/CAF is the rise of a global technology industry that is now outpacing the capacities of the public sector. The implications of this market-driven transformation are difficult to overstate. China, for example, is becoming a major force in shaping AI by leveraging its enormous commercial market. China's AI is evolving quickly and will soon represent a major force multiplier for the Chinese military. As the country's broad range of startups, scale-ups and large corporations continue to close the gap with the United States, China will become a global leader in military AI.

National innovation necessarily depends upon institutional actors collaborating across sectors. For this reason, Canadian national security strategy must stress the need for coordinated flows of technology and information among people and institutions in driving long-term innovation. This kind of multi-domain collaboration has

20 Several models have been proposed for predicting technological change over time, but Wright's law has been the most accurate (Nagy et al. 2013). Pioneered by Theodore Wright in 1936, Wright's law states that for every cumulative doubling of units produced, costs will fall by a constant percentage. Perhaps the best model for making sense of this creative destruction is the S-curve. Developed by E. M. Rogers in 1962, the S-curve model is an attempt to understand how and why new ideas and products spread throughout cultures at an accelerated rate.

21 An additional and perhaps even more compelling explanation for this technological acceleration is the human capacity to improve performance through innovation. This process is defined as the "experience curve" or learn-by-doing. As Metcalfe's law dictates, the value of a network increases exponentially with the number of nodes or computers attached to that network. The global proliferation of digital technologies has introduced laterally scaling infrastructure for accelerating the speed at which human beings collectively learn.

22 One clear example of this collective intelligence over the past decade has been the rise of smartphones pioneered by Apple and Google – two companies with no previous experience in building mobile phones. Leveraging the convergence of battery technologies, touchscreen interfaces and digital platforms, Apple and Google were able to successfully disrupt numerous incumbents.

historically been defined in terms of a National System of Innovation (NSI) (Organisation for Economic Co-operation and Development 1997).

NSI policy and planning can take many forms, ranging from loose coordination to highly integrated partnerships. For example, the various NSI planning models applied in the United States (Atkinson 2020), China (Song 2013) and Europe (Wirkierman, Ciarli and Savona 2018) demonstrate the substantial economic and social returns inherent in maximizing government-industry-research partnerships. Government should work to build out Canadian technological capacity through tax incentives, procurement and research funding, and strategic planning. But it cannot act alone.

Tighter coupling between industry, government and academia is key to scaling Canada's technological and military capabilities. Notwithstanding the fact that Canada has world-class research in AI, quantum computing and clean energy technologies, these resources are not fully leveraged for the purposes of national security.

Strategic partnering between government and Canada's technology industry will be key to upgrading the military platforms (for example, war-gaming, modelling, fielding new autonomous and semi-autonomous systems, and data-enhanced decision-support systems) that will drive warfighting in the decades ahead. This will require:

- an extensive mapping of Canadian military AI/pan-domain C2 needs;
- stakeholder education and consensus building;
- the development of a formal DND AI strategic plan;
- specific funding allocations for research, engagement and staff;
- a DRDC and DND/CAF focus on building an agile and responsive ecosystem with innovative tools to engage industry, academia and other government departments in leveraging joint capabilities, speeding up procurement and facilitating access to top experts for short-term duration; and
- the institutionalization of governance mechanisms and oversight bodies.

Governing AI: Multilateralism and the Law

The ongoing evolution of AI reflects a step-change in the architecture, speed and complexity of a global technology market. This vast commercial landscape is increasingly borderless even as nation-states and rising regional powers compete for influence. The rise of China, Russia, India, Turkey, Iran and other regional powers suggests that international relations may no longer be based on a shared appreciation for a global rules-based order. For this reason, it has become critical to develop and promote the rules guiding the evolution and deployment of AI, particularly in the context of war.

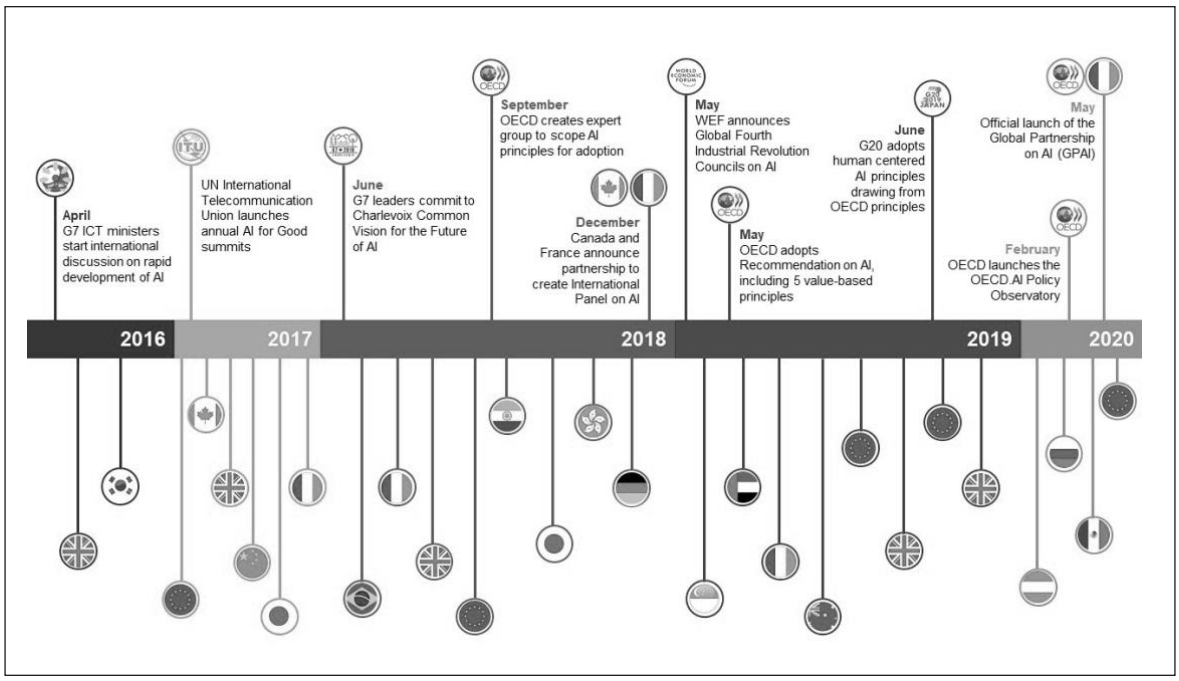
Governing AI and other EDTs is central to reducing the risk of future conflict across a multipolar order. Given the expanding rivalry between the United States and China, the need for treaties governing the use of LAWS and their proliferation could not be more timely. Developing guardrails in the evolution of military AI will be essential to reducing the potential for future conflict. The laws of war regulating the use of AI both in terms of the conditions for initiating wars (*jus ad bellum*) and the conduct of AI in war (*jus in bello*) remain to be determined.

Beyond unwarranted exaggerations on military AI, it is important to recognize the need for checks and balances in limiting both the concentration and proliferation of AI technologies (see Figure 8). AI remains limited to narrow-focused tasks. However, the need for common international rules and regulations in managing AI and other digital technologies will help to shape the pace and direction of AI as the technology matures.

Active engagement by Canada and other NATO countries in this discussion could be key to the future of global peace and security. As NATO's Advisory Group on Emerging and Disruptive Technologies (2020) observes, Canada and its allies should seek to promote, establish and participate in collaborative opportunities that enable a comprehensive architecture for the development and governance of AI. In 2018, Canada adopted the Declaration on Ethics and Data Protection in Artificial Intelligence, co-written by France, Italy and the European Union. Canada is also supporting the international ban on LAWS.

As a recent white paper from the World Economic Forum (2019) makes clear, global governance

Figure 8: Global Governance on AI



Source: Giardino (2020).

of EDTs remains a patchwork. Given Canada's middle-power status, Canada should look to align more closely with allies in Europe and elsewhere to instantiate democratic values in the development and regulation of AI.

Despite divergent views on AI and its weaponization, past negotiations such as treaties[23] on conventional weapons, nuclear arms control, and biological and chemical weapons can serve as a basis for future treaties defining the rules of AI and AI-driven warfare. Notwithstanding the daunting challenges that remain ahead, global governance has an important role to play in regulating military AI. In fact, Canada has already contributed to NATO's AI strategy (NATO 2021) to ensure that the deployment of AI is in accordance with the principles of lawfulness, responsibility and accountability.

Recommendations

- → Tighter coupling between industry, government and academia is key to scaling Canada's technological and military capabilities.
- → DND/CAF will need to harness decentralized networks for pan-domain C2. Military strategies that leverage decentralized agents across kill webs will have asymmetrical advantage over rigidly "monolithic systems."
- → The global governance of AI is fundamental to peace and security. Active engagement by Canada and other NATO countries in multilateral discussions on AI governance is needed to avoid future instability.

23 See www.armscontrol.org/treaties.

Conclusion

As AI, renewable energy technologies, quantum computing and space-based weapons come to the fore, pressure to adapt and transform the Canadian military will grow. In fact, Canada's current defence policy partly reflects this understanding in its call to adopt a range of new technologies. Indeed, Canadian defence planning has already begun incorporating remotely piloted drones and space-based surveillance assets into the national defence network (National Defence 2017).

However, a substantial challenge for DND/CAF over this decade will be appreciating the development and convergence of EDTs in new forms. The convergence of physical, digital and biological technologies represents the early stages of an enormous technological revolution with uncertain consequences. Much as in the past, emerging technologies will trigger widespread social, economic and military developments beyond their initial application.

For Canada to adapt and evolve within this changing technological landscape, government and industry must intentionally collaborate with each other and with international allies. In fact, no nation-state operating in isolation can expect to keep pace with the rapid expansion and diffusion of AI and other EDTs. As NATO's annual report on EDTs (NATO 2021) makes clear, keeping pace with technological change necessitates agility and rapid iteration with respect to the development, experimentation and application of technology.

While major advances in military and defence technologies were once generated in government laboratories or under government direction, innovations in AI and other EDTs are now largely the province of commercial industry. Leveraging technological innovation for the purposes of Canadian national defence must be part of a wider national innovation ecosystem that effectively integrates research and implementation.

In order for Canada to advance a national security posture tailored to the digital age, government, industry and academia will need to collaborate as an organic whole. Indeed, the most advanced national defence strategies (Canadian Association of Defence and Security Industries 2019) employed today necessarily bridge industry, academia and government in the incubation of frontier technologies.

Notwithstanding the fact that Canada has world-class research in AI, quantum computing and clean energy technologies, these resources are not fully leveraged for the purposes of national security. Part of the answer to resolving this challenge will involve the development of public infrastructure that can secure and govern a data-driven society. A rising digital economy is fuelled by data and will continue to drive the creation of ever-more data-driven technologies — especially AI. For this reason, Canadian military capacities will need to be recalibrated to reflect this reality.

Data is now the basis for Canadian national security. Upgrading government and military platforms around federated data networks will be important to transforming the single points of failure inherent to industrial-era bureaucracies. Stronger collaboration between industry, government and higher education is essential to scaling Canada's digital infrastructure.

Alongside military modernization, Canada must also work toward the goal of AI governance itself. The rise of military AI and autonomous weapons represents a very real shift in the nature of war. Unlike the substantial costs and planning needed to carry out conventional interstate conflict, the devastating impact of cyberattacks and drone strikes can be launched against critical infrastructure by small groups and non-state actors alike, with little more than a personal computer.

In addition to the enormous military potential of EDTs, these technologies also represent an inherent risk to global peace and security. Mistakes in the use of AI and other "smart systems" could — and very likely will — lead to catastrophic outcomes. Given the destructive potential of weaponized EDTs, it is critical that we consider the design of a comprehensive global architecture for managing their development.

Historically, Canada's capacity to influence other states has been tied to its support for coalition building and conflict management — particularly UN peacekeeping.[24] As Canadian scholar John Holmes suggests, the principal

24 See www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/psop.aspx?lang=eng.

characteristic of a middle power is its pursuit of solutions to international problems through institution building rather than through hard power or coercive diplomacy.

In the face of a rapidly evolving multipolar order, multilateral cooperation will be essential to ensuring peace and security. Information sharing, expert conferences and multilateral dialogue can help the world's nation-states and their militaries develop a better understanding of one another's capabilities and intentions in order to avoid future conflict.

Alongside the need for new and different resources and expertise, DND/CAF will need to balance a capacity for hard power with support for multilateral governance across a changing technological landscape. Amid a disparate assortment of fields and industries, the challenges we now face are not only facilitated by advances in science and technology but also represent new risks in and of themselves. What seems clear is that a rising era of geotechnological competition will be a major driver of great power rivalry (Goodman and Khanna 2013).

As a new generation of security threats continues to blur the traditional distinctions between land, sea, air, cyber and space, the goal for Canadian defence planning should be peace and security. Even as great power rivalry and a multipolar order reshape the contours of the global landscape, an expanding era of networks and data-driven algorithms has begun to transform traditional definitions of power. As a global middle power, Canada could be a major partner in managing these tensions.

Works Cited

Adams, John. 2016. "Canada and Cyber." Calgary, AB: Canadian Global Affairs Institute. www.cgai.ca/canada_and_cyber.

Andreessen, Marc. 2011. "Why Software Is Eating The World." *The Wall Street Journal,* August 20. www.wsj.com/articles/SB10001424053111903480904576512250915629460.

Atkinson, Robert D. 2020. "Understanding the U.S. National Innovation System, 2020." Information Technology & Innovation Foundation, November. www2.itif.org/2020-us-innovation-system.pdf.

Balsillie, Jim and Konstantinos Georgaras. 2021. "Prosperity & Security: Canada's IP Imperative, Featuring Jim Balsillie." Keynote address for 4th Annual IP Data & Research Conference, Centre for International Governance Innovation, March 11. Video, 40:18. www.cigionline.org/multimedia/prosperity-security-canadas-ip-imperative-featuring-jim-balsillie/.

Bergen, Peter, Melissa Salyk-Virk and David Sterman. 2020. "Introduction: How We Became a World of Drones" New America, July 30. www.newamerica.org/international-security/reports/world-drones/introduction-how-we-became-a-world-of-drones.

Berryhill, Jamie, Kévin Kok Heang, Rob Clogher and Keegan McBride. 2019. *Hello, World: Artificial intelligence and its use in the public sector*. November. Paris, France: Organisation for Economic Co-operation and Development, https://oecd-opsi.org/publications/hello-world-ai/.

Bradley, Chris and Clayton O'Toole. 2016. "An incumbent's guide to digital disruption." *McKinsey Quarterly*, May 18. www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/an-incumbents-guide-to-digital-disruption.

Bresnahan, Timothy F. and Manuel Trajtenberg. 1995. "General purpose technologies 'Engines of growth'?" *Journal of Economics* 65 (1): 83–108.

Canadian Association of Defence and Security Industries. 2019. *From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence*. Ottawa, ON: Canadian Association of Defence and Security Industries.

Carson, Lee and Brian Mersereau. 2022. "Canada Needs to Make NORAD Modernization a Priority." Opinion, Centre for International Governance Innovation, March 28. www.cigionline.org/articles/canada-needs-to-make-norad-modernization-a-priority/.

Congressional Research Service. 2020. *Artificial Intelligence and National Security*. November 10. https://sgp.fas.org/crs/natsec/R45178.pdf.

Fyffe, Greg. 2021. *Prepared: Canadian Intelligence for the Dangerous Decades*. Reimagining a Canadian National Security Strategy Report No. 6, Centre for International Governance Innovation, November 15. www.cigionline.org/publications/prepared-canadian-intelligence-for-the-dangerous-decades/.

Giardino, Elisa. 2020. "The mirage of a global framework for AI governance." Medium.com, November 7. https://medium.com/carre4/the-mirage-of-a-global-framework-for-ai -governance-35b88a36615c.

Global Advantage Consulting Group. 2021. "The Impact of Budget 2021 on the Performance of Canada's R&D/Innovation Ecosystem." April. https://globaladvantageconsulting.com/portfolio/canadas-rd-innovation-ecosystem-map-2021/.

Goodman, Marc and Parag Khanna. 2013. "The Power of Moore's Law in a World of Geotechnology." The National Interest, January 2. https://nationalinterest.org/article/the-power-moores-law-world-geotechnology-7888.

Government of Canada. 2018. *Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service*. www.canada.ca/content/dam/pco-bcp/documents/clk/Data_Strategy_Roadmap_ENG.pdf.

Holmes, John W. 1979. *The Shaping of Peace: Canada and the Search for World Order, 1943–1957*, vol. 1. Toronto, ON: University of Toronto Press.

Jovanovic, Boyan and Peter L. Rousseau. 2005. "General Purpose Technologies." In *Handbook of Economic Growth,* 1st ed., vol. 1, edited by Philippe Aghion and Steven Durlauf, 1181–224.

Kania, Elsa B. 2017. *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*. Center for a New American Security. November 28. www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power.

Khan, Imtiaz and Ali Shahaab. 2020. "Estonia is a 'Digital Republic' — What that Means and Why It May Be Everyone's Future." SingularityHub, October 15. https://singularityhub.com/2020/10/15/estonia-is-a-digital-republic-what-that-means-and-why-it-may-be-everyones-future/.

Kopp, Carol M. 2021. "Creative Destruction." Investopedia, June 23. www.investopedia.com/terms/c/creativedestruction.asp.

Lee, Kai-Fu. 2018. *AI Superpowers: China, Silicon Valley, and the New World Order*. New York, NY: Harper Collins.

Li, David and Eleonore Pauwels. 2018. "Artificial Intelligence for Mass Flourishing." Our World, October 15. https://ourworld.unu.edu/en/artificial- intelligence-for-mass-flourishing.

Lucas, Louise and Emily Feng. 2017. "China's push to become a tech superpower triggers alarms abroad." *Financial Times*, March 19. www.ft.com/ content/1d815944-f1da-11e6-8758-6876151821a6.

Manson, Katrina. 2021. "US has already lost AI fight to China, says ex-Pentagon software chief." *Financial Times*, October 10. www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0.

McCoy, Alfred W. 2021. *To Govern the Globe: World Orders and Catastrophic Change*. Chicago, IL: Haymarket Books.

Modigliani, Pete, Dan Ward, Tyler Lewis and Wayne McGee. 2020. *Modernizing DoD Requirements: Enabling Speed, Agility, and Innovation*. MITRE Center for Technology and National Security. March. www.mitre.org/sites/default/files/publications/pr-19-03715-2-modernizing-dod-requirements-enabling-speed-agility-and-innovation.pdf.

Nagy, Béla, J. Doyne Farmer, Quan M. Bui and Jessika E. Trancik. 2013. "Statistical Basis for Predicting Technological Progress." *PLoS ONE* 8 (2): e52669.

National Defence. 2017. *Strong, Secure, Engaged: Canada's Defence Policy*. Ottawa, ON: Government of Canada. http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf.

———. 2021. "Joint Statement on Norad Modernization." August 14. www.canada.ca/en/department-national-defence/news/2021/08/joint-statement-on-norad-modernization.html.

National Intelligence Council. 2021. *Global Trends 2040: A More Contested World*. March. www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

National Security Commission on Artificial Intelligence. 2021. *National Security Commission on Artificial Intelligence Final Report*. https://assets.foleon.com/eu-west-2/uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf.

NATO. 2021. "NATO releases first-ever strategy for Artificial Intelligence." News release, October 22. www.nato.int/cps/en/natohq/news_187934.htm.

NATO Advisory Group on Emerging and Disruptive Technologies. 2020. *Annual Report 2020*. Brussels, Belgium: NATO. www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf.

Office of the Prime Minister. 2019. Letter from Prime Minister Justin Trudeau to Minister of National Defence Harit Sajjan, December 13. https://pm.gc.ca/en/mandate-letters/2019/12/13/archived-minister-national-defence-mandate-letter.

Organisation for Economic Co-operation and Development. 1997. *National Innovation Systems*. Paris, France: Organisation for Economic Co-operation and Development Publications. www.oecd.org/science/inno/2101733.pdf.

Public-Private Analytic Exchange Program. 2019. *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar*. www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.

Rice, Nikolai F. 2019. "Estonia's Digital Embassies and the Concept of Sovereignty." *Georgetown Security Studies Review*, October 10. https://georgetownsecuritystudiesreview.org/2019/10/10/estonias-digital-embassies-and-the-concept-of-sovereignty/.

Romei, Valentina and John Reed. 2019. "The Asian century is set to begin." *Financial Times*, March 25. www.ft.com/content/520cb6f6-2958-11e9-a5ab-ff8ef2b976c7.

Singer, Peter W. 2012. "Rise of the Machines: Drones as the Next Game-changer." Brookings, September 4. www.brookings.edu/on-the-record/rise-of-the-machines-drones-as-the-next-game-changer/.

Slaughter, Matthew J. and David H. McCormick. 2021. "Data Is Power: Washington Needs to Craft New Rules for the Digital Age." *Foreign Affairs*, May/June. www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age.

Song, Hefa. 2013. "China's National Innovation System." In *Encyclopedia of Creativity, Invention, Innovation and Entrepreneurship*, edited by Elias G. Carayannis. New York, NY: Springer.

Stanley, Jay. 2012. "Drones: The Nightmare Scenario." ACLU (blog), May 12. www.aclu.org/blog/national-security/privacy-and-surveillance/drones-nightmare-scenario.

Thales. 2021. "NATO Selects Thales to Supply Its First Defence Cloud for the Armed Forces." Press release, January 25. www.thalesgroup.com/en/group/journalist/press-release/nato-selects-thales-supply-its-first-defence-cloud-armed-forces.

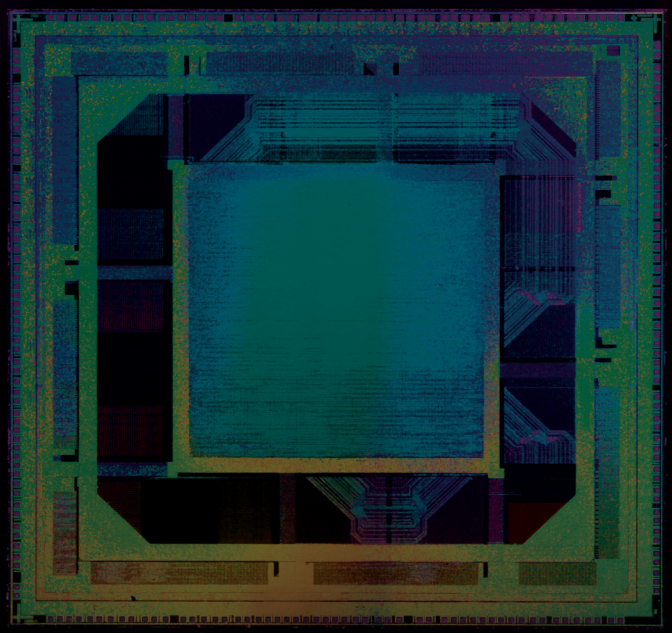
United States Department of Defense. 2018. "Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge." https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Wirkierman, Ariel L., Tommaso Ciarli and Maria Savona. 2018. "Varieties of European National Innovation Systems." ISI Growth Working Paper. www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/08/Wirkierman-et-al.-2018-Varieties-of-EU-National-Innovation-Systems-132018-ISIGrowth-WP.pdf.

World Economic Forum. 2019. "Global Technology Governance: A Multistakeholder Approach." World Economic Forum White Paper. October. www3.weforum.org/docs/WEF_Global_Technology_Governance.pdf.

World Intellectual Property Organization. 2021. "China Leads the World in AI Related Patent Filing." September 28. www.wipo.int/about-wipo/en/offices/china/news/2021/news_0037.html.

Zegart, Amy. 2021. "American Spies Are Fighting the Last War, Again." *The Atlantic,* September 6. www.theatlantic.com/ideas/archive/2021/09/us-intelligence-osama-bin-laden/619781/.



Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org