ON TRACK

Conference of Defence Associations Institute

L'Institut de la conférence des associations de la défense

National Security in the Age of AI and Robotics

Volume 35 | January 2025

ON TRACK

Volume 35 | January 2025

ON TRACK is the official journal of the CDA Institute. Through its pages, the CDA Institute promotes informed public debate on security and defence issues and the vital role played by the Canadian Armed forces in society. ON TRACK facilitates this educational mandate by featuring a range of articles that explore security, defence, and strategic issues that may have an impact on the Canadian strategic interests and on the safety of its citizens. The views expressed in ON TRACK are those of the authors and do not necessarily represent those of the CDA Institute.

CDA Institute / L'Institut de la CAD
701-350 Sparks Street, K1R 7S8, Ottawa, ON
(613) 236-9903
https://cdainstitute.ca/

On the Cover

Combat Camera / Flickr
"Ex Northern Challenge"
Photo by Corporal Sébastien Lauzier-Labarre, Canadian Forces Combat Camera
https://www.flickr.com/photos/cfcombatcamera/54213921842/

TABLE OF CONTENTS

National Defence and Security in the Age of AI and Robotics

Daniel Araya, PhD

Accelerating advancements in artificial intelligence (AI) and robotics have ushered in a new era in Canadian security planning. Like the Cold War, the race to develop military applications based on advanced science and technology has provoked a bifurcation in the world's research ecosystem and a rupture in the global security environment. Indeed, the convergence of high-performance computing and recent advancements in machine learning are beginning to fundamentally alter the global balance of power (DARPA, 2020; Antal, 2023).

Notwithstanding the fact that technological innovation has always shaped the nature of power, the scale and velocity of investment in AI is unprecedented. Global annual spending on AI is forecast to reach $826.70 billion by 2030 with an annual growth rate of 28.46 percent over that same period (2024-2030). Techniques such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are now instrumental in image recognition, natural language processing (NLP), time-series analysis, and human-machine integration.

Nations around the world now find themselves confronted by a new multipolar order in which AI and robotics are not merely tools for economic influence but instruments for military predominance. AI is predicted to transform command-and-control systems, intelligence gathering and analysis, target recognition, and information warfare. This transformation not only challenges conventional notions of military primacy but also introduces new ethical and legal dilemmas regarding government accountability, national autonomy, and military escalation.

This series of essays underscores the dual-use nature of AI and the need for strategic planning in adapting Canadian military affairs to an era of "machine intelligence." How do governments today navigate a technology arms race in which code, rather than conventional weaponry, becomes the decisive factor in military primacy? What does accountability look like in an era in which machines execute military decisions? And, most pressingly, what resources are needed to revitalize the Canadian military for an era of AI and robotics?

Over the course of this decade and the next, Canadian security planners are likely to face a highly volatile security environment in which a new geopolitical reality has begun to reconfigure the landscape of global security. At the center of the new reality lies an escalating rivalry between the United States and China. As Australia's Strategic Policy Institute (Leung et. al., 2024) concludes, China's meteoric rise as a global technology superpower is a stark reminder that technological capability is synonymous with military prowess (Kania, 2020). Through global infrastructure planning like the Belt and Road Initiative (BRI) and sizeable investments in "military-civilian fusion," Beijing is not only reshaping the international security environment but provoking a tectonic shift in the global order.

A New Balance of Power

Historically isolated by geography and shielded by membership in the North Atlantic Treaty Organization (NATO), Canadian security planning must now adapt to an era of accelerating technological change. While Canadian policymakers have historically taken a "wait and see" approach to policy and planning, this is no longer a strategic option. In this new era, lines are not merely drawn by geography or nation but by algorithms, software ecosystems, and data.

As AI and robotics ascend from the research frontier to operational reality, these technologies are challenging longstanding assumptions about the boundaries of national security. Indeed, the emerging horizon of AI represents more than a shift in technology, it represents a profound reconfiguration in the architecture of global security. Together, the distinguished authors in this collection explore the consequences of this new geopolitical environment and the need for strategic planning moving forward.

The collection begins with a sobering analysis by Defence Research and Development Canada (DRDC) on the rise of China as a great power and the need to advance Canada's defence industrial base. Building on this important discussion, Canadian economist Dan Ciuriak explores the contours of military procurement in the context of "machine knowledge capital." This is followed by a thoughtful evaluation of the rapidly changing frontiers of space and cyber by retired Brigadier General Roberto Mazzolin. As retired US Army Officer and university lecturer Amos Fox explains, no nation is an island today. In his view, data-driven military systems are best understood in terms of strategic interoperability. Finally, researchers at DRDC introduce "Mockingbird," a technology prototype for managing AI-driven information warfare.

As these experts make clear, Canadians must now confront hard questions about our country's strategic vulnerabilities. As nations around the world weaponize AI and robotics for cyber warfare, machine autonomy, and mass surveillance, the global order is being reconfigured. During the Cold War, countries were often obliged to align with either the Soviet Union or the United States, leading to competing economic and military alliances. Much as then, the current AI race is fomenting the creation of ever-larger spheres of influence, forcing nations to align across complex gravity wells of data and computation.

As the world's leading nations compete for dominance over AI, geopolitical rivalry is becoming a central feature of a multipolar world order. Given the dangers of military escalation, the authors in this collection explore the vulnerabilities and risks of falling behind in the application of AI and robotics to Canadian security planning. Notwithstanding the ethical dilemmas posed by military AI, Canadians must grapple with the pressing issue of multipolarity and a world in which AI systems threaten to undermine Canadian sovereignty.

Conclusion: What Role for Canada?

Unlike the bipolar order of the Cold War or the unipolar order of American hegemony, today's technology arms race stretches across a complex security landscape that is embedded in every layer of the global economy. Much as the industrial revolution, computational technologies have begun to catalyze a widespread social and economic transformation. Not surprisingly, AI has fomented a complicated discussion about the future of Canadian national security. Beyond the United States and China alone, an increasing number of states can be expected to develop and procure AI-driven weapons systems (Ashford and Cooper 2023). Indeed, the challenge of a multipolar

world order is its very unpredictability.

What is clear is that Canadian national security is at a crossroads. Even as the world's most powerful nations compete to augment conventional military assets, the fabric of international relations is unwinding. Like the Cold War, technological competition between the United States and China promises to reshape the global balance of power. Unlike the Cold War, the global order is no longer unipolar or even bipolar, it is multipolar. In the decades ahead, spin-off technologies overlapping algorithms and electronics will diffuse to countries around the world, resetting the conditions for international peace and security. Nations that lead in the weaponization of AI and robotics can be expected to shape the global norms surrounding the technology.

Of course, AI and robotics are not limited to military applications but extend into economic development and social control, blurring the boundaries between military and civilian applications. The same algorithms that optimize supply chains or predict natural disasters can now coordinate complex drone attacks or enhance mass surveillance. Unfortunately, conventional forecasts on technological change often make the common assumption that disruptive technologies like AI and robotics simply replace older technologies on a one-to-one basis. The hard reality is that general-purpose technologies frequently subsume older systems with dramatically new boundaries and capabilities.

The essays in this important collection expose the fault lines of this new reality. From the integration of autonomous weapons systems into national defence to the need for global governance on commercial AI, the decisions made today will shape not only our nation's security but also our broader role in a new global order. Canadian policymakers will need to chart a pragmatic course in this new security environment. While this is a role familiar to many Canadians, AI and robotics represent a unique challenge because the bulk of research and development is happening outside the public sector.

The truth is that AI has become a powerful driver of commercial innovation with enormous implications for global governance. Beyond military and security planning alone, AI governance will require a range of international partnerships in the development of common protocols on AI and a common regulatory language. Indeed, Canada's diplomatic and political heft will need to bridge a wide topography of academic, commercial, and security partnerships in the pursuit of a new multilateral system.

As a leader in AI research and a key member of inter-governmental organizations, Canada will need to pay particular attention to its strategic role in shaping military AI. As we navigate this new era, the insights offered in this collection will hopefully spark both policy debate and a shared concern for ensuring that advancements in AI and robotics strengthen, rather than undermine, the foundations of Canadian national security.

I encourage readers to critically engage with these perspectives in order to raise concerns with regard to how we shape the contours of Canadian security in the 21st century. The challenges posed by AI and robotics demand more than just technical solutions to national security. They demand a deep commitment to the principles that define our culture and society: transparency, democratic accountability, and respect for the rule of law.

Daniel Araya

Dr. Daniel Araya is senior partner with the World Legal Summit and senior fellow with the Centre for International Governance Innovation (CIGI). His work focuses on artificial intelligence and public policy and their impact on a changing global order. Dr. Araya is a regular contributor to various media outlets and policy organizations including Forbes, The Brookings Institution, The National Post, Futurism and Singularity Hub. He has been invited to speak on news and media programs such as Deutsche Welle (DW) and TRT World, and has given presentations at Harvard University; Stanford University; the American Enterprise Institute; the US Naval Postgraduate School; the Canadian Department of National Defence; the Center for Global Policy Solutions; and Microsoft Research. His most recent books include Augmented Education in the Global Age (2023); Augmented Intelligence: Smart Systems and the Future of Work and Learning (2018) and Smart Cities as Democratic Ecologies (2015). He has a doctorate from the University of Illinois at Urbana-Champaign.

References

Antal, John. 2023. *How We Fight the Next War: Reimaging How We Fight*. Havertown, PA: Casemate Publishers.

Ashford, Emma and Evan Cooper. 2023 "Yes, the World Is Multipolar," *Foreign Policy*, October 5. https://foreignpolicy.com/2023/10/05/usa-china-multipolar-bipolar-unipolar/.

DARPA. 2020. "Creating Cross-Domain Kill-Webs in Real Time." 10 April. https://www.darpa.mil/news-events/2020-09-18a.

Kania, Elsa B. 2020. "AI Weapons in China's Military Innovation", *Brookings, Global China Project*, April. www.brookings.edu/articles/ai-weapons-in-chinas-military-innovation/ .

Leung, Jennifer Wong, Stephan Robin, and Danielle Cave, "ASPI's two-decade Critical Technology Tracker: The rewards of long-term research investment." *Australian Strategic Policy Institute*, August 2024. https://www.aspi.org.au/report/aspis-two-decade-critical-technology-tracker.

Statista. 2024. "Artificial Intelligence: Worldwide – Market Size." Accessed January 23, 2025. https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide#market-size.

Militarizing AI: How to Catch the Digital Dragon?

Kurtis H. Simpson, Raphael Racicot, Samuel Paquette, Samuel Villanove, and Adam MacDonald (Researcher)

The global spread of Artificial Intelligence (AI) is now ubiquitous.[1] No single technology is having the pervasive impact that AI currently exerts over our individual lives. It is shaping decision-making, accelerating information flows, augmenting surveillance, improving intelligence gathering, changing communications, redefining data management, empowering analysis, and altering social behaviours.[2] The magnitude of this change is reflected in the investments being made. Global annual spending on AI, including enabled applications, infrastructure, and related IT (as well as services) is currently estimated at US$235 billion. This is expected to increase to US$632 billion by 2028 (Massey and Fang 2024). As a subset of this global transformation, AI holds the potential to fundamentally redefine modern warfare (Motwani 2024; Hirsh 2023; Lushenko 2023; Araya 2022; Takagi 2022).

In the face of this inescapable reality, Canada's military is adapting. In 2024, the Department of National Defence (DND) and the Canadian Armed Forces (CAF) published its first ever *Artificial Intelligence Strategy* (Department of National Defence 2024a). While an important departure point, the rate of the ongoing AI transformation and its subsequent incorporation by militaries around the world in various capacities necessitates further critical thinking, open debate, problematization, long-term planning, and creative policy options.

The purpose of this essay is fourfold. It is first necessary to familiarize the reader with the extent to which, and how, AI is becoming militarized. Second, consideration will be given to both the threats posed by adversaries, and the opportunities available for collaboration with partner countries in addressing AI as a novel, emerging, and disruptive technology (EDT). Third, Canada's national AI program, industry potential, and the proposed way forward by the DND/CAF will be explored to inform follow-on deliberations and possible recommendations. Finally, the potential for multinational military alliance organizations, most notably NATO, will be considered as an enabler in Canada's response to what some consider the next revolution in military affairs (Kania 2021).

The speed of AI development in military ap-

1 For a comprehensive index of countries, AI trends, and analysis see: (Nester Maslej et.al. 2024). Oxford Insights also provides a useful online source evaluating 193 countries and AI adoption across 39 indicators and three pillars including: government, the technology sector, as well as data and infrastructure.

2 One only need consider changes in transportation (autonomous vehicles), banking and finance (automated trading), law enforcement, social and behavioral sciences (fraud detection), life and medical sciences (bioinformatics, biological engineering), communications (language translation), education (adaptive learning tools), marketing (social media and sentiment analysis), energy management, manufacturing, public health (robotic controls, diagnostics and remote treatment), as well as security (anomaly detection/surveillance and authentication).

plications, its omnipresent nature, and its profound potential consequences have ushered in an era increasingly described as an "Oppenheimer moment."[3] Reportedly, some 60 counties have now developed national AI strategies of some type, and another 15 countries are progressing towards this goal (Stanford University 2023). National AI strategies are typically the driver behind military AI strategies. Worldwide estimates of military spending on AI indicate it has increased from US$4.6 billion in 2022, to US$9.2 billion in 2023, and is forecasted to reach US$38.8 billion by 2028.[4]

There is a relatively short list of countries leading in the research and testing of military AI applications.[5] Typically, the US, China, and Russia are considered the quantitative and qualitative 'tier one' military AI powers.[6] American military AI spending, for example, is now close to US$2 billion annually, with an additional US$1.7-3.5 billion on unmanned and autonomous systems. Likewise, expenditures on AI-enabled systems in the People's Republic of China (PRC) are estimated to be comparable (The Economist 2024). While Russian investments are far less (and difficult to accurately project) legislators recently approved a 30% increase in military outlays for 2025. Vladimir Putin views AI as critical for reducing a growing capability gap with the West, believing Russian security and sovereignty vulnerable to high-tech threats. He personally considers AI leadership a necessary part of retaining Moscow's international reputation as a Great Power (Zysk 2024).[7] In short, a comparative analysis of 25 countries across the globe indicates that the practice of militarizing AI is increasingly fluid and dynamic (Borchert et al. 2024). Large capital outlays are redefining military-industrial complexes as small, dynamic firms and start-ups have gained new ground (particularly in countries like India, the UK, Germany, South Korea, and France) over traditional defense behemoths and large defence focused State-Owned Enterprises (SOEs) (Brenes and Hartung 2024). While similarities often exist between countries, each individual state's adoption of a technological innovation path occurs uniquely within context specific conceptual, cultural, organizational, and operational transformations.

What Exactly is Militarized AI?

Military AI defies an easy and widely accepted definition. For the DND/CAF, AI is considered "the capability of a computer to do things that are normally associated with human cognition, such as reasoning, learning, and self-improvement" (Department of National Defence 2024a, 4). It is a means to solve a problem, not an end in itself. Central to this is the ongoing evolution of associated technologies.

NATO's Science and Technology Organization (STO), drawing on the research of the US Defense Advanced Research Projects Agency (DARPA), categorizes AI in terms of 'waves.' The first is 'knowledge-based' which relies on "rules-based deci-

3 AI's rapid development trajectory has outpaced international regulatory frameworks and is often compared with the challenges nuclear arms control faced immediately following the first successful tests and use of such weapons. As Muhammad Ali Baig and Anum A. Khan argue, an effective international legal system is needed to manage technological competition (particularly between the US and China) to reduce the risk of accidental or inadvertent war. See: (Baig and Khan 2024).

4 See, for example: (MarketsandMarkets 2024).

5 The US Department of Defence (DoD) has increased its spending on AI contracts according to estimate by 193% between 2022 and 2023. See (Larson et al. 2024).

6 For a comparative evaluation of these three countries see: (Hynek and Solovyeva 2022).

7 For an overview of Russia's AI development also see: (Rudd 2024).

sion-making, facilitating automation by using expert knowledge hand-crafted by humans and a number of if-then statements to dictate their actions. Knowledge-based systems cannot reason about situations outside of their carefully crafted if-then knowledge, nor can they learn from their experiences…" (Gray and Ertan 2021, 8).

The second-wave builds on probabilistic methods, statistical learning, and big data. "This type of AI includes machine learning (ML) and its sub-set deep learning (DL). Second-wave or 'data-based' AI systems solve specific problems by using statistical models that are trained on large, sometimes pre-labelled data sets. Data-based machine learning algorithms include supervised, unsupervised, and reinforcement learning. Data-based AI models are entirely reliant on the data they are trained on" (Gray and Ertan 2021, 8).

The third-wave aims to produce contextual adaptation and common-sense capabilities. DARPA asserts that this next generation of AI will be able to understand context, leverage that contextual understanding for common sense reasoning, and adjust to changing circumstances. Purportedly, this will enable more natural language interactions, improved reasoning skills, as well as adaptation to new tasks and situations, improving real-world interaction as AI systems merge with human-level cognition.[8] These three evolutionary stages are summarized by DARPA as (1) Describe (handcrafted knowledge), (2) Categorize (statistical learning), and (3) Explain (contextual adaptation) (Launchbury 2018).

The Military Uses of AI

AI's potential as a suite of technological tools enabling militaries is frequently oversold as 'revolutionary,' 'game-changing' and 'perilous,' but by any measure the difference is almost certainly profound and still unknowable (Brands 2024).[9] Adherents assert it will improve operational efficiency, facilitate autonomy, enable more informed military decision-making, and increase the velocity and scale of military actions (Congressional Research Service 2020). At the root of all these domains is a qualitative improvement in the capacity, speed, efficiency, accuracy, and scope of effective data management and processing.

Current military applications of AI can be broken down into eight broad categories (Araya and He 2024). These include: command and control; intelligence, surveillance and support (ISR); simulation and training; automated target recognition; autonomous systems and vehicles; information operations and electronic warfare; predictive maintenance and logistics; and finally medical applications.

Each will be briefly outlined in turn.

Command and Control: Given AI's capabilities to efficiently process large volumes of data, AI could improve strategic decision-making by assisting with complex assessments. Applications include enhanced risk assessments, smart virtual assistants, and an augmented capacity to anticipate the intent of potential adversaries.

Intelligence, Surveillance, and Reconnaissance (ISR): AI is further improving intelligence analysis and threat monitoring by identifying patterns in large datasets. This could include leveraging AI to conduct social media analysis, anomalous behavior detection, image recognition, or improving automated reasoning for intelligence. Predictive models using Machine Learning (ML) can identify weak signals, which might significantly alter the course of military opera-

8 This explanation is summarized online by MixedMode.
9 For a related discussion see: (Lushenko and Carter 2024).

tions.

Simulation and Training: When paired with virtual and augmented reality systems, AI has the potential to provide real-time adapted and customized training to individuals.[10] Other applications include virtual wargaming and improved human performance.

Automated Target Recognition: AI may improve rapid detection and identification of chemical, biological, radiological, and nuclear (CBRN) threats (as well as other targets) through data fusion and analysis.

Autonomous Systems and Vehicles: The integration of AI into air, sea, and weapons systems will also enhance weapons' navigation, sensor data, and surveillance. In weapons systems, AI applications can improve trajectory planning, collision avoidance, or cross-cueing. AI can also be leveraged for drone swarm operations, autonomous convoy and resupply vehicles, as well as robotics.

Information Operations and Electronic Warfare: AI may be utilized to conduct offensive and defensive cyber operations. It also aids in the analysis of intelligence data in the information space. In cybersecurity, AI can help build resilient networks and stop denial of service attacks (DoS) (Rashid et al. 2023, 15). Generative AI may also be used for cognitive electronic warfare, or to develop malware.

Predictive Maintenance and Logistics: Including AI in logistics planning will minimize equipment downtime and systems failures by analyzing sensor data and historical maintenance records of military vehicles. It can also plot and predict the most efficient supply routes for ammunition, troops, and goods.

Medical: Wearing equipment with AI capabilities permits real-time health monitoring and for difficult diagnosis to occur through the scanning of body temperature, heart rate, and electrocardiograms (Rashid et al. 2023, 15).

In light of the increasing number of military AI applications, an overriding concern for Canada is effectively assessing adversarial intent and capability. As so explicitly stated by Canada's recently retired Chief of Defence Staff (CDS), General Wayne Eyre, "China and Russia are Canada's main enemies, with both nations considering themselves to be at war with the West" (Pugliese 2023). Russia is framed as the immediate tactical threat in Europe, whereas China is viewed as the global strategic threat facing Canada. Of the two countries, China must be prioritized given its accelerating rate of military modernization, its threat potential to the most economically vibrant region in the world (and Canada's profound stakes in the Indo-Pacific region), as well as the Chinese Communist Party's national priority of employing non-kinetic military weapons (like AI) to win decisive victories at the earliest possible stages of conflict, most notably with the reunification of Taiwan to the mainland.[11]

China's Militarized AI Ambitions

Even though the US has had an important first-mover advantage in the field of AI, strategic competitors (read China) are mobilizing quickly to close the gap (Johnson 2021, 352). Understanding its motivation begins by first appreciating key tenets of the PRC's worldview.[12] Distilled down, the Chinese Communist Party (CCP) sees the current global order as dominated by strategic competition between rival

10 This section draws heavily on: (Gray and Ertan 2021, 14).

11 The primacy of China's threat potential is recognized widely by the US, NATO, and Canada's Department of National Defence. See, for example: (Peters and Beaver 2024).

states. It considers the East and West locked in a clash of opposing ideological and economic systems. Under the existent Rules-Based International Order (RBIO), Beijing considers itself disadvantaged and the national interests of 'the Global South' more generally overlooked. Feeling increasingly encircled and besieged, the current leadership is preoccupied by augmenting China's comprehensive national power (Drinhausen and Legarda 2022). Science, technology and innovation are deemed determining enablers in what Beijing refers to as 'the Chinese dream,' or the mainland's national rejuvenation and its restoration as a leader in international affairs.

Chinese President Xi Jinping has championed Science and Technology (S&T) as foundational in enabling 'China's rise' since his assumption of power in 2012. He defines the hi-tech sector as the "main battlefield" in superpower rivalry and has prioritized making the PRC a global scientific and innovation leader by 2035. As evidence of this commitment, in 2023 Chinese research and development (R&D) spending increased by 8% to US$458.5 billion annually (Xinhua 2024). Moreover, it has launched a US$1.4 trillion plan over the next six years to supplant the US as the world's innovation leader with a focus on AI (Jiang 2024). The rate of progress has been prodigious. Australia's authoritative technology tracker at the Strategic Policy Institute (ASPI) indicates that the PRC now leads the world in 57 of 64 critical technologies.[13] AI is chief among them.

Senior Chinese leadership prioritize AI as a tool, enabler, or methodology as it applies to and enhances other technologies spanning defence, space, energy, the environment, biotechnology, robotics, cyber, computing, advanced materials, nuclear, and quantum domains. For the military, AI synergizes across domains and platforms in truly novel ways, portending 'asymmetric advantage.' It is not a simple enhancement of kinetic capability, but rather a transformational approach to a full spectrum of conflict scenarios.

Xi's commitment to ongoing and long-term modernization of the People's Liberation Army (PLA) is deemed integral to the country's international standing, domestic stability, and the continued rule of the CCP (Heat 2023). Specific benchmarks are well documented, culminating in 2049 with the full transformation of the PLA into a world-class fighting force.[14] AI advances are fundamental in each of these developmental stages.[15]

China's robust AI trajectory traces its origins to the early 2000s. It is now being implemented as a core aspect of the PLA's ongoing transition from *mechanization* to *informatization,* ultimately culminating in the *intelligentization* of warfare.[16] As summarized by Stokes, "…mechanization refers to fielding modern platforms and equipment; informatization refers to linking those systems to networks such as GPS; and intelligentization refers to integrating artificial intelligence, quantum com-

12 The main tenants of this perspective are captured ad passim in the US DoD's annual publication entitled Military and Security Developments Involving the People's Republic of China.

13 As an indicator of the rate of change, China led in just three of 64 technologies from 2003–2007. See: (Leung et al. 2024).

14 The PRC's goals for modernizing its armed forces in the "New Era" are anchored to three core dates, 2027, 2035, and 2049.

15 The specific primacy AI holds was evident in China's 14th Five-year Plan (2021-2025) where it ranked first among "frontier industries." China's "New Generation AI Development Plan" elevates AI as a whole-of-nation and whole-of-military strategic priority as it seeks to be the world's leader in AI by 2030.

16 For a very good contextualization of this development, see: (Rira 2021).

puting, big data, and other emerging technologies into the joint force"(Stokes 2024).[17] This priority has increasingly become affirmed in official state Five-Year Plans, CCP public statements, military doctrine, and a new 2021 core operational concept, called "Multi-Domain Precision Warfare" (MDPW) (Osborn 2023).

In simple terms, MDPW leverages C4ISR and incorporates big data and AI into what the PLA refers to as a "network information system-of-systems," to rapidly identify key vulnerabilities in the operational systems of opposing forces, and then using combined joint forces to initiate strikes against identified vulnerabilities, like networks and satellites. A review of known areas where the PLA is currently adopting AI serves as a bellwether to important trendlines.

Recognizing that 'gaps' exist, open-source analysis has convincingly verified domains (as well as specific technologies) clearly prioritized by the Chinese military. These include: autonomous vehicles (air, land, and sea), intelligence analysis, information warfare, logistics, training, command and control, target recognition, and ISR (Fedasiuk et al. 2021).[18] Other research highlight the fields of wargaming, cyber, unmanned weapons (most notably drones), space, sensors, nuclear missile mobility, early-warning, as well as offensive and defensive capabilities in the nuclear domain (Takagi 2022). While concerning, our proclivity to focus on the 'known-knowns' or AI applied to software, hardware, and tangible systems vulnerabilities is at the risk of what is more important—our understanding of what comes next.

Although the PLA's escalating modernization anticipates a potential requirement for a direct military-to-military conflict with the US and other Western countries in future scenarios, China's preferred option is to 'win without fighting' vis-à-vis strategic influence campaigns, overt and covert media manipulation, lawfare, grey zone tactics, hybrid operations, and armed coercion. Cognitive warfare is considered the next evolution of this approach, fully enabled by AI (Rira 2021).[19]

In its ongoing quest to secure operational advantage, China's leadership is increasingly focused on new theories, capabilities, and technologies. One such vector of particular interest is harnessing the plausible synergies between brain science, biotechnology, and AI in addressing human-machine interfaces (Kania 2020). Following increasingly centralized Party direction, new pools of researchers are being directed to explore the interface between AI and human intelligence through linkages with other cutting-edge interdisciplinary technologies.[20] "Hybrid intelligence" is proposed as a means of better coping with the complexity and acceleration of operational tempo and its associated cognitive challenges. Likewise, a focus on the cognitive domain (empowered by AI) further holds the potential advantage of more effectively undermining both an adversary's *will* and its *resolve*.

In short, the spheres of military operations are expanding from the physical domain and the informational domain to that of consciousness as well (Fuchu 2017).[21] While this new frontier

17 Also see: (Fravel 2015).
18 Also see: (Araya and He 2024, 8-11).
19 Also see: (IIDA 2024).
20 The centralization of all political, security, economic and military decision-making in China is now realized. See: (US Government 2022).

evades easy definition, Chinese strategic culture accepts the risks, costs, and long-term commitments necessary to pursue low probability, high return innovation efforts. One such indicator of this is significant ongoing internal PLA organizational reforms to experiment with how best to achieve this targeted end-state.[22] Moreover, comprehensive "military-civilian fusion," talent acquisition, and aggressive government funding has mobilized society, industry, as well as academia and military resources to achieve 'leapfrogging' scientific breakthroughs.[23]

Canada's AI Response in Context and the Canadian Armed Forces (CAF)

The transformational potential of AI is increasingly noted by a growing number of Western powers. Indeed, when considering the AI revolution, Canada has been counted as a global leader in many respects.[24] Nationally, it has prioritized the goal as moving from a "digitally aware" to a "digitally transformed" nation. That said, unlike in China, the drivers informing strategic AI approaches and investments are largely informed by commercial, societal (particularly healthcare) and university research objectives. The military nexus is a distant, and all too often, isolated and insulated afterthought.[25]

Increased understanding of AI as a powerful tool that might reshape warfare has led to a growing number of countries adopting defence AI strategies to supplement national strategies, as Canada did in 2024 (Department of National Defence 2024a). While Canada has nurtured a dynamic and active AI innovation ecosystem, work is still needed for the CAF to be able to adopt and take full advantage of the potential AI offers. Critiques, for example, have identified challenge areas concerning the military's capacity to digitally transform as rooted in its organizational structure, history, and culture, more than any technological shortcomings (Engen 2024).

From Canada's standpoint as a Middle Power, keeping up with developments in the field of military AI is as much a reaction to rivals and adversaries, as an effort to remain a credible force and being interop-

21 Also see: (Hung and Hung 2022).

22 For instance, in 2015 the PLA centralized strategic space, cyberspace, electronic warfare, and information communications functions under the Strategic Support Forces (SSF) to develop new synergies. Ultimately disbanded in the Spring of 2024 for unknown reasons, it resulted in a bigger, more visible role for the PLA's Information Support Force, a unit reliant on AI-integration. This is part of a larger trend of the PLA optimizing its structure to favor AI-development, exemplified by the promotion of the Science and Technology Commission to an organ directly associated to the Central Military Commission. See: (Lin and Liao 2024).

23 The nature and scope of Military-Civil Fusion is outlined in numerous publications, such as: (Department of Defense 2023, 28-33).

24 In 2023, Canada ranked 5th globally in AI capacity. Key measurables include: a 2024 budget allocation of CAD$2.4 billion in new AI investments; nearly 700 AI firms nationally; a world leader in AI research citations; and CAD$2.8 billion in private sector investment. See: (Trudeau 2024).

25 The exception to this is Defence Research and Development Canada (DRDC) which has a long history of working in AI across multiple research centres nationally. Each facility has developed its own internal and external capabilities to deliver on program in diverse domains: land, air and maritime ISR; pan-domain situational awareness; influence activities; robotics and autonomous systems; cybersecurity; human performance modelling enhancements; and data enterprise management. Other pillars of AI effective application include the Canadian Special Operations Forces Command (CANSOFCOM) and Canadian Forces Intelligence Command (CFINTCOM).

erable with allies. The 2024 CAF AI strategy asserts that AI is essential for warfighting, as well as the modernization of the institution. It lays out five specific 'Lines of Effort.' For example, the military plans to integrate AI systems into the organisation for both military and corporate purposes, promote organisational change to enhance AI integration, ensure ethical and trustworthy AI use, foster talent through training and recruitment, and develop partnerships with other departments and non-government stakeholders (Department of National Defence 2024a, 1).

The strategy also broadly aligns with and supports other related initiatives. For instance, the DND/CAF Data Strategy stresses the importance of data management and analytics within the organization, a task in which AI can prove useful (Department of National Defence 2021). Likewise, the Digital Campaign Plan is the modernization plan for the force; it stresses the need to integrate digital technology into warfighting and corporate affairs, eventually enabling the enterprise to constantly improve itself and innovate (Department of National Defence 2023). Moreover, the Canadian Army, Royal Canadian Air Force and the Canadian Special Operation Forces Command have all recently published guiding documents which include AI considerations. The army, for example, has identified the need for AI-enhanced information management to prevent information overload for war fighters, autonomous systems, and algorithm-assisted support tasks like logistics (Department of National Defence 2019). CANSOFCOM stresses the need for increased digitalization to shape the battlespace and assist in tasks which are outside the conventional military's traditional mission set (Department of National Defence 2020). The RCAF stresses that it must innovate and integrate in the field of AI and machine learning at the speed of relevance (Department of National Defence 2023). In short, tangible AI advancements are rapidly becoming evident.

As noted by Engen, "there are many Canadian initiatives related to defence AI under development, and DND/CAF has solid mechanisms for funding and nurturing AI projects in partnership with academia and industry." (Engen 2024, 1). For example, DRDC's Innovation for Defence Excellence and Security (IDEaS) is a competitive funding model that fosters 'research clusters' to bring together academics, industry, and other partners to form collaborative networks. Approximately 65-70 per cent of proposals for annual grants awarded involve AI components (Jouan 2022). Likewise, another program sponsored by DND's Assistant Deputy Minister (Policy) "Mobilizing Insights in Defence and Security" (MINDS) engages external stakeholders to offer engagement opportunities and feedback loops on emerging defence priorities like AI. Moreover, novel DND/CAF AI partnerships are not only national in nature. Canada has a history of AI collaboration and leadership under multilateral research efforts, with the Five Eyes (FVEY) Technical Collaboration Program (TTCP) and with NATO.[26] Supplementing these initiatives, Canada, the US, and the UK's national military research organizations have just agreed to collaboratively pursue research, development, test, and evaluation technologies focused on AI, cyber, resilient systems, and information domain-related technologies.[27] Such collaboration and

26 Topics of research have included AI's application in intelligence, reconnaissance and surveillance, tactical application for the dismounted soldier, social media analytics, precision medicine, modelling and simulation, immersive simulation and training, as well as ethics and policies.

27 This undertaking will draw on the expertise of the US's Defence Advanced Research Projects Agency, (DARPA) the UK's Defence Science and Technology Laboratory (Dstl), and DND's Defence Research and Development Canada (DRDC).

demonstration of Canadian AI excellence may further open doors to other defence partnering, like the Pillar II focus on technology of AUKUS in the Indo-Pacific (Canada Defence Review 2024).

Finally, the most convincing evidence of the DND/CAF's embrace of AI is the reallocation of resources internally, and the official stand-up of new organizations to address this requirement. In order to promote a thriving AI ecosystem "where research, experimentation and collaboration coexist and result in innovative AI solutions" the DND/CAF inaugurated the Artificial Intelligence Centre (DCAIC) on July 29, 2024 (Mattews and Eyre 2024). Aimed at improving alignment with Allies, accelerating the adoption of AI capabilities across the defence-enterprise, and implementing coherent and comprehensive AI solutions to broadly defined defence and security challenges, this new Centre will improve operational readiness, and offer guidance on critical issues related to AI implementation, such as policy, ethics, gender, procurement, and training.

The Ongoing Need: Augmented NATO Partnerships

Despite the successes just detailed, for Canada, fully transitioning to an AI-enabled fighting force necessitates more than a national strategy, and an accompanying nascent defence AI strategy. With those critical steps complete, progress now requires synergizing this potential with global defence and industry partners. While the DND/CAF has established embryonic patterns of international AI collaboration, these are the product of a qualitatively different, less AI-informed era, one founded on institutional models (primarily focussed on R&D) that have since significantly evolved.

NATO, for example, formally adopted a unified AI strategy in 2021 and further updated it in 2024 (NATO 2024) to reflect the rapidly changing international reality, including China's growing S&T dominance and AI threat potential (Cheung 2024). Essential work has now been completed examining how individual NATO member states currently think about and use AI in their militaries (as well as future employment options), opening the door to improved partnering scenarios (Gray and Ertan 2021). Moreover, Canada already participates in key AI venues with NATO Allies and other interested states. For example, the DND/CAF is a committed member of the AI Partnership for Defence (PfD) established by the US Department of Defense's Joint Artificial Intelligence Centre (JAIC). Additionally, a growing number of linkages involve AI in the Indo-Pacific region. NATO's evolving partnerships with the Indo-Pacific Four (South Korea, Japan, Australia, and New Zealand) further complement Canada's recent focus on improved military to military ties to each of these countries (NATO 2024). In short, a catalyst increasingly drawing nations together is shared concerns over China and AI.

Most significantly, in October 2024 Canada opened the North American Regional Office of the Defence Innovation Accelerator for the North Atlantic (DIANA) in Halifax, Nova Scotia. A technology development hub comprising approximately 60 innovation sites across more than 20 Allied nations in North America and Europe, this organization will facilitate cooperation between civilian innovators, government scientists, and military operators to promote early-stage technologies addressing specific Allied defence and security problems (NATO 2024). An identified priority is AI. In short, the linking of a North American regional headquarters with its equivalent in Europe, the stand-up of an international accelerator network, test centres, rapid adoption services, and

trusted capital databases to help protect technology while fostering market opportunities, all open the door to Canadian leadership on promoting shared norms, standards, testing, procurement and overall military AI co-development with NATO members.

Conclusion

Artificial intelligence is now integral to almost all aspects of our daily lives. So much so that the depth of AI penetration in our lifestyles, workplaces, communications, and social interactions is becoming not merely accepted, but fundamentally so common it is less and less visible. This reality is increasingly possible for AI's integration into military affairs, including decision-making, targeting, weapons development, and force employment options—raising moral, ethical, legal, and policy dilemmas that will have to be confronted (Momani et al. 2022).

China's prioritization and increasing dominance in a growing number of select military AI domains dramatically complicates the picture, reducing the timelines available, and (as NATO's top strategic adversary) all but eliminates the possibility of indecision, inaction, and issue-avoidance. As demonstrated, President Xi Jinping is consumed with augmenting the PRC's comprehensive national power. Xi sees returning Beijing to the position of a preeminent global power, complete with the reunification of Taiwan (by force if necessary) as integral to his personal legacy.

For Xi, the high-tech sector is the "main battlefield" in Superpower rivalry. Emerging and disruptive technologies (most notably AI) will prove the defining difference. AI is more than a means to an end; it is also a force multiplier applicable to the 57 of 64 critical technologies China now globally dominates. Recognized by the Canadian Government as "an increasingly disruptive global power" the PRC's goal of attaining the intelligentization of warfare through a new evolving operational concept demonstrates it is not only pushing a new AI revolution in military affairs through unprecedented investments, research, and a nationally concerted campaign of military-civil fusion (aimed at securing asymmetric advantage), it is also concurrently exploring AI's potential in new frontiers of conflict—most notably AI-informed cognitive warfare (Global Affairs Canada 2022, 7). The risks to Canada's national defence and security in the Indo-Pacific region are menacing, particularly as the PRC often operates outside of accepted international norms.[28]

While striving to react to this new 'threat reality' DND/CAF efforts (although progressing on important fronts) remain embryonic in comparison. The challenge set is daunting, but surmountable.[29] As called for in *Our North Strong and Free,* the

28 While the PLA frequently advocates for the responsible use of AI, it is often selective in its application based on perceived self-interest. For instance, following a summit in Seoul this past September dedicated to responsible AI in the military domain, some 60 countries endorsed a "Blueprint for Action" to govern the responsible use of artificial intelligence in the military. China, however, did not endorse the legally non-binding document which addressed issues such as risk assessments, required human controls, and necessary confidence-building measures.

29 For instance, (while opinions may vary) for many stakeholders the application of AI in the CAF and within DND (as a department) are informed by different drivers and perceived levels of urgency. Overall, AI governance structures are largely underdeveloped. Procurement of new tools is cumbersome. Data sets exist but are not widely declassified and usable. Limited talent recruitment, as well as training and culture issues further hamper progress. Enterprise architecture is not unified, nor mature. Security issues promote a 'siloed' mentality. And finally, demographics of the workforce are not encouraging a rapid pace of adaptation or evolution. For a broad overview see: (Lukawiecki 2024).

government is committed to "…build[ing] a stronger defence industrial base to support a more resilient, modern, and sustainable military…" AI provides a unique constellation of interests between government, the private sector, and academia for a synergizing of all stakeholders' interests (Department of National Defence 2024b, ix). What is required is leadership, prioritization, and direction in a framework that has been described as "a national system of innovation" (Araya and King 2022).

Since 2017, when the federal government first instituted and funded the Pan-Canadian AI Strategy (renewed in 2022), Canada has fostered an AI ecosystem consisting of intersecting incubator programs, superclusters, academic institutes (such as the Quebec Artificial Intelligence Institute, the Vector Institute, and Alberta's Machine Intelligence Institute), as well as non-profit innovation hubs (Centech), world-leading federal research labs (including DRDC and NRC), and diverse partnerships with private sector start-ups. Further empowered by nearly 700 established AI firms across the country, and some CAD$2.8 billion in private sector investment, a network of expertise exists that National Defence could better leverage as a critical part of its implementation and long-term AI planning.

Given Canada's national and subsequent defence AI strategies, a robust country-wide AI research infrastructure, and a strong public-private AI developmental ecosystem, attention should now turn to international military AI partnering opportunities (most notably with NATO countries) in order to offset costs, encourage common standards, enable shared data sets, leverage technological innovations, promote interoperability, and help develop common operating pictures. The ongoing maturation of NATO's AI strategic planning, the rapid rate of individual member states domestic, industrial, and defence AI programs, as well as novel NATO institutional approaches (such as DIANA), well situate Canada to lead on effectively addressing the AI revolution in military affairs (AI-RMA).

In conclusion, as a global leader in AI, Canada must now fully integrate its national strengths in this domain specifically to the defence enterprise. These assets need then be synergized, integrated and amplified by international AI partnerships. The PRC's mounting AI threat potential leaves Canada with no other option. In protecting Canadian interests, values, and our stake in the continuance of a RBIO, AI is a test case for developing a new approach to a defence industrial base that prioritizes innovation, research excellence, pan-Canadian expertise, and one that unites public-private collaboration in common cause —the defence of our country and the well-being of all citizens—with other like-minded Western nations.

Acknowledgements

The author would like to thank the comments offered by two anonymous reviewers of this article. Their insights, challenges, and thoughtful suggestions qualitatively improved the calibre of this essay. Additionally, the continual review, research, and stylistic advice of Dr. Adam MacDonald were very much appreciated, as were the insights and editorial efforts of Jacob Benjamin.

Authors

Dr. Kurtis H. Simpson
Kurtis H. Simpson currently serves as a special advisor, Indo-Pacific affairs, with the Strategic Joint Staff at the Department of National Defence. As a senior defence scientist, he draws on several decades of experience in the Public Service, filling diverse research and management roles across government departments, including the Privy Council Office, Foreign Affairs, as well as defence and intelligence organizations. A China specialist by training, he has extensive expertise in Asian security issues, global affairs, as well as transnational threats and terrorism,

publishing over 100 largely classified assessments, articles, and conference proceedings. Dr. Simpson has also acted as the Head of Delegation abroad for the Canadian government, and worked in numerous international liaison roles with Australia, the U.S., NATO, and other 5EYES partners. He holds an M.A. and a Ph.D. in international relations from York University and is a graduate of the National Security Program.

Raphael Racicot
Raphael Racicot is a research intern at the Centre for Operational Research and Analysis at National Defence. A graduate student in International Affairs at NPSIA, Carleton University, he is specialising in strategic studies and great power competition. His current work focuses on hegemonic systems and power transitions between hegemons. A graduate of the Royal Military College of Canada (RMCC), he is a former Canadian Armed Forces infantry officer. He has a varied research background, notably working for the Electoral Integrity Project and conducting his own research on electoral scrutiny.

Samuel Paquette
Samuel Paquette is a research intern at the Centre for Operational Research and Analysis at National Defence. He is currently a graduate student studying International Affairs at the Norman Paterson School of International Affairs (NPSIA), specializing in conflict analysis and resolution. He currently researches security issues in the Indo-Pacific, focussing on China's foreign policy, critical minerals, cyber warfare, grey-zone tactics, Cross-Strait relations and critical technologies.

Samuel Villanove
Samuel Villanove is a research intern at the Centre for Operational Research and Analysis at National Defence. He is a graduate student at the University of Ottawa in public and international affairs and has government experience working at Global Affairs Canada. Specialized in Chinese and Taiwanese politics, he has extensive Chinese language skills and field experience in both China and Taiwan.

Researchers

Adam MacDonald
Adam MacDonald is a researcher with the Centre for China Policy Research at Global Affairs Canada.

References

Ali Baig, Muhammad and Anum A. Khan. 2024. "AI's Oppenheimer moment: Establishing regulations." *The Interpreter*, The Lowy Institute, January 16, 2024. https://www.lowyinstitute.org/the-interpreter/ai-s-oppenheimer-moment-establishing-regulations.

Araya, Daniel and Alex He. 2024. *United States-China Multilateralism in the Age of Military AI*. CIGI Paper No. 309. Waterloo: Centre for International Governance Innovation (CIGI). https://www.cigionline.org/publications/united-states-china-multilateralism-in-the-age-of-military-ai/.

Araya, Daniel. 2022. "AI Is Rapidly Transforming Warfare: New Rules Are Urgently Need." *Centre for International Governance Innovation* (*CIGI)*, July 18, 2022. https://www.cigionline.org/articles/ai-is-rapidly-transforming-warfare-new-rules-are-urgently-needed/.

Araya, Daniel, and Meg King. 2022. *The Impact of Artificial Intelligence on Military Defence and Security*. CIGI Papers No.263. Waterloo: Centre for International Governance Innovation (CIGI). https://www.cigionline.org/static/documents/no.263.pdf.

Borchert, Heiko, Torben Schütz and Joseph Verbovszky, eds. 2024. *The Very Long Game: 25 Case Studies on the Global State of Defense*. New York: Springer.

Brands, Hal. 2024. "6 Ways AI Will Change War and the World." *Bloomberg Opinion*, June 9, 2024. https://www.bloomberg.com/opinion/features/2024-06-09/how-will-ai-change-war.

Brenes, Michael, and William D. Hartung. 2024. "Private Finance and the Quest to Remake Modern Warfare." *Quincy Brief*, June 3, 2024. https://quincyinst.org/research/private-finance-and-the-quest-to-remake-modern-warfare.

Canadian Defence Review, 2024. "AUKUS Strengthens Ties with Canada and Allies for Advanced Capabilities." *Canadian Defence Review*, September 19, 2024. https://canadiandefencereview.com/aukus-strengthens-ties-with-canada-and-allies-for-advanced-capabilities/.

Cheung, Sunny. 2023. "AI Frontlines: China's PLA evolution vs. NATO's counterplay." Friedrich Naumann Foundation, November 24, 2023. https://www.freiheit.org/taiwan/ai-frontlines-chinas-pla-evolution-vs-natos-counterplay.

Congressional Research Service. 2020. *Artificial Intelligence and National Security.* CRS Report No. R45178 Washington, DC: Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45178/9.

DARPA. 2024. "DARPA Collaborates with UK and Canadian Government Partners in Agency's First Trilateral Project." *DARPA*, September 20, 2024. https://www.darpa.mil/news/2024/first-trilateral-project.

Department of National Defence (DND). 2019. *Close Engagement: Land Power in an Age of Uncertainty*. Ottawa: Department of

National Defence. Last modified November 2021. https://www.canada.ca/en/army/services/line-sight/articles/2021/11/close-engagement-land-power-in-an-age-of-uncertainty.html.

Department of National Defence (DND). 2020. *CANSOFCOM: Beyond the Horizon*. Ottawa: Department of National Defence. Last modified November 1, 2020. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/cansofcom-beyond-horizon.html.

Department of National Defence (DND). 2021. *DND/CAF Data Strategy*. Ottawa: Department of National Defence. Last modified May 5, 2021. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/data-strategy/data-strategy.html.

Department of National Defence (DND). 2022. *Canadian Armed Forces Digital Campaign Plan*. Ottawa: Department of National Defence. Last modified November 23, 2022. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-digital-campaign-plan.html.

Department of National Defence (DND). 2023. *DND/CAF Artificial Intelligence Strategy*. Ottawa: Department of National Defence. Last modified March 10, 2023. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/dnd-caf-artificial-intelligence-strategy.html.

Department of National Defence (DND). 2024. *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy*. Ottawa: Department of National Defence. https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/dndcaf-ai-strategy.pdf.

Department of National Defence (DND). 2024. Our North Strong and Free. Ottawa: Department of National Defence. Last modified May 5, 2024. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

Drinhausen, Katja and Helena Legarda. 2022. "Comprehensive National Security Unleashed: How Xi's Approach Shapes Policies at Home and Abroad." *MERICS*, September 15, 2022. https://merics.org/en/report/comprehensive-national-security-unleashed-how-xis-approach-shapes-chinas-policies-home-and.

Edmonds, Jeffrey, Samuel Bendett, Anya Fink, Mary Chesnut, Dmitry Gorenburg, Michael Kofman, Kasey Stricklin, and Julian Waller. 2021. *Artificial Intelligence and Autonomy in Russia.* Arlington: Center for Naval Analysis. https://www.cna.org/centers-and-divisions/cna/sppp/russia-studies/artificial-intelligence-and-autonomy-in-russia

Engen, Robert. 2024. "When the Teeth Eat The Tail: A Review of Canada's Defence Artificial Intelligence." In *The Very Long Game: 25 Case Studies Studies on the Global State of Defense*, edited by Heiko Borchert, Torben Sch and Joseph Verbovszky, 63-83. New York: Springer.

Fedasiuk, Ryan, Jennifer Melot, and Ben Murphy. 2021. *Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence*. Washington, DC: Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/harnessed-lightning/.

Fravel, Taylor. 2015. "China's New Military Strategy: 'Winning Informatized Local Wars.'" *Jamestown China Brief,* June 23, 2015. https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/ .

Global Affairs Canada. 2022. "Canada's Indo-Pacific Strategy." https://www.international.gc.ca/transparency-transparence/indo-pacific-indo-pacifique/index.aspx?lang=eng.

Gray, Maggie and Amy Ertan. 2021. *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/library/publications/artificial-intelligence-and-autonomy-in-the-military-an-overview-of-nato-member-states-strategies-and-deployment/.

He, Fuchu. 2017. "The Future Direction of the New Global Revolution in Military Affairs." *Reference News*, August 24, 2017.

Heath, Timothy R. 2023. "Why is China Strengthening Its Military? It's Not All About War." *The Rand Corporation*, March 24, 2023. https://www.rand.org/pubs/commentary/2023/03/why-is-china-strengthening-its-military-its-not-all.html.

Hirsh, Michael. 2023. "How AI Will Revolutionize Warfare." *Foreign Policy*, April 11, 2023. https://foreignpolicy.com/2023/04/11/ai-arms-race-artificial-intelligence-chatgpt-military-technology/.

Hung, Tzu-Chieh, and Tzu-Wei Hung. 2022. "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars." *Journal of Global Security Studies* 7 (4). https://doi.org/10.1093/jogss/ogac016.

Hynek, Nyk and Anzhelika Solovyeva. 2022. *Militarizing Artificial Intelligence: Theory, Technology, and Regulation*. London: Routledge.

IIDA, Masafumi. 2024. "China's Chilling Cognitive Warfare Plans: War is entering a new, and very frightening domain." *The Diplomat*, May 5, 2024. https://thediplomat.com/2024/05/chinas-chilling-cognitive-warfare-plans/.

Jiang, Ben. 2024. "China's AI industry could see $US1.4 trillion investment in 6 years, executive says," *South China Morning Post*, September 9, 2024. https://www.scmp.com/tech/big-tech/article/3277743/chinas-ai-industry-could-see-us14-trillion-investment-6-years-executive-says.

Johnson, James. 2021. "The End of Military-Techno Pax Americana? Washington's Strategic Responses to Chinese AI-Enabled Military Technology." *The Pacific Review* 34 (3): 351–78. https://doi.org/10.1080/09512748.2019.1676299.

Jouan, Alexandre. 2022. "Artificial Intelligence." Presentation, DRDC Directorate of Strategic Partnerships, Ottawa, September 2022.

Kania, Elsa B. 2020. "Minds at war: China's Pursuit of Military Advantage through Cognitive Science and Biotechnology." *Prism: A Journal of the Center for Complex Operations* 8 (3): 82-101. https://www.proquest.com/scholarly-journals/minds-at-war-chinas-pursuit-military-advantage/docview/2354302828/se-2.

Kania, Elsa B. 2021. "Artificial intelligence in China's revolution in military affairs." *Journal of Strategic Studies* 44 (4): 515-42. https://doi.org/10.1080/01402390.2021.1894136.

Larson, Jacob, James S. Denford, Gregory S. Dawson, and Kevin C. Desouza. 2024. "The Evolution of Artificial Intelligence (AI) Spending by the U.S. Government." *Brookings*, March 26, 2024. https://www.brookings.edu/articles/the-evolution-of-artificial-intelligence-ai-spending-by-the-u-s-government/.

Launchbury, John. 2018. "A DARPA Perspective on Artificial Intelligence." https://journalismai.com/2018/04/04/a-darpa-perspective-on-artificial-intelligence-darpa/.

Lee, John. 2024. "Overtaking on the Curve?: Defense AI in China," in *The Very Long Game: 25 Case Studies Studies on the Global State of Defense*, edited by Heiko Borchert, Torben Sch and Joseph Verbovszky, 465-486. New York: Springer. https://link.springer.com/chapter/10.1007/978-3-031-58649-1_21.

Lin, Ying Yu and Tsu-Hao Liao. 2024. "RIP, SSF: Unpacking the PLA's Latest Restructuring," *The Diplomat*, April 23, 2024. https://thediplomat.com/2024/04/rip-ssf-unpacking-the-plas-latest-restructuring/.

Lukawiecki, Emanuel. 2024. "A Blueprint for AI Integration in the Canadian Armed Forces." *CIGI Digital Policy Hub Working Paper*, Winter 2024. https://www.cigionline.org/static/documents/DPH-paper-Lukawiecki.pdf.

Lushenko, Paul. 2023. "AI and the Future of Warfare." *Bulletin of the Atomic Scientists*, November 29, 2023. https://thebulletin.org/2023/11/ai-and-the-future-of-warfare-the-troubling-evidence-from-the-us-military/.

Lushenko, Paul and Keith Carter. 2024. "A new military-industrial complex: How tech bros are hyping AI's role in war," *Bulletin of Atomic Scientists*, October 7, 2024. https://thebulletin.org/2024/10/a-new-military-industrial-complex-how-tech-bros-are-hyping-ais-role-in-war/.

MarketsandMarkets. 2024. "Artificial Intelligence in Military Markets - Global Forecast to 2028." Last modified January 2024. https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-military-market-41793495.html.

Maslej, Nestor, Loredana Fattorini, Raymond Perrault, Vanessa Parli, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, and Jack Clark. 2024. *The AI Index 2024 Annual Report*. Stanford: AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. https://aiindex.stanford.edu/report/.

Massey, Karen and Mariana Fang. 2024. "IDC's Worldwide AI and Generative AI Spending-Industry Outlook." *IDC Blog*, August 21, 2024. https://blogs.idc.com/2024/08/21/idcs-worldwide-ai-and-generative-ai-spending-industry-outlook/.

Mattews, Bill and General Wayne D. Eyre. 2024. "CM/CDS Message: Launch of the DND/CAF Artificial Intelligence Strategy." March 7, 2024. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2024/03/dm-cds-message-launch-dnd-caf-artificia-intelligence-strategy.html.

MixedMode. n.d. "What is Third Wave AI." https://mixmode.ai/what-is/third-wave-ai/.

Momani, Bessma, Aaron Shull, and Jean-François Bélanger. 2022. "Introduction: The Ethics of Automated and Artificial Intelligence." *The Centre for International Governance Innovation*, November 28, 2022. https://www.cigionline.org/articles/introduction-the-ethics-of-automated-warfare-and-ai/.

Motwani, Nishank. 2024. "The danger of AI in war: it doesn't care about self-preservation," *ASPI, The Strategist*, August 30, 2024. https://www.aspistrategist.org.au/the-danger-of-ai-in-war-it-doesnt-care-about-self-preservation/.

NATO. 2024. "Summary of NATO's revised Artificial Intelligence Strategy." July 10, 2024. https://www.nato.int/cps/en/natohq/official_texts_227237.htm .

NATO. n.d. "Defence Innovation Accelerator for the North Atlantic: Uniting disruptors to shape a peaceful future." https://www.diana.nato.int/.

NATO. 2024. "Relations with Partners in the Indo-Pacific." October 24, 2024. https://www.nato.int/cps/en/natohq/topics_183254.htm.

Osborn, Kris. 2023. "China's New 'Multi-Domain Precision Warfare' Operational Concept 'Mirrors' US Strategy." *Warrior Maven Centre for Military Innovation*, October 25, 2023. https://warriormaven.com/china/chinas-new-multi-domain-precision-warfare-operational-concept-completely-mirrors-us-strategy.

Oxford Insights. 2023. "Government Readiness AI Index." 2023. https://oxfordinsights.com/ai-readiness/ai-readiness-index/.

Peters, Robert and Wilson Beaver. 2024. "The Defence Department's China Military Power Report: The Threat Is Worse Than Advertised." *The Heritage Foundation*, January 30, 2024. https://www.heritage.org/defense/commentary/the-defense-departments-china-military-power-report-the-threat-worse-advertised.

Pugliese, David. 2023. "Russia and China at War with Canada, says Gen Wayne Eyre," *Ottawa Citizen*, October 26, 2023. https://ottawacitizen.com/news/national/defence-watch/russia-and-china-at-war-with-canada-says-gen-wayne-eyre.

Rashid, Adib, Ashfakul Kausik, Ahamed Al Sunny, and Mehedy Hassan Bappy. 2023. "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges." *International Journal of Intelligent Systems* (1): 1-31. https://doi.org/10.1155/2023/8676366.

Rira, Momma. "China's Preparations for Informatized Warfare." In *NIDS China Security Report 2021: China's Military Strategy in the New Era*, 6-20. Tokyo: National Institute for Defence Studies. https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2021_A01.pdf.

Royal Canadian Air Force. 2021. *Royal Canadian Air Force Strategy*. Ottawa: Royal Canadian Air Force. Last modified July 22, 2021. https://www.canada.ca/en/air-force/corporate/reports-publications/royal-canadian-air-force-strategy.html.

Rudd, David. 2024. *Russia and artificial intelligence: Background and preliminary threat picture. DRDC-RDDC-2024-L081.* Ottawa: Defence Research and Development Canada.

Stokes, Jacob. 2024. "Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition," Testimony Before the U.S.-China Economic and Security Review Commission, *CNAS*, February 1, 2024. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Jacob_Stokes_Testimony.pdf.

Takagi, Koichiro. 2022. "Artificial Intelligence and Future Warfare." *Hudson Institute*, November 23, 2022. https://www.hudson.org/defense-strategy/artificial-intelligence-future-warfare.

Takagi, Koichiro. 2022. **"**Xi Jinping's Vision for Artificial Intelligence in the PLA." *The Diplomat*, November 16, 2022. https://thediplomat.com/2022/11/xi-jinpings-vision-for-artificial-intelligence-in-the-pla/.

The Economist. 2024. "How AI is Changing Warfare." *The Economist,* June 20, 2024. https://www.economist.com/briefing/2024/06/20/how-ai-is-changing-warfare.

Trudeau, Justin. 2024. "Securing Canada's AI Advantage." *Prime Minister of Canada Public Statement*, April 7, 2024, Montreal. https://www.pm.gc.ca/en/news/news-releases/2024/04/07/securing-canadas-ai.

U.S.-China Economic and Security Review Commission. 2022. *CCP Decision-Making and Xi Jinping's Centralization of Authority*. Washington, DC: U.S.-China Economic and Security Review Commission Annual Report to Congress. https://www.uscc.gov/sites/default/files/2022-11/Chapter_1--CCP_Decision-Making_and_Xi_Jinpings_Centralization_of_Authority.pdf.

U.S. Department of Defence. 2023. *Military and Security Developments Involving the People's Republic of China.* Washington, DC: Annual Report to Congress. https://www.hsdl.org/c/annual-china-military-power-report/.

Wong Leung, Jennifer, Stephan Robin, and Danielle Cave. 2024. ASPI's two-decade Critical Technology Tracker: The rewards of long-term research investment. Canberra: Australian Strategic Policy Institute. https://www.aspi.org.au/report/aspis-two-decade-critical-technology-tracker.

Xinhua. 2024. "China's R&D expenditure exceeds 3.3 trln yuan in 2023: minister." *The State Council of the People's Republic of China*, March 5, 2024. https://english.www.gov.cn/news/202403/05/content_WS65e6ff4dc6d0868f4e8e4b66.html.

Yoshihara, Toshi. 2012. "China's vision of its seascape: the first island chain and Chinese seapower." *Asian Politics & Policy* 4 (3): 293-314. https://doi.org/10.1111/j.1943-0787.2012.01349.x.

Zelikow, Philip. 2024. "Confronting Another Axis? History, Humility, and Wishful Thinking." *The Strategist* 7 (3): 80-99. https://doi.org/10.26153/tsw/54040.

Zysk, Katarzyna. 2024. "High Hopes Amid Hard Realities: Defence AI in Russia." In *The Very Long Game: 25 Case Studies on the Global State of Defense*, edited by Heiko Borchert, Torben Sch, and Joseph Verbovszky, 353-374. New York: Springer. https://link.springer.com/chapter/10.1007/978-3-031-58649-1_16.

Military Modernization in the Age of Machine Knowledge Capital

Dan Ciuriak

1. A Statement of the Challenge

The world has become more dangerous for many reasons. One is the re-emergence of great power rivalry, a shift that has already metastasized into proxy wars. A second is the rise of American isolationism, which has weakened external constraints on international violence. The peace dividend that Canada enjoyed for decades – perhaps to excess – is no more and Canada now faces a daunting task of substantially expanding its defence capability in an international security environment radically reshaped by the digital transformation, artificial intelligence (AI), and the secular change in the global power configuration.

In this essay, I set out the economic case for a strategic focus on technology development in Canada's defence procurement. This reflects the rapidly expanding role of artificial intelligence (AI), data analytics, and cybersecurity (including quantum computing) in modern defence doctrine (DND 2024; 9); Canada's comparative advantage in these areas coupled with our comparative disadvantage in heavy industry; and the central role that these dual use technologies could play in supporting the economic development that underpins Canada's wherewithal to meet its defence needs.

The digital transformation has opened up multiple new fronts, complicating the challenge of maintaining national security. Cyberspace is borderless – multinational corporations and hostile actors can operate in Canada without passing through immigration (Ciuriak 2024a). The attack landscape is expanding exponentially as the backbone infrastructure of our economy becomes increasingly digitalized and akin to a hackable interactive central nervous system, while Internet-of-Things (IoT) connected devices from cars to pagers become potential weapons, software updates introduce backdoors into our digital control systems to be exploited at the discretion of foreign actors at the time of their choosing, and immense amounts of data are streamed into the cloud to be processed by increasingly powerful AI systems. We can be read like a book and disrupted by pre-positioned cyberagents that are figuratively "living off the land" – our land.

That's scary enough but that is far from all of it. While technological developments have radically changed battlefield dynamics with autonomous weapons, loitering drones, swarm tactics, electronic warfare, and big-data/AI-enabled real-time tactical planning, etc., not all the world lives in the 21st century. There are countries run by 19th century types fighting mechanized 20th century wars. Shells and hulls and logistics still matter. And the world is getting smaller: as emphasized in Canada's updated defence vision (DND 2024), missiles are getting faster, space is being weaponized, and climate change is opening up the Arctic, which is at risk of becoming a Russian-Chinese lake as shipping flows mainly along the Siberian coast through the Northeast Passage or Northern Sea Route and the infrastructure – including Russia's maintenance of ice-breaking support and China's Polar Silk Road – is developing there (and perhaps much faster than anticipated given extant plans for year-round Arctic shipping; e.g., Humpert 2024).

And it should go almost without saying, given the immense amount of ink that has been spilled in writing about industrial competition, that our challenge does not allow us to choose between guns and butter – we need to expand our production of both given the need for military-civilian fusion to create the supply capability for the modern arsenal.

That's the bad news. There is some good news.

From one perspective, Canada's historic under-investment in defence spending has some silver linings. First, our penny-pinching conserved fiscal capacity. Canada has the best fiscal position in the G7: our net general government debt is only 13% of GDP; our structural deficit less than 1% of GDP; and our current account is in surplus meaning we are not borrowing internationally. All IMF figures for 2024. This provides the fiscal room to ramp up defence spending – and dollar for investment dollar, defence spending today gives Canada a capability better suited to today's conflict conditions than it would have had with prior spending on legacy military hardware.

Second, as noted, we have important strengths in precisely the area that is disrupting the national security space: digital technological development, including in critical areas like AI, quantum computing and cybersecurity. Canada also features the fastest-growing technological workforce in North America – Ottawa has the same density of tech jobs as San Francisco and our major cities are adding tech jobs much faster than their US counterparts.

Third, the main challenge we face in both defence and industrial development is one and the same: the areas of Canada's comparative advantage are inherently dual use and building the companies with the necessary capabilities to help meet Canada's defence requirements will also address our economic development challenge.

The term "comparative advantage" is a reminder that Canada is an open economy that depends heavily on international trade. Unfortunately, Canada has grown small in the world. Our annual GDP runs at about US2.2 trillion. That is not enough to buy even one modern superstar firm – Nvidia's market cap as of January 2025 is US$3.3 trillion.

The reason we have grown small is because we don't produce the really valuable stuff – Nvidia's output by weight is very small, but it is extremely valuable. The raw materials and industrial output that Canada produces are heavy but low value. By weight, we have a lot of production; by market cap, not so much. US market cap is 200% of its GDP; ours is about 120%.

Our heavy industry is mostly foreign-owned and generates no economic rent (above-normal profits) that is captured by Canada – and often requires both protection and subsidies (negative rent for Canada). If defence modernization emphasizes heavy industry, it will do the minimum for Canada economically and also ensure that we get the least amount of national security we can possibly achieve on our budget.

This necessarily points us to a strategic focus on technology.

A preliminary question is how to reconcile the claim that Canada has comparative advantage in technology development but lacks high value production? Simple. Canada has a large surplus on R&D services, meaning we work as developers of technology for foreign companies who capture the economic rents – and then we pay handsomely to license the resulting intellectual property (IP). See Table 1.

The quintessential example of how our business model works is the fact that the deep learning technology that powered Google to superstar firm

heights was developed in Canada at the University of Toronto by Nobel Prize winner Geoffrey Hinton, who went to work for Google. Google operates in Canada largely on a virtual basis, captures large profits from its operations in Canada, but pays little or no taxes here. Eric Schmidt, former CEO of Google, publicly thanked Canada for making Google great in the era of the data-driven economy. Canada's business model makes us the digital equivalent of the hewer of wood and drawer of water in the material economy. Properly conceived, our industrial policy needs to focus on changing that business model.

We are now in the early phase of a new economic era – that of machine knowledge capital. It is essential for Canada to position itself to prosper in this era – and military modernization can greatly assist. In the next sections, I walk through the basic economics of firm-centred industrial policy in support of this argument and how defence procurement can play a leading role in fostering the growth of dual-use technology firms to meet defence needs and to generate the economic development to help pay the defence bill.

2. Some Basic Economics

To understand how to use military modernization strategically, we first have to establish three key economic stylized facts: the firm structure of an industry matters; new forms of capital capture economic rents; and innovation is getting more costly in terms of resource requirements as new ideas get harder to find.

2.1 Firm Structure

Traditional economic policy analysis looked "through" the firm and focussed on the total amount of labour employed and capital invested.[1] For many purposes, this worked well enough. However, in trade economics it did not and new theoretical frameworks were developed to explain the observed impact of trade liberalization. Modern heterogenous firms trade theory (Melitz 2003 and others) takes into account that firms vary in size, productivity and innovation success - a good innovation bet makes a firm more profitable (hence more "productive"), the firm grows faster, pays better wages and has first call on skilled labour. This theoretical framework immediately integrates Canada's three much lamented "problems": challenges in scaling firms, poor innovation outcomes despite quality inputs, and lagging productivity growth.

In trade, the reduction of barriers to trade changes the firm structure of industries. Lower-productivity firms exit the market due to increased import competition and cede their market share to higher-productivity firms as well as to imports. In addition, the highest-productivity firms gain expanded access to foreign markets and adjust their business models for larger scale production. The observed result from this transfer of market share to higher-productivity firms is higher average productivity in the economy, more innovation and the scaling up of the successful firms.

Table 1: Canada's Trade Balance on R&D Services and IP, 2016, CDN$ billions

	R&D Services	IP	Total
Receipts	5.5	6.0	11.5
Payments	1.6	15.3	16.9
Balance	3.9	-9.3	-5.4

Source: Ciuriak and Goff (2021). R&D services data from Global Affairs Canada (2021b); IP receipts and payments from World Bank Indicators, charges for the use of IP, receipts and payments (BoP, current US$) converted to CDN$.

This is the nexus that strategic procurement for military modernization needs to target.

2.2 New Forms of Capital, the Capture of Economic Rent, and Geopolitics

When a new form of productive capital is introduced, it is relatively scarce and captures economic rents. Existing factors are not made "more productive" – they continue to earn their marginal productivities while the new kid on the block skims off a disproportionate share of the additional profit (since being the relatively scarce and hence critical factor provides bargaining power).[2]

It is useful to think of AI technologies as a form of productive capital – "machine knowledge capital" – since it competes with and complements "human knowledge capital". With the explosive growth of generative AI (GenAI) applications in productive tasks, the emerging stock of intangible productive assets will rise and capture a growing share of national income.

A scan of economic history suggests that the characteristics of an economy, the social orders that emerge from it, and the source of military power are based on the nature of the essential productive assets of the age (Table 2).

The significance for international relations of dominance in the essential productive asset is underscored by transition in power across the ages. The first mover in the industrial revolution, England, forged an empire on which the sun did not set by dominating sea lanes and ports and the ability to project mechanized power, not by having a dominant ground game. The United States forged its unipolar moment by becoming the first mover in the knowledge-based economy at a time when it was back on its heels in the mature industrial economy competition with the rising East Asian "Tigers". The US lost its unipolar advantage when China entered the data-driven economy contemporaneously with it – but with scale advantages and with less vulnerability to information warfare because of its Great Firewall and state censorship.

We are now in a new economic era, that of machine knowledge capital, ushered in by the jaw-dropping advances in scaling and training AI systems during the data-driven economy era that set up the breakthroughs in large language models (LLMs) in 2022, which triggered the shock waves of 2023. While the United States, just as in the data-driven era, has led the development of cutting-edge models, the disruption is likely to come from the bottom – where China has the scale advantage in terms of sheer number of firms developing basic applications in a ferociously competitive environment that is driving down the cost of access to AI support platforms.

The prospects for the West are not helped by the manufacturing FOMO ("fear of missing out") that has taken a grip here, including an incomprehensible economic "originalism" in the United States where Alexander Hamilton's tariff policy is being cited as a model to make America a great manufacturing powerhouse again (e.g., Cass, 2024). Hamilton lived in the

1 For a deeper discussion of the difference between "looking through" firms to underlying assets and "looking at" firms to understand firm structure of industries, see Ciuriak (2023a).

2 Bargaining power ultimately determines the distribution of additional economic rent enabled by the new factor of production. See, e.g., the discussion in Guzman and Stiglitz (2024), note 1. When the knowledge-based economy took hold after 1980 with the widespread deployment of the personal computer, measured "labour productivity" rose but real wages did not – in reality, the additional returns were captured by the owners of the new technology and were reflected in the soaring value of intangible assets on the books of companies. See Ciuriak (2024b) for a discussion.

pre-industrial era, when manufacturing was artisanal – when Hamilton delivered his famous *Report on Manufactures* in 1791, the first steam-powered cotton mill had just been established in Manchester in 1790, the first Luddite riots were still two decades in the future, and Ricardo's famous pamphlet introducing the theory of comparative advantage in support of a pro-manufacturing policy in England would not come for more than half a century. There were no complex supply chains; tariff lines numbered in the dozens (Hamilton's *Report on Manufactures* proposed tariffs on just over 20 items; Irwin 2004). The idea of a firm like the Netherland's ASML, whose lithography equipment is a key cog in the computer chip manufacturing chain, with a supply chain of 5,100 suppliers (ASML 2024), was simply beyond that world. Whatever tariffs might have done for Hamilton's nascent United States of America, they won't do it in this world – not for the Trump administration, which is contemplating across the board tariffs on products that the United States produces (the majority of which Canada also produces) and punitive tariffs on China and others under the proposed Trump Reciprocal Trade Act (Ludwikowski et al. 2024), and not for Canada if it follows suit. Recognizing which areas to emphasize in our current economic age will determine relative success – and for Canada it certainly won't be in areas such as shipbuilding where we already apply 25% MFN tariffs and petitioners are pressing for 100% (Maritime Executive 2024). More on this below.

Table 2: Characteristics of Economic Ages Based on New Forms of Capital

	Time Frame	Essential Productive Asset	Dominant Economic Institutions	Rent Capture through International Relations
Pre-Industrial	Pre-1820	Land (well-watered)	Fiefs and the manorial system	Wars of conquest for control of land and its rents
Industrial Capitalism	1820-1980	Machinery for mass production	Firms that have achieved minimum efficient scale	Market expansion through colonies / gunboat "diplomacy"
Knowledge-Based Economy	1980-2010	Technology controlled by IP rights	Firms controlling IP with freedom to operate (FTO)	Trade agreements (TRIPS, FTAs)
Data-Driven Economy	2010-2022	Data	Superstar firms controlling data and data analytics	Access to data (including FTA clauses on free flow/data localization)
Machine Knowledge Capital Era	2023 and on	AI	Massively parallel development of AI apps	Arm's race to dominate AI development

Source: The author.

2.3 Innovation is Accelerating but Also Getting Harder

Since the dawn of the knowledge-based economy in the early 1980s, numerous indicators suggest an accelerating pace of innovation. These include: rising share of research and development (R&D) spending in GDP; steeply rising numbers of patent applications and awards; a rising share of market capitalization of firms accounted for by intangible assets, much of which is comprised of protected IP; a steep increase (until recently) in international receipts for IP; the emergence around 2013, and the subsequent steep rise, in the number of unicorns (private companies valued at over US$ 1 billion); and the exponential increase in the volume of venture capital.

Other indicators of innovation acceleration include the number of scientific publications (which are precursors to technological advance, particularly in emerging sectors like biotechnology, nanotechnology, and most recently AI); and the shrinking time between the introduction of new technologies and their widespread adoption. For example, in the latter regard, smartphones and cloud computing went mainstream much more quickly than the telephone or electricity; Brynjolfsson and McAfee 2014). The same is true of LLMs; notably, ChatGPT became the fastest technology in history to gain over one million users upon its release on November 30, 2022.

At the same time, many indicators point to an apparent waning of business dynamism in the advanced economies, including: a decline in the rate of new business formation (e.g., Decker et al. 2014; Hathaway and Litan 2014); increasing market concentration (which is associated with the rise of superstar firms; Autor et al. 2020); fewer workers switching jobs or moving between industries (Hathaway and Litan 2014; Molloy et al. 2016) – although the pandemic shock interrupted this trend at least temporarily; declining productivity growth, which could reflect a slowdown and declining in the diffusion of new technologies and innovations from leading firms to the rest of the economy (Andrews et al. 2016; Olmstead-Rumsey 2019).

A coherent explanation for this confluence of indicators is that, while the automation of R&D and the advent of machine learning has accelerated the pace of innovation, it has also made innovation more resource-intensive and changed the risk-return calculation for entrepreneurs since higher investment costs and shorter payback periods: (a) drive up the hurdle rate required to justify a venture, and (b) shorten the runway for scaling before seeking exit strategies. This skews innovation into superstar firms which can innovate on their own account and snap up start-ups with successful innovations at attractive prices. This works against the interests of small, open economies like Canada, since the superstar firms are US-based.

2.4 The Economic Bottom Lines

The main takeaway for military modernization from the foregoing is that the civilian part of military-civilian fusion faces three imperatives: the need to build firms that can scale (which almost by definition in an age of innovation means they own valuable IP that provides them the “freedom to operate” needed to grow); the need to carve out competitive niches in the development of machine knowledge capital, with a likely focus on software, quantum and cybersecurity given that we are out-muscled on heavy industry; and (c) the need to provide Canadian firms the runway to scale up rather than seek early exit strategies. These imperatives should inform the procurement strategy as Canada modernizes its military.

3. Building Winners: The Procurement Solution

Government procurement is a well-established tool of industrial policy in general and in defence procurement in particular, as illustrated by iconic programs such as the US Defense Advanced Research Projects Agency (DARPA). It is also the tool that is most relevant for a small, open economy in an age of innovation (Carbonneau and Ciuriak 2024).

Government acting as a launch customer leverages the role of "sophisticated demand" (Porter 1990) to stimulate innovation through initial contracts, which allow firms to acquire "learning by doing" skills (Arrow 1962); the purchase contract then serves as the runway for investment to commercialize the required technology and scale up production. Importantly, procurement of novel systems involves the client in the development of the solutions and naturally results in a "connected system". As described in Carbonneau and Ciuriak (2024), the connected system developed in the United States for military procurement was the successful model for innovation, not the disconnected system adopted for civilian innovation policy.

With limited resources Canada needs to focus on its comparative advantage in the new economy. For example, Canada will need hulls and drones and, based on Ukraine's success in the Black Sea, drone hulls. The geopolitical problem with connected devices is not the devices necessarily, but the connections. For example, US restrictions on connected vehicles focus on 'vehicle connectivity systems' (VCS) – that is, systems and components connecting the vehicle to the outside world, including via Bluetooth, cellular, satellite, and Wi-Fi modules – and 'automated driving systems' (ADS), which allow highly autonomous vehicles to operate without a driver behind the wheel" (White House 2024). This suggests a rule of thumb: buy the hulls or drones from the low-cost supplier and focus on developing and building the secure communications. The supply chain challenge is to obtain the device without the connections and supply the latter on a secure basis. Building this capacity in Canadian firms then will allow Canada to scale up to address similar problems encountered by our allies and indeed leverage their procurement.

This raises, in the first instance, the political economy challenge of going decisively against manufacturing FOMO instincts. A little bit of history might help provide the political backbone. Let's return to shipbuilding. The United States was the world's leading builder of hulls in the age when sail was the most economical model and the American-built clipper ships dominated commercial shipping. It clung to its established position when steel hulls became more efficient and resorted to protection through the infamous Jones Act. The results can be read from Table 3. The North American auto industry is going down the same route. Canada's military procurement should emphatically avoid this and focus on 21st Century technology.

This raises a second issue: that of discovery. How to identify which niches can be filled by innovative products and which Canadian firms can fill these niches? This can only be done by talking to Canadian companies. At present, there are hundreds of thousands of firms worldwide using the AI development platforms. Talking to the Canadian users of these platforms informally to identify possible connections to the slate of procured goods and services would be the first step towards what we would hope to be a match made not in heaven but in cyberspace.

For example, when considering potential dual use cases that would fill a current procurement niche, the Canadian government could start with a set of questions to Canadian firms that appear to have rel-

evant expertise and use the responses to refine a request for expressions of interest and/or a full-fledged request for proposal. This would prioritize use cases in which Canadian firms have good prospects. Also, importantly, if any individual Canadian firm lacks the breadth of expertise to undertake such a project, the government could support the participation of several in a joint venture. The key outcome at the end of the day, in addition to the procured solution, should be a Canadian firm that holds IP and is on a "learning by doing" curve that enables it to tackle adjacent use cases. Putting out parallel contracts to multiple firms raises the probability of a successful solution – recall the US experience with replacing vacuum tubes that resulted in the silicon chip – Texas Instruments succeeded where Westinghouse and General Electric did not. The engagement of government experts in the project development, and the use of the convening power of the government to pull in academic research to solve problems (recall the German Fraunhofer Institutes which engage with private firms to solve thorny technical problems), raises the chances of success, a point underscored by the success of the US "connected system" of innovation that characterized military procurement in the post-WWII era (see Carbonneau and Ciuriak 2024).

This raises a third issue: rapidly ramping up a capability to engage with innovation is not something that fits the profile or job description of risk-averse civil servants. If Canada is to meet the challenge of addressing its military modernization and economic development objectives in our new age of machine knowledge capital – which is unfolding with unprecedented rapidity – it will take a SWAT team of experts, reporting to a hierarchy in which career prospects are tied to risk-taking, not risk avoidance (DARPA comes to mind), to establish a new interface between government and industry.

That would not be the end of the challenges. Many things won't be easy: fostering a mindset of risk-taking in developing solutions; navigating the trade commitments that Canada has made with respect to government procurement at the World Trade Organization and in its regional free trade agreements; and preparedness to address other policy constraints on Canada's innovation in areas ranging from taxation to federal-provincial relations. However, it would be a start in the right direction.

Table 3. Year-end Orders for Large Ocean-going Ships. Number of Ships

	2022	2021	2020
China	1,794	1,708	1,216
South Korea	734	626	441
Japan	587	612	533
Europe	319	288	284
United States	5	3	4

Source: Potter (2024)

Dan Ciuriak (ciuriakconsulting@gmail.com)

Dan Ciuriak is a senior fellow at CIGI, where he is exploring the interface between Canada's domestic innovation and international trade and investment, including the development of better metrics to assess the impact of Canada's trade agreements on innovation outcomes. Based in Ottawa, Dan is the director and principal of Ciuriak Consulting, Inc. Dan is also a fellow in residence with the C. D. Howe Institute, a distinguished fellow with the Asia Pacific Foundation of Canada and an associate with BKP Economic Advisors GmbH of Munich, Germany. Previously, he had a 31-year career with Canada's civil service, retiring as deputy chief economist at the Department of Foreign Affairs and International Trade (now Global Affairs Canada).

References

Andrews, Dan, Chiara Criscuolo, and Peter N. Gal. 2016. "The global productivity slowdown, technology divergence, and public policy: A firm level perspective," Hutchins Center Working Paper #24, 27 September, Brookings.

Arrow, Kenneth J. 1962. "The Economic Implications of Learning by Doing," *Review of Economic Studies* 29(3): 155-173

ASML. 2024. "Responsible supply chain: Upholding our sustainability principles throughout our supply chain," Webpage. https://www.asml.com/en/company/sustainability/responsible-supply-chain.

Autor, David, David Dorn, Lawrence F Katz, Christina Patterson, and John Van Reenen. 2020. "The Fall of the Labor Share and the Rise of Superstar Firms," *The Quarterly Journal of Economics* 135(2), May: 645–709. https://doi.org/10.1093/qje/qjaa004.

Brynjolfsson, Eric and Andrew McAfee. 2014. *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W.W. Norton & Co.

Carbonneau, Laurent and Dan Ciuriak. 2024. "Building Winners: Strategic Procurement in the Age of Innovation," Policy Report, Council of Canadian Innovators, 10 September. https://www.canadianinnovators.org/content/building-winners-strategic-procurement-in-the-age-of-innovation.

Cass, Oren. 2024. "When 'That's How It's Always Been Done' Is a Winning Argument," American Compass, 18 November. https://americancompass.org/when-thats-how-its-always-been-done-is-a-winning-argument/.

Ciuriak, Dan. 2024a. "The Investment Canada Act: Updates for the Knowledge-Based and Data-Driven Economy at the Dawn of the Age of Machine Knowledge Capital," Brief in support of remarks to the Standing Senate Committee on Banking, Commerce and the Economy at its hearing on Bill C-34, An Act to amend the Investment Canada Act, 20 March 2024. https://papers.ssrn.com/abstract=4771331.

Ciuriak, Dan. 2024b. "The USMCA Review: Whither North American Integration?" Working Paper, 15 April. https://papers.ssrn.com/abstract=4800082.

Ciuriak Dan. 2023a. "Enterprise Value and the Value of Data," Conference paper, IARIW-CIGI Conference on "The Valuation of Data", November 2-3, 2023, Waterloo, Ontario, Canada. https://papers.ssrn.com/abstract=4617940.

Ciuriak, Dan and Patricia Goff. 2021. "Economic Security and the Changing Global Economy," Centre for International Governance Innovation Series: *Reimagining a Canadian National Security Strategy Report No. 8*. 13 December. https://www.cigionline.org/publications/economic-security-and-the-changing-global-economy/.

Decker, Ryan, John Haltiwanger, Ron Jarmin, and Javier Miranda. 2014. "The Role of Entrepreneurship in US Job Creation and Economic Dynamism," *Journal of Economic Perspectives* 28(3), Summer: 324.

DND. 2024. "Our North, Strong and Free: A Renewed Vision for Canada's Defence," Department of National Defence. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

Guzman, Martin M. and Joseph E. Stiglitz. 2024. "Post-Neoliberal Globalization: International Trade Rules for Global Prosperity," Working Paper 32533, June. http://www.nber.org/papers/w32533.

Hathaway, Ian and Robert E. Litan. 2014. "Declining business dynamism in the United States: A look at states and metros," *Economic Studies at Brookings*, May.

Humpert, Malte. 2024. "China-Russia Announce Plans for Five Ice-Capable Containerships for Year Round Arctic Service," *High North News*, 15 October. https://www.highnorthnews.com/en/china-russia-announce-plans-five-ice-capable-containerships-year-round-arctic-service.

Irwin, Douglas A. 2004. "The Aftermath of Hamilton's 'Report on Manufactures'," *Journal of Economic History* 64(3), September: 800-821. DOI: https://doi.org/10.1017/S0022050704002979.

Ludwikowski, Mark R., R. Kevin Williams and Sally Alghazali. 2024. "Trade policy following Trump's 2024 election victory," Reuters, 19 November. https://www.reuters.com/legal/legalindustry/trade-policy-following-trumps-2024-election-victory-2024-11-19/.

Maritime Executive. 2024. "Canadian Shipbuilders Calls for 100 Percent Tariff on Chinese-Built Ships," Press Release, 30 August. https://maritime-executive.com/article/canadian-shipbuilders-calls-for-100-percent-tariff-on-chinese-built-ships.

Melitz, Marc J. 2003. "The Impact of Trade on Intra-Industry Reallocations and Aggregate Industry Productivity," *Econometrica* 71(6): 1695-1725.

Molloy, Raven, Riccardo Trezzi, Christopher L. Smith, and Abigail Wozniak. 2016. "Understanding Declining Fluidity in the U.S. Labor Market," Brookings Papers on Economic Activity, Spring: 183-259.

Olmstead-Rumsey, Jane. 2019. "Market Concentration and the Productivity Slowdown," MPRA Paper, 93260.

Porter, Michael E. 1990. *The Competitive Advantage of Nations*. New York: Free Press.

Potter, Brian. 2024. "Why Can't the U.S. Build Ships?" guest post, Noahpinion, 05 September. https://www.noahpinion.blog/.

White House. 2024. "Protecting America from Connected Vehicle Technology from Countries of Concern," Fact Sheet, 23 September. https://www.whitehouse.gov/briefing-room/statements-releases/2024/09/23/fact-sheet-protecting-america-from-connected-vehicle-technology-from-countries-of-concern/.

The Intersection of Artificial Intelligence with Space and Cyber in the Contemporary Security Environment

BGen (Ret'd) Roberto Mazzolin Ph.D., P.Eng., OMM, CD, SMIEEE
Chief Defence, Security and Technology Strategist Rhea Inc., Starion Group, Nexova

Global competitiveness is increasingly being characterized by national technological capabilities. In fact, strategic security is increasingly dependent upon advanced technological capabilities and a presence in the space and cyber environments. Artificial Intelligence (AI) has witnessed a form of rebirth following since the early days of Machine Learning and affords new opportunities and risks as its rapid development is contributing to the new military operational domains of Space and Cyber. Space and cyber operations and their convergence with AI are increasingly recognized as key enablers in modern intense interstate competition where key global players endeavour to take advantage of the digital revolution and military conflicts where non-state actors, private industry, and nongovernmental organizations (NGOs) are increasingly directly involved. In fact, the confluence of these capabilities is reshaping the manner by which nations approach national geopolitical and military strategy and supporting operations. Aside from the US, key among these nations are China and Russia who are currently at the forefront of security challenges to the West. This paper will highlight a number of key areas where AI is making particularly notable contributions to the space and cyber domains to further amplify their impact to military and security affairs.

The Chinese Belt and Road Initiative ties directly with President Xi Jinping's vision of returning China to its historical role at the centre of the world. Chinese strategic documents have historically emphasized information dominance in pursuit of its strategic objectives and this is reinforced through its developments in the areas of advanced technologies such as AI, the domination of the electromagnetic spectrum and space deterrence (Arora and Doshi 2020, page 26). China's efforts to dominate the international technology environment by influencing core innovation in emerging technological fields such as 5G and AI as part of its "Civil Military fusion" strategy to enhance China's capacity to transform the international standardization landscape. To that end, China has established technical standardization agreements that embrace both civil and military capabilities with over 49 countries and regions along the Belt and Road to promote adherence to Chinese standards, which in turn enable it to assert exceptional influence in the strategic security domain given the dual use nature of the technologies it seeks to dominate (Baark 2021, page 3).

The contribution of AI to the enablement of the rapidly evolving Space and Cyber domains aligns with many of the concepts articulated in Sun Tzu's "The Art of War" relating to "deception and the formless" in the battle space. Russian military thought sees modern warfare as a struggle over information dominance and netcentric operations that can take

place without clear boundaries and is pursuing the goal of incorporating Electronic Warfare (EW) capabilities throughout its military to both protect its own space-enabled capabilities and degrade or deny those capabilities to its adversary. In space, Russia is seeking to mitigate the superiority of US and NATO space assets by fielding a number of ground, air, and space-based offensive capabilities that increasingly leverage AI capabilities (Zysk 2017, page 1).

AI and its Role in Evolving Security Considerations

AI has democratized space and cyber to a broader range of players such as start-ups, universities and small nations by facilitating economical implementation of many new civil and military capabilities that historically were limited to major nation states. Given the degree of interconnectedness associated with these environments, one of the collateral consequences of such activities is the potential for conflict to propagate into other geographic areas and outer space.

Countries such as the US, China and Russia, along with NATO allies are competing to secure battlefield advantage through the use of data and supporting analytics to effect superior speed in decision-making and supporting manoeuvre (DIA 2022, page 4). AI enables the rapid screening and analysis of large volumes of data and provides decisional support information in short time frames. The Ukrainian conflict is serving as a test bed for the integration of AI and digital technologies into the operational kill chain and supporting operations. Lessons learned are feeding concept development in China and Russia as well as the US Joint All Domain Command and Control (JADC2), NATOs Multi-Domain Operations (MDO) development and new programme development to field future generation systems for AI centric space and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities (Odgen et al. 2024, page 6).

In the coming years, AI will increasingly play a powerful role in evolving operations in military and broader security domains supporting national interests and societal resilience by furthering new disciplines. Cyber and Space as new military domains share a particular interdependence and furnish critical capabilities that form central elements of critical national infrastructure supporting modern economies. This environment is particularly impacted by AI advancement with key development areas focused on anticipating and responding to threats with greater speed and precision.

AI Enablement of Space and Related Cyber Capabilities

The recent number of commercially financed, launched and operated space constellations that characterize the "New Space" environment have relied heavily upon AI to enable autonomous flight, navigation, tracking and flight manoeuvre activities. These include remotely controlling satellites and landers on remote planets, and docking systems to decrease reliance on human responsibility for mission control activities while ensuring safety and security. AI enabled real-time tracking of satellite and space debris

1 Where "the location where we will engage the enemy must not become known to them. If it is not known, then the positions that they must prepare to defend will be numerous. If the positions the enemy prepares to defend are numerous, then the forces we engage will be few and further developed by the observation. In accord with the enemy's disposition, we impose measures on the masses that produce victory, but the masses are unable to fathom them".

trajectories facilitate space surveillance and domain awareness to anticipate potential collisions and automatically manoeuvre satellites to ensure longevity, safety and debris removal, but also hold the potential to facilitate dual use anti-satellite capabilities under the guise of peaceful commercial purposes.

Although the U.S. has a moratorium on future anti-satellite weapons (ASAT) tests, Russia, India and China all continue to develop ASAT capabilities. Although the last publicly announced Chinese ASAT test was conducted in 2007, it continues to develop capabilities to target satellites via proximity and rendezvous operations via kinetic strike or close proximity robots, cyber and electronic warfare/laser systems. Russia tested an ASAT in 2021 that created over 1500 pieces of debris from one of its own satellites (Hadley 2023). Further, in 2020 US Space Command indicated that the Russian Cosmos 2453 satellite was manoeuvred within 20 kilometres of the USA 245 surveillance satellite (NASA 2013). It was deemed an inspection satellite, however, given that Russia has developed a co-orbital ASAT capability programme called Burevestnik, the potential for offensive capabilities is obvious (Weeden and Samson 2021, page ix).

Further, AI can facilitate the rapid testing and development of satellite systems and components to mitigate the need for expensive bespoke physical prototypes. Such agile system development contributes to the rapid development of tailored assets supporting innovative focused mission sets in space such as "Bodyguard" co-orbital active defence satellites that integrate with terrestrial based counterspace capabilities to protect against increasing threats to satellites in orbit (Harrisson, Johnson and Young 2021, page 4).

The development of such dual-use capabilities afford a range of new and innovative warfighting capabilities in space that afford plausible deniability of military intent and may otherwise be characterized as deterrents to prevent war.

For example, the Ukrainian theatre has served as the most visible example that has witnessed a variety of innovative AI applications that serve to shape the information space. These facilitate among other capabilities, automated real-time battle damage assessment, facial recognition to detect infiltrators, identify corpses, reunite families and counter disinformation. The use of Large Language Models (LLMs) enables commercially available earth observation data, geotagging products and mapping tools to significantly enhance imagery analysis in support of both open source and geospatial intelligence. Intelligence capabilities have been further aided through AI implementations of searchable text databases and voice transcription and translation to intercept and process Russian communications. Further, AI enabled loitering and unmanned drone systems have been extensively used in ISR, strike and logistic operations (Bergengruen 2024).

Given the large number of constellations being fielded, communications are improved through the use of AI algorithms that optimize network resources to efficiently manage bandwidth and associated traffic, as well as rapidly analyze the massive amount of imagery and associated data that are transmitted across these networks. Such capabilities also contribute to the development of scientific activities that support critical infrastructure related to weather, environmental monitoring, agricultural and urban "smart city" development.

As the nature of space operations evolves from individual satellites or small constellations provided by individual governments and operators to very large constellations that are owned and operated by large consortiums serving multiple user communities, security of space and terrestrial activities mandates an increasing requirement to gain transparency and

determine if specific satellites are either malfunctioning or are masking nefarious intent. Here, traditional approaches involve the placement of space-based sensors in outer space to observe movements and facilitate laborious human analysis. Emerging AI techniques involve inverse reinforcement learning to automatically correlate a space assets behaviour to intent without requiring human intervention (Finn et al. 2016, page 2; Ho and Ermon 2016, page 1; Baram et al. 2017, page 1; Saurabh and Doshi 2020, page 1). Such automated analysis enables correlation to potential strategic intent as to why a specific satellite may be acting in a specific manner.

To achieve this, key functions involve automating anomaly prediction, missile warning and tracking, prediction and recovery of systems to protect and defend space-based assets and their associated missions. Increasingly important capabilities supporting military and security operations include dim target tracking, the identification of specific satellites within large constellations to assess the nature of their behaviour and associated anomalous activities such as those to create deception, camouflage and concealment. This is critical in order to distinguish between benign outliers or those that pose a legitimate threat to specific satellites that provide key support to national force projection capabilities or support critical civil infrastructure. Clearly, the ability to rapidly detect and adjudicate an appropriate response would impact geopolitical dynamics.

Given the exponential increase in the number of satellites with greater manoeuvrability to be launched over the next 10 years by state and non-state actors, the utility, protection and successful operation of these constellations will be increasingly dependent on AI. China intends to launch two mega-constellations comprising over 20,000 satellites beginning in 2025 (Shunsuke 2024). The potential for hostile capabilities to be hidden in such large constellations is clearly recognized. To that end, Russia has launched a counterspace platform that could conceivably target western low Earth orbit (LEO) based assets.

Here further potential exists for AI in the area of defensive counterspace to automate defensive response actions in contested environments. Once again, given the dramatic increase in space activity and its application to military and national security interests, there is scope for AI application to the issue of the characterization of foreign launches and the concept of predictive sustainment, for example, the ability to predict maintenance and associated manoeuvre capabilities that would characterize operational intent.

As commercial based assets increasingly support many different logical networks representing various user communities, the vectors for adversary penetration increase exponentially. This is particularly true given the reliance upon COTS technologies, whose inherent vulnerabilities are well understood and exploited by hostile actors. Most commercial "new space" satellite capabilities that are based on "cubesat" architectures are modestly protected from a cybersecurity perspective. As western nations and institutions increasingly rely on commercial terrestrial and space-based infrastructure for the provision of critical infrastructure, they become targets for hostile foreign state and non-state actors. The reliance on space-based communications, earth observation and Position Navigation and Timing (PNT) capabilities are integrated in the very fabric of critical infrastructure that supports societal and military functionality, which in turn impacts government legitimacy. To that end, the Russian attack of the Viasat KA-SAT constellation as a precursor for its invasion had far-reaching effects outside of functionality supporting Ukrainian Armed Forces to that of users in Europe, and particularly critical energy infrastructure in Germany.

To address such vulnerabilities, a further key development area is that of AI enabled adaptive waveforms and associated transmitters and receivers in outer space to more efficiently, reliably and securely transmit data communications in the hostile electromagnetic and congested environment of space where the threat of jamming from hostile actors is increasingly a risk. Here AI provides potential utility in the provision of autonomous platform-based capabilities to detect and respond to radio frequency jamming and interference through adaptive antenna techniques. Further, Zero Trust security frameworks leverage AI technology to gather and synthesize network activity data and identify heuristic behaviour of adversary movement in the network to establish the appropriate cyber situational awareness to posture effective response actions, not only from a cyber security perspective but also from a broader multi-domain operational perspective (Mazzolin and Madni 2022, page 16). Such observations inform mission planners and operational staffs as to adversary intent impacting missions and facilitate rapid response options.

The ability to analyze data faster and maintain decision superiority in critical operational scenarios is vital in the space and cyber domains. The use of AI algorithms to undertake predictive analysis, natural language processing for enhanced communications and computer vision for better surveillance and reconnaissance is an important enabler. Such technical developments further mandate additional investments in professional development and training in order to enable users to take full advantage of such capabilities and understand the implications of their use.

Operational Impacts

AI/ML technology has matured to the point that it is being rapidly applied across a variety of commercial capabilities. This increasingly includes Space Domain Awareness derived from a variety of earth and space sensors supporting military decision-making and future-generation conflicts in the areas of autonomous space-based capabilities and cyber operations.

As in other domains, the emerging field of Generative AI using LLMs to translate human prompts into various forms of media generates the potential to automate many staff processes, augmenting decisional advantage in critical situations. LLMs not only enhance analytical effectiveness, but also significantly improve Course of Action development in multi-domain offensive and defensive operations that would be beyond purely human-based capabilities (Clark 2023). The use of LLMs will enhance the accuracy and speed of military intelligence to identify threats in a multi-domain environment and support the ability to prosecute a much larger number of targeted, complex campaigns.

Just as in other emerging areas of AI application, such as in the case of Lethal Autonomous Weapon Systems, there is an imperative to understand the vulnerabilities and limitations of the technology. To that end, it will be essential to ensure that humans remain "in the loop" so as to correctly guide decisional processes and ensure that they are not corrupted (Mazzolin 2020).

This mandates constant vigilance, flexibility and ability to react along with commitment to progressive AI policy development. Notwithstanding the potentially significant operational cost savings, economic development and functional advantages to be realized through the implementation of AI, the technology also presents the opportunity for hostile actors to actively seek both operational and economic advantage by exploiting vulnerabilities in the space-based infrastructure and associated supply chain. Moreover, it affords the possibility of threat actors to attack on a variety of fronts with nominal infrastructure invest-

ment and plausible deniability.

Ensuring cooperation between governments and corporations in the development of innovative AI capabilities that are both safe to use and can effectively respond to the associated threats will be essential to realizing the promise that this technology holds. Here the ability to keep pace with and anticipate AI developments that may contribute to society along with maintaining a clear understanding of potential threats will be key to ensuring a secure and prosperous future in this rapidly evolving environment.

Looking Forward

The intersection of AI, Space and Cyber represents an inflection point in how nations approach security and military strategy as they directly connect with issues of national security, international cooperation and the nature of armed conflict and key national security considerations. The rapid developments in AI enhance the import of the emerging operational domains of space and cyber. In order to maintain strategic competitiveness and advantage, western nations must carefully posture the development of the emerging dual-use space and cyber economies and the intricacies of national security. Here the intersection of AI, space and cyber afford the possibilities of economic innovation contributing to societal resilience, digital sovereignty and strategic autonomy and security. Investment, development and international choices that nations make now will significantly shape the future geopolitical landscape and must be considered in the context of ensuring global stability.

Clearly, AI offers the potential to greatly improve the efficiency and accuracy of decision-making in the increasingly complex and rapidly changing battlespace and security environment. In light of its dual-use nature, the potential exists for a new arms race among major powers resulting in increased instability and distrust in the international technology, economic and security environments. Although AI militarisation offers enhanced situational awareness in facilitating more efficient decision-making and control which could revolutionize modern commercial and military space and cyber capabilities, it also presents unique challenges.

Among these are security concerns that arise from incongruities between operational AI system data training and actual employment in actual conflict, the potential for escalated use of lethal capabilities due to reduced thresholds, and resultant ethical and human rights issues arising from civil/military codependence on critical space and cyber infrastructure.

To mitigate such negative consequences, a potential way forward requires major AI powers such as China, the US and NATO partners, and other key emerging players to foster greater collaboration in the militarization of AI and lead in the development of global governance in this critical security realm. This would afford greater guarantees of security and opportunities for development opportunities in other nations with emerging AI capabilities.

The approach to collaboration and the development of consensus on a framework for AI in the space and cyber environments will require a combination of technical, policy and legal reforms to ensure transparency. Given that the challenges associated with AI deployment are truly global as they transcend international civil, commercial, military and ethical boundaries, international cooperation is critical. To that end, it behooves modern technologically advanced nations to devote particular focus to AI development and regulation to ensure that its full potential may be realized safely and effectively.

Robert Mazzolin

Brigadier General (Retired) Roberto Mazzolin is the Cyber, Space, Security and Technology Strategist at the RHEA, Starion and Nexova Groups which are multinational companies providing bespoke engineering solutions, systems development and security services for space, military, government and other critical infrastructure. He establishes corporate direction, guiding development and works with client organizations to evolve their programs and capabilities, contributing to corporate engagement with an increasingly diverse and expanding institutional community within the space and cyber disciplines. During his military career, he served in a variety of key command and staff roles at all ranks. Notable appointments during his military service include responsibility for all Canadian Armed Forces and Department of National Defence strategic network, signals intelligence, electronic warfare and cyber operations, strategic cyber policy development, and responsibility for the engineering and program management of the Canadian Army C4ISR (command, control, communications, computers and intelligence, surveillance and reconnaissance) system. Prior to his retirement from the military, he also served at United States Cyber Command as the vice director for strategic policy, plans, force development and training, (the first foreign flag officer to do so).

He is also a Senior Fellow at the Centre for International Governance Innovation and has written numerous publications and spoken extensively in a wide array of international engineering, commercial and industry fora. He holds a Bachelor of Electrical Engineering, a Master of Science with specialization in electronics and guided weapon systems, a Master of Arts in Security and Defence Management and Policy, and a Ph.D. in Engineering. He is a licensed Professional Engineer and a Senior Member of the Institute of Electrical and Electronics Engineers. He is an officer of the Canadian Order of Military Merit, and his many awards include the US Legion of Merit, the US Meritorious Service Medal, the Canadian Chief of Defence Staff Commendation and the Italian Army Chief of General Staff's Commendation in recognition of professionalism and courage for combat actions in Somalia.

References

Arora, Saurabh, and Prashant Doshi. 2020. "A Survey of Inverse Reinforcement Learning: Challenges, Methods, and Progress." *Artificial Intelligence* 297. https://arxiv.org/abs/1806.06877.

Baark, Erik. 2021. China's International Technology Standards Strategy and the Digital Silk Road. *EAI Background Brief No*. 1604. East Asian Institute, National University of Singapore. https:// research.nus.edu.sg/eai/wp-content/uploads/sites/2/2022/07/EAIBB-No.-1604-ChinaStandards-and-Digital-Silk-Road-2.pdf.

Bergengruen, Vera. 2024. "How Tech Giants Turned Ukraine Into an AI War Lab," *Time*, February 8. https://time.com/6691662/ai-ukraine-war-palantir/.

Clark, Joseph. 2023. "DOD Releases AI Adoption Strategy," DOD News. November 2, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/.

Defense Intelligence Agency. 2022. *Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion*. Washington, DC: Defense Intelligence Agency (DIA). https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf.

Finn, Chelsea, Paul Christiano, Pieter Abbeel, and Sergey Levine. 2016. "A Connection between Generative Adversarial Networks, Inverse Reinforcement Learning, and Energy-Based Models." ArXiv. November 25, 2016. https://doi.org/10.48550/arXiv.1611.03852.

Hadley, Greg. 2023. "Saltzman: China's ASAT Test Was 'Pivot Point' in Space Operations." *Air & Space Forces Magazine*, January 13. https://www.airandspaceforces.com/saltzman-chinas-asat-test-was-pivot-point-in-space-operations/.

Harrison, Todd, Kaitlyn Jonson, and Makena Young. 2021. *Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons*. CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?VersionId=wAqLQjDIzXK84wzzWPNbU1WRYs5dnFfU.

Mazzolin, Roberto, and Asad Madni. 2022. "An Overview of Cyber Security Considerations and Vulnerabilities in Critical Infrastructure Systems and Potential Automated Mitigation – A Review." *Journal of Engineering Research and Sciences* 1 (4): 9-21.

Mazzolin, Roberto. 2020. "AI and Keeping Humans in the Loop." CIGI. November 23, 2020. https://www.cigionline.org/multimedia/ai-and-keeping-humans-loop/.

National Aeronautics and Space Administration (NASA). Cosmos 2491-NSSDCA/COSPAR ID: 2013-076E. https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2013-076E.

Ogden, Theodora, Anna Knack, Mélusine Lebret, James Black, and Vasilios Mavroudis. 2024. *The Role of the Space Domain in the Russia-Ukraine War and the Impact of Converging Space and AI Technologies*. Centre for Emerging Technology and Security, The Alan Turing Institute. https://cetas.turing.ac.uk/sites/default/files/2024-02/cetas_expert_analysis_space_and_ai_convergence.pdf.

Shunsuke, Tabeta. 2024. "China to Launch 26,000 Satellites, Vying with U.S. for Space Power," *Nikkei Asia*, January 10. https://asia.nikkei.com/Business/Aerospace-Defense-Industries/China-to-launch-26-000-satellites-vying-with-U.S.-for-space-power.

Stokes, Mark A. 1999. "China's Quest for Information Dominance." In *China's Strategic Modernization: Implications for the United States*. Strategic Studies Institute, US Army War College.

Weeden, Brian, and Victoria Samson. 2021. *Global Counterspace Capabilities: An Open Source Assessment*. Secure World Foundation. https://swfound.org/media/207161/swf_global_counterspace_capabilities_es_2021_en.pdf.

Zysk, Katarzyna. 2017. "Struggling, Not Crumbling: Russian Defence AI in a Time of War**."** *RUSI*, November 20. https://www.rusi.org/explore-our-research/publications/commentary/struggling-not-crumbling-russian-defence-ai-time-war.

Strategic Interoperability in the Age of AI and Robotics

Amos Fox

We are at the threshold of a punctuated shift in military affairs because of the increased relevance of artificial Intelligence (AI), robotics, and autonomous weapon systems. In the Russo-Ukrainian War, for example, Ukraine has used robots—in this case, semi-autonomous drones—to successfully attack, sink, and largely render irrelevant Russia's Black Sea Fleet (Axe 2024). Ukraine's robots consist primarily of suicide maritime drones, one-way aerial drones, and precision guided munitions (PGMs) (Epstein 2024). Ukraine's ability to plug into Western training and technology, quickly grasp the nuances required for those technologies, and then effectively use them on the battlefield are prime examples of interoperability and its importance to the continued relevance of robotics and AI. Ukraine's employment of the US-provided Patriot air defense system is an example of this (Babb 2024). The Patriot's targeting detection and attack software is driven, in part, by AI and semi-autonomous robotic operations (Watts 2021). The proliferation of robotics and AI-enabled robots, which include many PGM variants, is not exclusive to international armed conflict (IAC) like we see between Russia and Ukraine.

Jakub Grygiel (Grygiel 2018) reminds us that technology diffusion to non-state groups and proxy forces will further complicate 21st century concerns pertaining to robotics and AI. The decision by states to arm non-state groups will make the challenge of countering robotics and AI in non-international armed conflict (NIAC) just as challenging as it is in IAC. Yemen's Houthi Rebels, a regional proxy of Iran, provide a glimpse into what we might expect to see in NIAC as robotics and AI continue to be funneled to non-state groups.

Throughout the winter of 2023 and well into the summer of 2024, the Houthis – using Iranian provided technology – harassed international trade, the US Navy, and other state naval forces across the Red Sea region (Gambrell 2024). The link between states and non-state groups in this area is not just speculation. In January 2024, for instance, the US intercepted an Iranian shipment of weapons to the Houthis (US Central Command 2024). The Houthi's elusiveness has resulted in the US and regional partners playing a long-running game of whack-a-mole to contain the Houthis. The approach looks quite similar to the US's failed counterinsurgency strategies for both Afghanistan and Iraq. Iran's diffusion of military robotics and AI-enabled weaponry to the Houthis, coupled with what can be classified as a similar counter-strategy to those used by the US in Afghanistan and Iraq provides policymakers, strategists, and military practitioners tough challenges to ponder regarding the future of technology diffusion to non-state groups in NIAC (Lederer 2024). Tactical success in this conflict, however, results from the ability of allies and partners to work quickly and to work quickly alongside one another.

This essay addresses the challenge of strategic interoperability in the age of AI and robotics from an operational lens. That is, the essay addresses the subject from the position that political units—states

or non-state groups—will find robotics and AI useful, and thus continue to explore their use on 21st century battlefields. The resulting hypothesis is that interoperability is key for addressing internal and external challenges in both IAC and NIAC pertaining to the continued use of robotics and AI.

Interoperability

Western States Don't Go Alone

Why focus on interoperability? The simple answer is that Western warfighting is inherently multinational. As the Chief of Staff of the United States Army, General Randy George asserts, Western states and their militaries do not go to war alone (Baruah 2023). As a result, Western militaries require AI and robotics that are not hidden behind walls of secrecy, but instead are capable of transnational use. To be sure, interoperability is of increasing importance because of the expansion of military alliances, such as the North Atlantic Treaty Organization (NATO), and coalitions, like we see in Iraq and Syria with the Combined Joint Task Force-Operation Inherent Resolve (CJTF-OIR). NATO, which recently celebrated its 75th birthday, notably added both Finland and Sweden (NATO 2024) to its roster during the past 15 months. In addition to organizations like NATO, less formal military partnerships exist to address emergent regional problems. CJTF-OIR was created by the US because of the United Nations Security Council's effort (United Nations Security Council 2015) to address the Islamic State expansion across both Syria and Iraq. CJTF-OIR, which is closing in on its 10th birthday, is the largest military coalition today, consisting of more than 30 states (CJTF-OIR 2024).

Despite a recent announcement about joint funding for weapons and ammunition procurement, currently alliances and coalitions still do not develop technologies, they integrate the technology of their members (Ruitenberg 2024). As it currently stands, states develop AI and robotics in isolation of their alliance or coalition partners (Gubbels 2022). While this continues to make since from a national security and operational security perspective, it makes interoperability (that is, all members working together as a unified singular organization) very challenging (NATO 2023). Some of the pressing challenges include (Derleth 2015), to include (1) technological disparity, (2) command and control factors, and (3) resource differences.

The US, for example, develops technology like the Precision Strike Missile (PrSM). PrSM is the replacement for the US Army's Army Tactical Missile System (ATACMS) (Judson, DefenseNews 2024). During a field exercise in June 2024, the US Army used a land-based PrSM system positioned in Palau engaged a moving target in the Pacific Ocean (Page 2024). PrSM – the missile itself – is an AI-infused robot of sorts. Designed for durability and accuracy, it is built with onboard systems that help it achieve those two aims (LockHeed Martin 2024). However, if that capability remains something that only the US can provide to the coalition, then that limits the capability's dexterity and ability to be used in multiple locations by multiple alliance members.

NATO is making strides to improve interoperability through several initiatives such as its Partnership Interoperability Initiative (NATO 2024) and its Combined Training Initiative (Derleth 2015), but the many of these challenges focus on command and control considerations, but fall short of considering plug-and-play weapon systems. Put another way, NATO focuses on integrating military forces possessing discrete weapon system capabilities, at the cost of finding better ways of harnessing AI-enabled technology and robotics that are shareable across member forces.

Although this challenge has not directly impacted NATO in a meaningful way yet, this problem will become increasingly important as robotics and AI-driven sensors, formations, and command and control systems proliferate on 21st century battlefields. The US Army, arguably the pacing military for Western states, is working hard to replace humans in future front-edge combat formations (Olay 2024). Both George and General James Rainey, commander of Army Futures Command have stated that in future conflicts the US Army, "Will not trade blood for first contact" (Judson, The Robots Are Coming: US Army Experiments with Human-Machine Warfare 2024) and as a result future front line forces will be AI-enabled robotics (Deutsch 2024).

Interoperability Isn't an Academic Exercise

Interoperability is of increasing importance today as IAC and NAIC both appear to be at all-time, post-Cold War highs. Despite the disengagement from Afghanistan in 2021 and drawdowns in Iraq, many Western states are invested in providing security, combating terrorism, and thwarting non-state proxy forces across the greater Middle East. The US and the UK have conducted many punitive attacks on Houthi Rebel camps and facilities in Yemen (Garamone 2024), while CJTF-OIR continues to combat the Islamic State and Iranian militia groups in both Iraq and Syria.

Nonetheless, robotics and AI-enabled weapons systems are not only being used by Western states. Iranian-supplied groups like the Houthi Rebels regularly use unmanned surface vehicles (USVs) to attack Western military forces in the Red Sea (U.S. Central Command 2024). Furthermore, Iran's April 2024 drone attack on Israel, in which Tehran launch upwards of 300 drones from locations within Iran, against cities within Israel, might well offer a glimpse into evolving character of 21st century NIAC and IAC (Hafezi 2024). In this engagement, Israeli, US, and UK air defense and air forces shot down many of these drones before they reached Israel (al-Khalidi 2024). Clearly, the use of AI-enabled robotics is thriving throughout the greater Middle East. Yet, the use of AI and robotics is not limited to this theater.

Both Russia and Ukraine's use of robotics, to include suicide drones, first-person view (FPV) drones, and USVs is another example of robotics and AI on 21st century battlefields. Ukraine has used a combination of USVs and PGMs to neuter Russia's Black Sea fleet, while each state has traded blows with suicide and FFV drones. Interestingly, the use of robotics has not provided either side with an asymmetric advantage, but rather has fully contributed to the war's attritional character and status as a stalemate.

Nevertheless, both Russia and Ukraine's use and production of drones raises questions and concerns with regard to international humanitarian law (IHL). The first question is to what degree are attacks in urban areas – by either side – properly buoyed by the principles of distinction. The second consideration, which is related to the first, is how to address the targeting of dual-use equipment manufacturing in order to limit undue suffering. In Ukraine, for instance, drone production moved into residential apartment buildings and civilian neighborhoods early in the conflict. By operating from civilian infrastructure, any attack on those production facilities which kills a civilian will cause undue suffering. As robotics continue to diversify and diffuse to other states and non-state actors, and AI becomes more prevalent as a tool of war, states will likely have to address additional IHL-related concerns. Notwithstanding the fact that some analysis exaggerates the impact of AI and robotics on the Ukrainian battlefield, they remain an important feature of IAC (Kofman 2024).

The examples outlined above are not the only areas in which robotics and AI have become a con-

cern. To be sure, China's advanced development of robotics and AI and their potential use in annexing Taiwan is a tangible concern. China might use those capabilities across fleets of robotic aircraft and watercraft to blockade Taiwan and deny Western access across the Pacific region to assist Taiwan. Across the board, advanced robotics and AI— perhaps more so than any other weapon system since the proliferation of nuclear weapons in the mid-20th century, are creating waves of concern in the security and defense domain.

Recommendations

This article concludes with three recommendations for policymakers to consider. First, given the multinational nature of Western warfighting, interoperability must be at the forefront of developing future robotics and AI-enabled combat, sustainment, and command and control systems. Remaining agile and responsive to the dynamics of international affairs demands this innovation. As Western military leaders posit, the speed of war is increasing (Association of the United States Army 2024). Thus, the need for strategic agility and responsiveness in addressing the 21st century challenges that robotics and AI now pose, requires multinational formations operating on the technological frontier.

Second, the loss of a robotic system does not carry the same symbolism, emotional cost, nor financial cost as does losing a human soldier. As a result, the willingness to use robotics in more risky operations and tactical schemes are now becoming a routine feature of military planning. Furthermore, states that possess little regard for the lives of their soldiers, much as we have seen with Russia's war in Ukraine (to include the Wagner Group), will likely become even more exaggerated as robotics replace human beings. Robotic systems are also likely less inclined to seek physical security in the ways human forces do. Human soldiers operating on the battlefield often move slowly, from relatively protected position to protected position. Thus, human-centric warfare is somewhat slow when compared to the possible speeds of AI and robotics on future battlefields. As a result, Western states and their militaries must find methods for producing relatively inexpensive robotics and AI that are capable of being rapidly manufactured and produced at the speed and scale of competing nations.

Third, Western states and their militaries must not fall prey to the belief that they have an edge or an upper hand on states like Russia, China, or Iran as it relates to robotics and AI. For each emerging technology that a state and their military develop, many other states, militaries, and non-state actor are observing and working toward the development of means and methods for circumventing that technology. As a result, there are no wonder weapons and very few game-changing weapons in the era of AI and robotics.

The true impact of AI and robotics' on 21st century defense and security remain to be determined. Unfortunately, the full impact of those capabilities will take time and many iterations of IAC and NIAC before policymakers, practitioners, scholars, and analysts can make informed conclusions on the technology. Nevertheless, strategic interoperability amongst allies and partners alike is critical to maximizing robotics and AI on the battlefields of the 21st century.

Amos Fox

Amos Fox is a retired US Army Lt. Col. with multiple combat deployments to Iraq. Amos has a PhD in International Relations from the University of Reading and he is a Research Fellow with Arizona State University's Future Security Initiative. Amos also hosts the Revolution in Military Affairs podcast and is the author of Conflict Realism: Understanding the Causal Logic of Modern War and Warfare.

References

al-Khalidi, Suleimani. 2024. “Most of the Iranian Drones Over Syria Were Downed by Israel, US, Intelligence Sources Say.” *Reuters*, April 14. Accessed July 4, 2024. https://foreignpolicy.com/2024/04/06/us-army-military-robots-soldiers-technology-testing-war/.

Association of the United States Army. 2024. *Association of the United States Army.* June 4. https://www.ausa.org/news/rainey-army-must-adapt-faster-future-fight.

Axe, David. 2024. *Forbes.* March 6. https://www.forbes.com/sites/davidaxe/2024/03/06/ukraines-drone-boats-may-have-herded-a-russian-warship-into-open-water-before-striking/.

Babb, Carla. 2024. “Biden: Ukraine to Get 5 More Air Defense Systems.” *Voice of America*, July 9.

Baruah, Sanjib. 2023. *The Week.* September 26. Accessed July 6, 2024. https://www.theweek.in/news/india/2023/09/26/us-doesnt-fight-wars-alone-anymore-says-us-army-chief-in-delhi.html.

CJTF-OIR. 2024. *Operation Inherent Resolve: Combined Joint Task Force.* July 4. Accessed July 9, 2024. https://www.inherentresolve.mil/WHO-WE-ARE/History/.

Derleth, James. 2015. *NATO.* June 16. Accessed July 2, 2024. https://www.nato.int/docu/review/articles/2015/06/16/enhancing-interoperability-the-foundation-for-effective-nato-operations/index.html#:~:text=Key%20tactical%20interoperability%20challenges%20include,doctrinal%20differences%2C%20and%20resource%20gaps.&te.

Deutsch, Jack. 2024. “America’s Next Soldiers Will Be Machines.” *Foreign Policy*, April 6. Accessed July 4, 2024. https://foreignpolicy.com/2024/04/06/us-army-military-robots-soldiers-technology-testing-war/.

Epstein, Jake. 2024. *Business Insider.* May 6. https://www.businessinsider.com/ukraine-drone-dodges-fire-kills-russian-ship-fighting-black-sea-2024-5.

Gambrell, Jon. 2024. *Associated Press.* June 28. Accessed May 30 , 2024. https://apnews.com/article/yemen-houthi-rebels-israel-hamas-war-43272fa6d0d20728074cad5184700bb1.

Garamone, Jim. 2024. “U.S., U.K. Launch Strikes Against Houthi Targets in Yemen to Protect Red Sea Shippin.” *U.S. Department of Defense*, February 4. Accessed July 4, 2024. https://www.defense.gov/News/News-Stories/Article/Article/3665898/us-uk-launch-strikes-against-houthi-targets-in-yemen-to-protect-red-sea-shipping/.

Grygiel, Jakub. 2018. *Return of the Barbarians: Confronting Non-State Actors from Ancient Rome to Present.* Cambridge: Cambridge Univeresity Press.

Gubbels, Frank. 2022. “NATO Command and Control Center of Excellence.” *NATO.* December. Accessed July 9, 2024. https://c2coe.org/wp-content/uploads/Library%20Documents/Annual%20Overviews/Articles/Annual%20Overview%202022/20230301%20Annual%20Overview%202022%20-%20NATOs%20Interoperability%20Challenge%20is%20FMN%20on%20its%20own.pdf.

Hafezi, Dan Williams and Parisa. 2024. “Iran launches retaliatory attack on Israel with hundreds of drones, missiles.” *Reuters*, April 14. Accessed July 4, 2024. https://www.reuters.com/world/middle-east/iran-launches-drone-attack-israel-expected-unfold-over-hours-2024-04-13/.

Judson, Jen. 2024. “The Robots Are Coming: US Army Experiments with Human-Machine Warfare.” *Defense News*, March 22. Accessed July 4, 2024. https://www.defensenews.com/unmanned/2024/03/25/the-robots-are-coming-us-army-experiments-with-human-machine-warfare/.

2024. *DefenseNews.* June 25. Accessed July 2, 2024. https://www.defensenews.com/global/asia-pacific/2024/06/25/us-armys-new-precision-missile-hit-moving-target-in-pacific-exercise/.

Kofman, Michael, interview by Amos Fox. 2024. "Attrition, Doodling Range Rings, and Magical Thinking in Modern War." *Revolution in Military Affairs [podcast]*. (April 1). Accessed July 4, 2024. https://shows.acast.com/revolution-in-military-affairs/episodes/attrition-doodling-range-rings-and-magical-thinking-in-moder.

Lederer, Edith. 2024. *Associated Press.* May 14. Accessed June 30, 2024. https://apnews.com/article/un-yemen-iran-weapons-houthis-attacks-shipping-ff551c53db019b91bd02684f66f7b29f.

LockHeed Martin. 2024. *LockHeed Martin.* Accessed July 2, 2024. https://www.lockheedmartin.com/en-us/products/precision-strike-missile.html.

NATO. 2024. *NATO.* March 7. Accessed July 2, 2024. https://www.nato.int/cps/en/natohq/news_223446.htm.

2023. "NATO." *NATO.* April 11. Accessed July 4, 2024. https://www.nato.int/cps/en/natohq/topics_84112.htm.

2024. *NATO.* March 7. Accessed July 4, 2024. https://www.nato.int/cps/en/natohq/topics_132726.htm.

Olay, Matthew. 2024. "Promising Experiment Signals Future Integration of Advanced Tech Into Army Units." *U.S. Department of Defense.* March 22. Accessed July 4, 2024. https://www.defense.gov/News/News-Stories/Article/Article/3716688/promising-experiment-signals-future-integration-of-advanced-tech-into-army-units/.

Page, Stephen. 2024. *US Army Pacific.* June 25. Accessed July 2, 2024 . https://www.usarpac.army.mil/Our-Story/Our-News/Article-Display/Article/3814236/3d-mdtf-demonstrate-ability-to-operate-in-the-indo-pacific/.

Rondeaux, Candace and Sterman, David. 2022. "Twenty-First-Century Proxy Warfare." In *Understanding the New Proxy Wars: Battlegrounds and Strategies Reshaping the Greater Middle East*, by Candace Rondeaux, Daniel Rothenberg, and David Sterman Peter Bergen, edited by Candace Rondeaux, Daniel Rothenberg, and David Sterman Peter Bergen, 431. Oxford: Oxford University Press.

Sharp, Jim Zanotti and Jeremy. 2024. *Israel and Hamas Conflict In Brief: Overview, U.S. Policy, and Options for Congress.* Washington D.C.: Congressional Research Institute.

U.S. Central Command. 2024. *Twitter.* July 4. Accessed July 4, 2024. https://twitter.com/CENTCOM/status/1808945587490079074.

United Nations Security Council. 2015. *Resolution 2254.* Resolution, New York, NY: United Nations Security Council.

US Central Command. 2024. *US Central Command.* February 15. Accessed June 30, 2024. https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/3677794/centcom-intercepts-iranian-weapons-shipment-intended-for-houthis/.

Yousur Al-Hlou, Masha Froliak, Dmitriy Khavin, Christoph Koettl, Haley Willis, Alexander Cardia, Natalie Reneau, and Malachy Browne. 2022. *New York Times.* December 23. Accessed July 2, 2024. https://www.nytimes.com/2022/12/22/video/russia-ukraine-bucha-massacre-takeaways.html.

AI and Information Warfare:

The Mockingbird Prototype

Zachary P. Devereaux, Alexandre Bergeron-Guyard, Bruce Forrester, Marc-Andre Labrie, C2I DRDC Valcartier

"Sub-threshold" conflict refers to confrontations that fall below the threshold of traditional warfare but encompass hostile activities and strategies between nations. These conflicts often involve tactics of misinformation, disinformation and malinformation (MIDI) and foreign interference and manipulations of information (FIMI) aimed at undermining democratic alliances and sowing confusion (EEAS 2025). Artificial Intelligence (AI) presents an invaluable tool for detecting and countering deception in these scenarios, enabling collaborative efforts among allies to mitigate the adverse effects of information warfare. Mockingbird, is one such project.

Mockingbird offers a unique capability to discern increases and decreases in text automation over time, providing a bulwark against the malaise that threatens veracity and trust in the digital space. As a prototype, Mockingbird is guided by principles rooted in natural language processing (NLP), machine learning, and statistical analysis.

The scale and scope of the battlespace within which all-domain command and control (C2) occurs in the current day leads to the increasing need for automations of information environment assessment. AI has seen incredible advancements in information processing and as such is a primary candidate to assist in the production of situational awareness through human-machine-interfaces. Some would argue, for example, that AI is the newest weapon in the SIGINT toolkit (Priems, 2023)

This article aims to explore the groundwork required to address the challenge of information warfare in the digital age. By combining a set of novel detection and AI approaches, Mockingbird provides a set of tools for understanding where automated content creation was used, and if a deception campaign is present.

AI and Information Warfare

Sub-threshold inter-state conflicts are characterized by non-kinetic activities that span multiple domains, including cyberspace, information operations, and psychological warfare. Unlike conventional warfare, these conflicts aim to exploit vulnerabilities, influence public opinion, and erode trust between nations. The use of deceptive tactics such as disinformation (intentional falsehoods), misinformation (unintentional false information), and malinformation (genuine information manipulated to deceive or extort) is pervasive in these conflicts.

When the notion of trust— as found in literature on the will to fight (Atran, 2022; Gomez, 2023)— is compared to the context of international competition as follows US doctrine (Staff, 2022), it becomes readily apparent that AI generated text (AIGT) will form at least an OSINT part of a multi-domain battlespace. In such a battlespace, narrative competition will begin with AIGT, and proceed to evolve into images, video and audio, (AIGI, AIGV, and AIGA),

with consequences for all-domain intelligence, and the potential for the detection of indicators and warnings that are currently under-explored, but recognized in the domain of activity based intelligence (ABI) for cyber and social media OSINT (Justice, 2024a, 2024b).

Artificial Intelligence, specifically advanced machine learning algorithms, can play a pivotal role in detecting and countering deception in sub-threshold inter-state conflicts. By leveraging AI's capabilities in processing vast amounts of data, pattern recognition, and natural language processing, deception detection algorithms can be developed to identify and analyze deceptive content, narratives, and malicious actors in real-time. This is where Mockingbird comes in.

AI algorithms can analyze large datasets, including social media posts, news articles, and official statements, to identify patterns and indicators of deception. By examining linguistic cues, sentiment analysis, and cross-referencing with trusted sources, AI can help distinguish between reliable information and deceptive narratives.

AI tools can assist in identifying and tracking the sources of disinformation and misinformation. By analyzing online behavior, network connections, and content propagation patterns, AI can aid in mapping out influence networks and exposing the entities behind malicious MIDI/FIMI campaigns.

In the realm of continental defence, the intelligence community faces the challenge of understanding complex situations with numerous rapidly changing factors. To perform this task, there is a need to consider a variety of information sources, including Open Source (OSINT) and Social Media (SOCMINT) information. Proper exploitation of OSINT/SOCMINT is key to gaining situation awareness, and anticipating emerging threats means that AI will become increasingly involved in the detection of indicators and warnings related to hybrid threats (Dragos, 2020 ; Forrester, 2023).

However, in order make best use of OSINT/SOCMINT, it is essential to determine if the available sources of information are reliable. There is a need to: assess the credibility of a source; understand how much we can rely on the information; and determine if an outside actor is influencing a given narrative through the use of automation.

This article aims at explaining the groundwork required to address this challenge. By combining a set of novel detection and AI approaches, Mockingbird is going to lead the way for a better exploitation of OSINT/SOCMINT as part of ABI by helping understand where automated content creation was used, and if a deception or MILDEC campaign is present.

Given the scale at which data creation, circulation, and storage, is expanding, and the constraints on resources that modern militaries must deal with, AI foundational models as a technological advancement will bring concrete benefits to defence. This will occur both through military partnership with innovators, and the adoption of AI into military intelligence, indicators and warnings, as well as NORAD modernization. AI will be used to prevent, predict, prepare, and protect against the evaporation of long-standing protections afforded by geography and distance. Moreover, 'real-time' narrative led operations in the information environment will necessitate that AI tools, techniques and practices be adopted for the defense of North America (Charron, 2022).

Why the Mockingbird prototype?

Automatically generated text has been a pivotal contributor to the spread of false news or misinformation. Bots, AI systems, or malicious users can employ software to generate text and Bots automat-

ically, which can be disseminated on platforms at a scale and speed that drowns authentic and credible information (Orabi, Mouheb, Al Aghbari, & Kamel, 2020). For example, during OP Trident Juncture 2018 up to 12% to 30% of actors around the exercise were Russian bot automations, depending on the issue-area (Uyheng, Magelinski, Cox, Sowa, & Carley, 2018). Mockingbird will stand up capacity to detect this issue by identifying patterns indicative of automation within text-based communication, thereby segregating likely bot-generated content from human-posted text.

The development of Mockingbird is guided by advancement in the military use of AI, ML, and LLMs. The preliminary phase involves creating a robust text classification model that can distinguish between human and machine-generated text.

In order to build a data driven model, we need to collect a substantial amount of training data: text generated by humans and automated systems. This data will need to be labelled appropriately, such that the model can learn to identify the distinguishing features between the two. The data collection phase may require open-source data access, and careful precautions must be taken to anonymize and secure the data to maintain user privacy and comply with ethical standards. Collaboration between DRDC and the National Research Council of Canada (CNRC) is underway to augment state-of-the-art (SOTA) understanding of current text detection methods, as well as sources of potential data for training machine learning models, and generating AIGT (Fraser, K., Dawkins, H., & Kiritchenko, S., 2024a, 2024b).

Once a sizable and varied dataset is curated, the next phase will involve feature extraction and selection. This will include identifying grammatical patterns, repetition, semantic nuances, frequency of posting, and time-series analysis to note increases and decreases in automation. The compiled features will then be fed into ML models for AI-based pattern recognition.

Lastly, the Mockingbird prototype will require continuous learning mechanisms in order to adapt to ever-evolving text automation techniques. This attribute will require the integration of feedback loops and regular model retraining.

Narrative analysis and the creation of essential elements of information (EEI) in a system to detect enhanced indicators and warning (I&W) left of launch (LoL) is a strong priority in the NORAD modernization S&T project. Generative AI detection capacity is needed as a type of sensor for the detection of influence operations meant to affect democratic societies. Some researchers have shown these influence operations are carried out continually by malign actors on contemporary media with the goal of undermining democracy (McQuinn, 2023. Boucher, 2022). While other research argues that AI forms the best and newest tool in the military toolbox meant to defend democracy (Schick, 2020. Mirghahari, 2023).

Testing and measuring the percentage of AIGT related to military deception (MILDEC) within narratives is required as part of readiness for all-domain intelligence and situational awareness (B. Forrester, Waldman, S., and Ghajar-Khosravi, S., 2023; Verrall, 2022).

Preliminary research results analyzing human and automated texts for comparison and detection were compiled using commercial off the shelf (COTS) detection services highlighted in bold in Table 1, below. This benchmarking tested on the original text in the following section, labelled (1) through (7) is meant to demonstrate that current detection methods are brittle, leading to a need for Mockingbird and new LLM based detection methods. This requirement for automation is largely extrapolated to the need for

AI-assisted methods in various military domains, but especially in IEA and C2 for OIE.

Example: AIGT Essay on Pricing as Information

The following seven AIGT enumerated paragraphs were created using a retrieval augmented generation (RAG) process, and merged with two real sentences. This seven paragraph AIGT essay serves as a test for current, readily available detection methods.

(1) Thus, the pursuit of good society is seen in the battle of pricing strategies, an ongoing drama where traditional economic theories and modern digital complexity dance together in an intricate ballet. Among this whirlwind of digits and discounts, there's an underpinning reality – the essential need for consumer literacy. In this chapter of economic evolution, consumers require more than a simple understanding of price per unit; they need to grasp the ramifications of platform loyalty, subscription models, and the almost omnipresent dynamic pricing.

(2) Adam Smith's baker, brewer, and butcher interacted directly with their customers, and their word-of-mouth reputation was tied to straightforward, if not simple, transactions. Today, consumers interact with faceless algorithms which predict, sometimes eerily accurately, our purchasing behaviour. In economics, there's a term for this predictive ability: price discrimination of the first degree. This echelon implies companies know exactly how much we are willing to pay for a product and charge us accordingly, fine-tuning prices in ways Bentham couldn't have dared to imagine.

(3) Indeed, as we explore further, it becomes glaringly apparent that pricing is not a static signal in the digital marketplace. Algorithms track and change prices in real-time, monitoring competitors, inventory levels, consumer demand, and individual behaviour. Black Friday sales, flash discounts, and personalised promo codes are battle cries in a war for consumer attention, loyalty, and, ultimately, wallets. The price tag, once a stable, democratic informer, has now become a chameleon, changing hues to best blend with the predispositions of its observers. This begs the question – in such a fluctuating environment, does the price tag still serve as the fundamental information mechanism it was intended to be?

(4) Consider the ethical quandaries faced by contemporary consumers. We wrangle with the implications of convenience versus support for local businesses, the allure of immediate gratification

Table 1 : Table of tested AIGT detection COTS (Fraser, 2024a).

Name	URL	Languages	Min input length
CopyLeaks	http://copyleaks.com/ai-content-detector	30 languages	70 words
GPTZero	http://gptzero.me	English	30 words
Sapling	http://sapling.ai/ai-content-detector	English	50 words
Winston AI	http://gowinston.ai	6 languages	90 words
Scribbr	http://scribbr.com/ai-detector	3 languages	25 words
ZeroGPT	http://zerogpt.com	6 languages	70 words

against the sustainability of enduring value. In some sense, we are all Gyges in the marketplace, invisible yet omniscient, grappling with the very nature of our consumption. Are we contributing to a virtuous economic cycle, or are we swept away by the ease of access to a cornucopia of global commodities? *And what of when we are paralyzed by the cornucopia of choices presented to us?*

(5) And just as a society must watch over the moral development of its young through education and mentorship, so too should the collective consumer conscience be nurtured to foster understanding and responsibility within this digital market maze. A yen for sustainable consumption habits and the guidance to navigate through predatory pricing algorithms are as necessary in today's economy as literacy and numeracy were during the Industrial Revolution.

(6) This digital landscape requires a new breed of invisible hand, not of market forces but of consumer education – one that teaches the savvy needed to understand the nuance of our hyper-connected economic environment. Public policy can nudge this process forward, advocating for transparency in pricing algorithms and company accountability. This revolution would not see the replacement of the price tag, rather the elevation of its status – from mere number to nuanced narrative.

(7) In this ever-more-complex world, the good society must nurture a market where transparency isn't hidden behind a dynamic display, and where the consumer is informed, empowered, and therefore truly sovereign. This is not to decry digital marketplaces or their dynamism, but to call for a balance – maintaining the power of the consumer

Table 2 : AIGT COTS detection results for Essay on pricing as information.

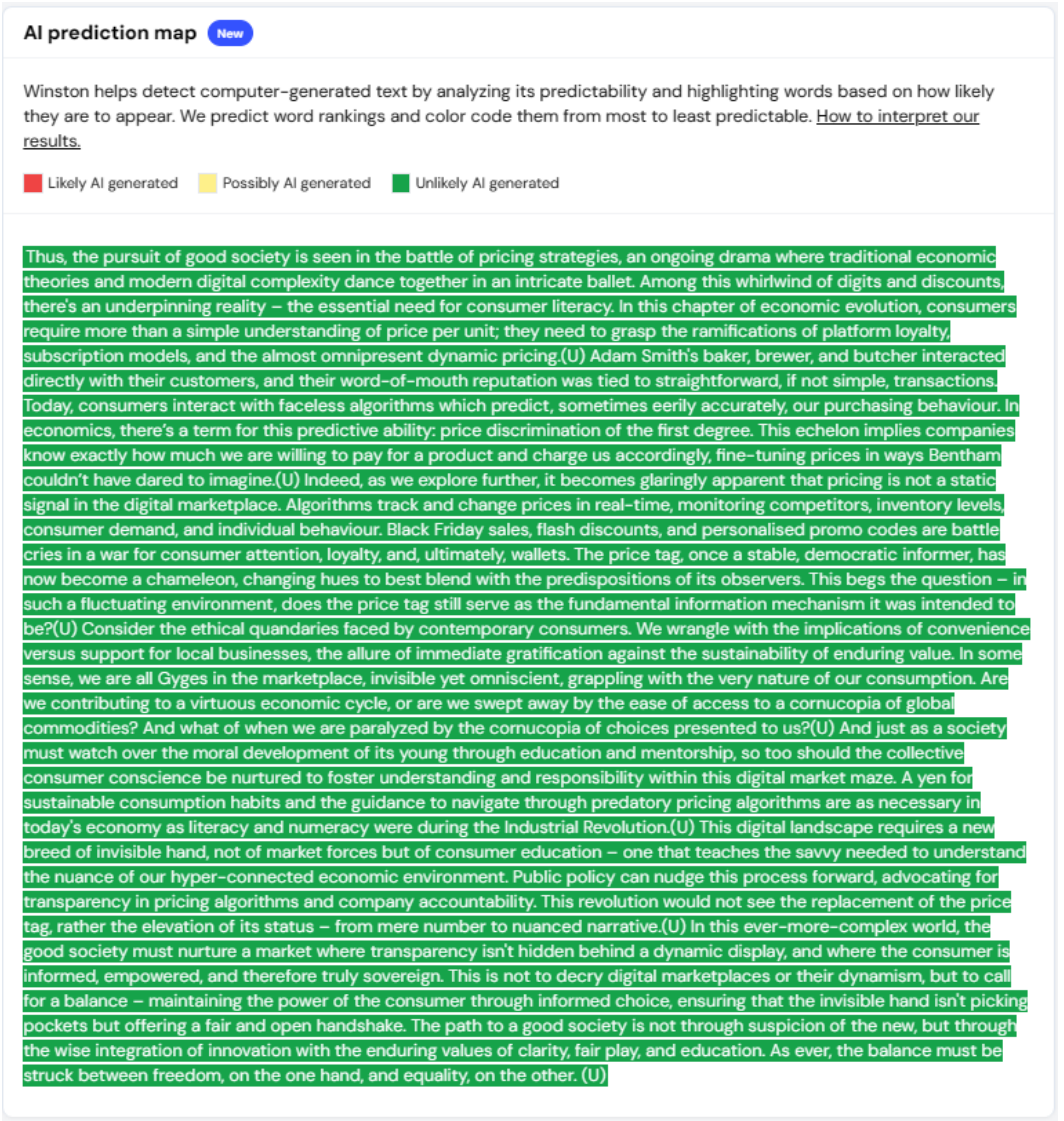
AIGT detection results for Essay on Pricing as Information (only two sentences by the original human author): 7 Paragraphs.
Copyleaks: All Paragraphs = AI content detected **GPTZero: All Paragraphs = 72% AIGT** **Sapling: Paragraphs 1,2 = 99.6 % fake. Paragraphs 3,4 = 99% fake, Paragraphs 5,6 = 0% fake, Paragraph 7 = 0.1% fake** **Winston.AI: All Paragraphs = 99% human** **Scribbr: Paragraphs 1,2,3,4 = 42% chance of AI generation. Paragraphs 5,6,7 = 41% chance of AI generation.** **ZeroGPT: All Paragraphs = This Text is Human written** **LLM based detection : "**AI detection Essay ; the following two sentences were highlighted as most likely written by human within the essay: **Today, consumers interact with faceless algorithms which predict, sometimes eerily accurately, our purchasing behaviour. In economics, there's a term for this predictive ability: price discrimination of the first degree.** **Public policy can nudge this process forward, advocating for transparency in pricing algorithms and company accountability."**

through informed choice, ensuring that the invisible hand isn't picking pockets but offering a fair and open handshake. The path to a good society is not through suspicion of the new, but through the wise integration of innovation with the enduring values of clarity, fair play, and education. *As ever, the balance must be struck between freedom, on the one hand, and equality, on the other.*

The Essay on Pricing as Information has only two sentences created by human writing, highlighted in *Italics* and the rest is AIGT. The two human composed sentences are as follows: *"And what of when we are paralyzed by the cornucopia of choices presented to us?"* and *"As ever, the balance must be struck between freedom, on the one hand, and equality, on the other."* Many of the AIGT detection COTS tested failed to detect either the overall AIGT nature of the essay, or the two human-written embedded sentences, specifically.

As seen from these results, at the time of writing, AIGT detection is still brittle (Stiff, 2022). This motivates the case to develop the Mockingbird proto-

Figure 1: WINSTON AI free version detection results for Essay, section three; the overall AIGT is not detected, and the human sentences in the AIGT are missed.



type for AIGT detection. Producing new AI and LLM capacity for source-characterization and deception detection is an important military undertaking in a generational battle against MIDI and FIMI.

Conclusion: OIE and AI

Discussions on the use of artificial intelligence within Canada's federal government have been ongoing since 2017 (Government of Canada 2025). As the technology has evolved, its potential to support and improve operations has become clear, and increasingly attainable, particularly in a defense context (Department of National Defence 2025).

This supportive capacity extends to several subjects presented in this collection of essays and CAF OIE capacity is needed both for CAF future-proofing, and for improving interoperability with our US allies (Eyre & Matthews, 2024, section 6, 10, 12, and 20 in particular). These AI and ML based capabilities could prove themselves especially useful in the world of government public affairs (PA) for proactive maneuver, and in the world of OSINT and operations in the information environment (OIE) for defensive maneuver (Forrester, 2023). It is, therefore, imperative that Mockingbird is stood up for ascertaining source validity and provenance at the forefront of technology adoption. One set of principles, called the "FAST-ER" (fair, accountable, secure, transparent, educated, relevant) principles, was developed by the Treasury Board of Canada Secretariat for federal institutions to ensure AI tools are responsible and maintain public trust (Government of Canada 2025). This has been expanded on with the current directive for policy via the guide for responsible use of AI in Government (Government of Canada 2025). It is this set of directives, which respects privacy, ethics, legal, and security considerations, that will be the foundation for future defence usage of AI and LLM technologies by DRDC, including Mockingbird. But there can be no mistake that the battle to modernize NORAD, defend North America, and detect MIDI and FIMI cannot be won without the military adoption of AI into C2 and TTP against malign MILDEC.

Zachary P Devereaux

In September 2021 Zachary P Devereaux joined DRDC Valcartier as a Defence Scientist, where he works on analytics and Artificial Intelligence for understanding unstructured text and data-driven methods that have an impact on command, control, and intelligence, including source-characterization. Zach has served as a track co-chair with the International Command and Control Institute since 2022 and is a technical authority on collaborations with industry, the National Research Council of Canada, and the North Atlantic Treaty Organization.

Bruce Forrester

Bruce Forrester is a Defense Scientist at DRDC who has led the development of social media analytics for intelligence exploitation at CAF and NATO. Bruce was recently awarded the NATO Scientific Achievement Award 2018 for SAS-IST-102 on Intelligence Exploitation of Social Media. Bruce spent 26 + years in the Canadian Navy before becoming a defence scientist in September 2010. He graduated from Royal Roads Military College in 1988 with a BSc in Math and Physics and he has a Ph.D. from University of Toronto. He is currently researching influence and detection of values in social media.

Marc-André Labrie

Marc-André Labrie transitioned from the private sector to join Defence Research and Development Canada (DRDC) Valcartier as a computer scientist in 2021. Specializing in software development for Command, Control, and Intelligence (C2I) systems, Marc-André brings a wealth of expertise in artificial intelligence, natural language processing, and data analytics. His work focuses particularly on analytics for understanding unstructured text and data-driven methods, supporting innovative projects that enhance the capabilities of the Canadian Armed Forces.

Alexandre Bergeron-Guyard

Alexandre Bergeron-Guyard is a Defense Scientist at DRDC who has worked on Intelligence analysis systems for over 20 years. He specialises in knowledge based and learning approaches to enhance situational awareness and identify potential indicators of unforeseen events.

References

Atran, S. (2022). The will to fight. *AEON*. Retrieved from https://aeon.co/essays/wars-are-won-by-people-willing-to-fight-for-comrade-and-cause.

Boucher, J.-C. (2022). *Disinformation and Russia-Ukrainian War on Canadian Social Media*. University of Calgary.

Charron, F., Fergusson, J. (2022). NORAD : In perpetuity and beyond.

CSE. (2023). *Cyber Threats to Canada's Democratic Process : 2023 Update*. (ISSN 2563-8165). Ottawa, Ontario, CANADA: Government of Canada Retrieved from https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update.

CSIS. (2023). *The Evolution of Disinformation: A DEEPFAKE FUTURE.* Paper presented at the AOSE - AXIS.

Danry, V., Pataranutaporn, P., Epstein, Z., Groh, M., Maes, P. (2022). Deceptive AI Systems That Give Explanations Are Just As Convincing As Honest AI Systems in Human-Machine Decision Making. *arXiv:2210.08960v1*.

Department of National Defence. 2025. «Foreword.» DND/CAF Artificial Intelligence Strategy. Accessed January 24, 2025. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/dnd-caf-artificial-intelligence-strategy/foreword.html.

Devereaux, Z., Lecocq, R., Forrester, B., Labrie, M.A. (2023). *AI Simulations and MILDEC: Image and texts produced by Artificial Intelligence and thier potential for military deception (AI-IMTXT for MILDEC).* Paper presented at the ICCRTS 28, Maryland, USA.

Devereaux, Z., Lecocq, R., Labrie, M.A., Forrester, B. (2023, Sept 21, 2023). *Contemporary Media and the AI Goldrush from a Military Perspective: Generative AI as War of the Worlds Redux?* Paper presented at the Annual IDeaS Conference: Disinformation, Hate Speech, and Extremism Online, Pittsburgh.

Dragos, V., Forrester, B., Rein, K. . (2020). Is hybrid AI suited for hybrid threats? Insights from social media analysis. Paper presented at the 23rd International Conference on Information Fusion (FUSION), Rustenburg, South Africa.

European External Action Service. 2025. "Beyond Disinformation: What Is FIMI?" Accessed January 24, 2025. https://www.eeas.europa.eu/eeas/beyond-disinformation-what-fimi_en.

Eyre, W. D., Matthews, B. (2024). Department of National Defence and Canadian Armed Forces Policy for The Information Environment. Ottawa, Canada: Offices of the Chief of Defense Staff and the Deputy Minister.

Forrester, B. (2023). Social Media Exploitation: Fighting for Democracy. (DRDC-RDDC-2023-B008). CANADA

Fraser, K., Dawkins, H., Kiritchenko, S. (2024a). *Artificial Intelligence (AI)-Generated Text Detection*. Valcartier: Devereaux, Z., Bergeron-Guyard, A.

Fraser, K., Dawkins, H., Kiritchenko, S. (2024b). *Artificial Intelligence (AI)-Generated Text Detection : Report on Datasets*. Valcartier: Devereaux, Z., Bergeron-Guyard, A.

Gomez, A., Vazquez, A., Atran, S. (2023). Transcultural pathways to the will to fight. PNAS, 120 (24) e2303614120. Retrieved from https://doi.org/10.1073/pnas.2303614120.

Government of Canada. 2025. "Guide to the Responsible Use of Generative AI." Digital Government Innovations. Accessed January 24, 2025. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html.

Government of Canada. 2025. "Progress on Responsible Use of Artificial Intelligence." Accessed January 24, 2025. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/progress.html.

Government of Canada. 2025. "Responsible Use of Artificial Intelligence." Digital Government Innovations. Accessed January 24, 2025. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html.

Gregory, S. (2022). Deepfakes, misinformation and disinformation and authenticity infrastructure responses: Impacts on frontline witnessing, distant witnessing, and civic journalism. *Journalism, 23*(3), 708-729.

Griffin, L. D., Kleinberg, B., Mozes, M., Mai, K.T., Vau, M., Caldwell, M., Marvor-Parker, A. (2023). Susceptibility to Inflence of Large Language Models.

Hwang, T. (2020). *Deepfakes - Primer and Forecast*: NATO - OTAN.

Justice, U. D. o. (2024a). Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm. Retrieved from https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners.

Justice, U. D. o. (2024b). Office of Public Affairs | Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) | United States Department of Justice. Retrieved from https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian.

Lange, B., Lechterman, T.M. . (2021). Combatting disinformation with AI: Epistemic and ethical challenges. *IEEE Access*.

Lee, J., & Shin, S. Y. (2022). Something that They Never Said: Multimodal Disinformation and Source Vividness in Understanding the Power of AI-Enabled Deepfake News. *Media Psychology, 25*(4), 531-546.

McQuinn, B., Kolga, M., Buntain, C., Corchesne, C. (2023). Enemy of my Enemy: Russian Weaponization of Canada's Far Right and Far Left to Undermine Support for Ukraine.

Mirghahari, M. (2023). The Newest Weapon in Irregular Warfare - Artificial Intelligence.

Orabi, M., Mouheb, D., Al Aghbari, Z., & Kamel, I. (2020). Detection of Bots in Social Media: A Systematic Review. Information Processing & Management, 57(4).

Padgett, S. (2019). The Art of Digital Deception: Getting Left of Bang on Deepfakes. *Small Wars Journal*

Priems, G. G., P. (2023). Leveraging Artificial Intelligence For Canada's Army: Current Possibilities and Future Challenges. The Canadian Army Journal, 19.2.

Staff, U. J. C. o. (2022). Joint Concept for Competing. Washington, DC: USA Department of Defense

Schick, N. (2020). *Deep Fakes The Coming Infocalypse*: Twelve.

Stiff, H. J., F. (2022). Detecting computer-generated disinformation. international Journal of Data Science and Analytics, 13, 363-383.

Uyheng, J., Magelinski, T., Cox, R.V., Sowa, C., & Carley, K. (2018) Information Operations Analysis of NATO Trident Juncture Exercise 2018. CASOS, Institute for Software Research, Carnegie Mellon University.

Verrall, N. (2021). Ruse de Guerre Redux. *The RUSI Journal, 166*(3), 68-82. doi:10.1080/03071847.2021.1948803

Verrall, N. (2022). *Closing Knowledge Gaps in "the space between": Adding Explanatory Power to Grey Zone and Hybrid Activities in the Sub-Threshold.* Staffordshire University, Published Works in International Security.