Araya, Daniel; King, Meg

Working Paper

The impact of artificial intelligence on military defence and security

CIGI Papers, No. 263

Provided in Cooperation with:
Centre for International Governance Innovation (CIGI), Waterloo, Ontario

Suggested Citation: Araya, Daniel; King, Meg (2022) : The impact of artificial intelligence on military defence and security, CIGI Papers, No. 263, Centre for International Governance Innovation (CIGI), Waterloo, ON, Canada

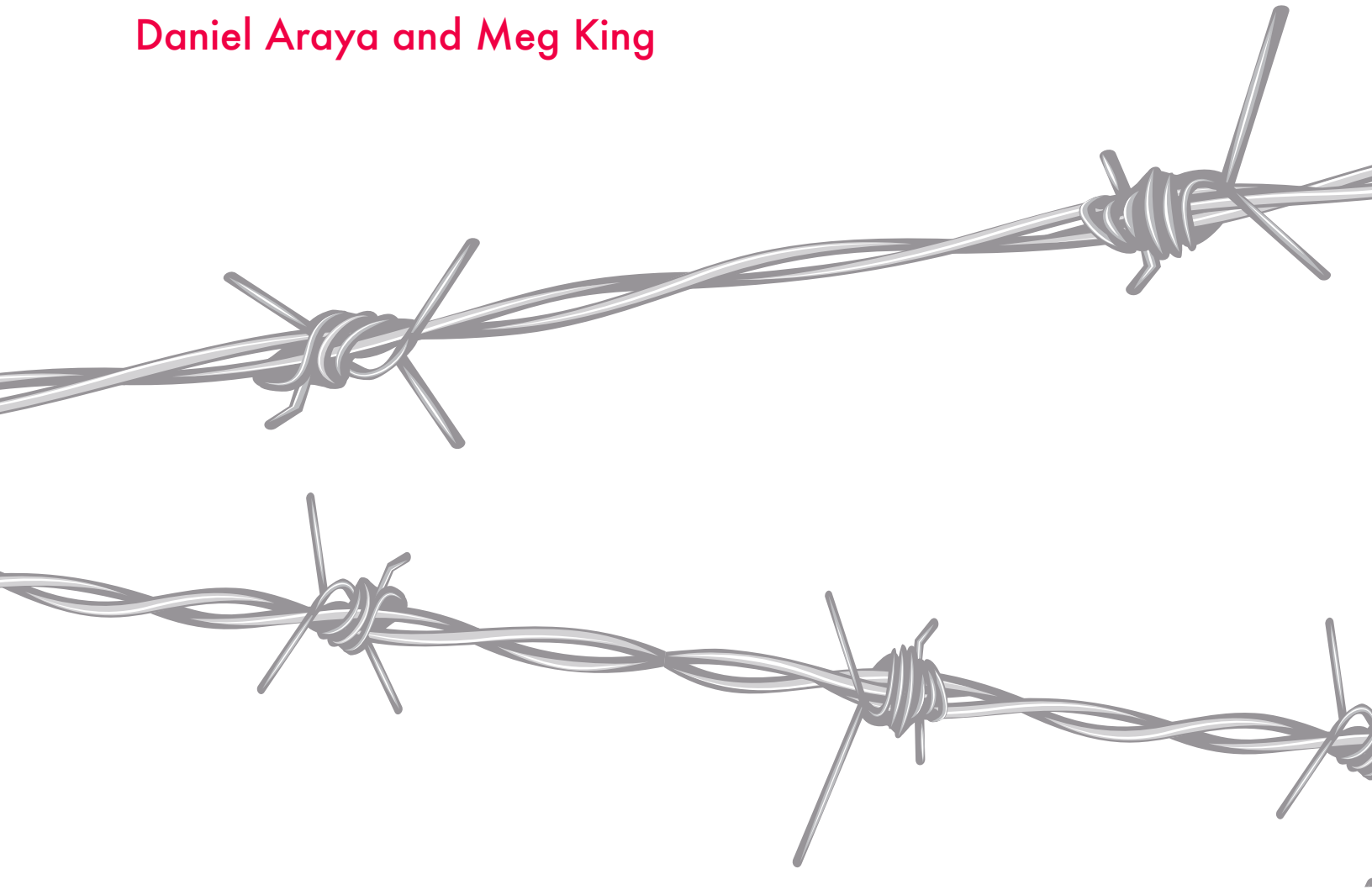
This Version is available at:
https://hdl.handle.net/10419/299735

Centre for International
Governance Innovation

CIGI Papers No. 263 — March 2022

The Impact of Artificial Intelligence on Military Defence and Security

Daniel Araya and Meg King



Centre for International
Governance Innovation

CIGI Papers No. 263 — March 2022

The Impact of Artificial Intelligence on Military Defence and Security

Daniel Araya and Meg King

About CIGI

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

À propos du CIGI

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

Credits

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

This work was carried out with the aid of a grant from the Department of National Defence's Mobilizing Insights in Defence and Security (MINDS) program, Ottawa, Canada.

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

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

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

Table of Contents

About the Project

Without a doubt, the most complex governance challenges surrounding artificial intelligence (AI) today involve national defence and security. CIGI's Facilitating Strategic Engagement: The Impact of AI on Military Defence and Security project brought together leading experts in this area with more than 40 public servants from the Department of National Defence and personnel from the Canadian Armed Forces to discuss the force-multiplying effects of AI on the national security and military sphere.

This endeavour relied on a series of four workshops to generate forward thinking on how data-driven technologies are provoking vast geotechnological restructuring that stands to have profound implications for Canadian national defence planning. Specifically, the workshops centred on data governance and policies (ethics, cloud computing, data readiness and interoperability); decision making (trustability, human-machine integration, biotechnologies and accountability); simulation tools (training, war gaming, human-machine cooperation, robotics, autonomy and trusted AI); and Canadian intelligence in the information age (applying AI to intelligence). CIGI also hosted a graduate seminar to inspire emerging scholars studying in fields such as global public policy, computer science and security throughout Canada.

About the Authors

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

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

Meg King is the founder of the Wilson Center's Technology Labs and former director of the Science and Technology Innovation Program. Previously, she was an international manager for the US Department of Defense's Cooperative Threat Reduction Program. In that role, Meg developed the strategy for a new program in Sub-Saharan Africa established by the Office of the Secretary of Defense to address major digital and physical security gaps in high-risk facilities. Until 2011, she was a senior staff member to the Chair of the House Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. Meg negotiated introduction of the Protecting Cyberspace as a National Asset Act in the House. Key components of that bill became law in 2015. She also shepherded passage of the Reducing Over-classification Act, which President Barack Obama signed into law in 2010. Meg was named one of the 40 under 40 think tank leaders by the University of Pennsylvania. She is a member of the International Institute for Strategic Studies and the Women in International Security Network.

Acronyms and Abbreviations

5G	fifth-generation
AI	artificial intelligence
CAF	Canadian Armed Forces
CCW	Convention on Certain Conventional Weapons
DARPA	Defense Advanced Research Projects Agency
DLT	distributed ledger technologies
DND	Department of National Defence
EDT	emerging and disruptive technologies
GANs	generative adversarial networks
GPAI	Global Partnership on Artificial Intelligence
IoT	Internet of Things
LAWS	lethal autonomous weapons systems
LEO	low-Earth orbit
NATO	North Atlantic Treaty Organization
NORAD	North American Aerospace Defense Command
NSI	national system of innovation
OECD	Organisation for Economic Co-operation and Development
OODA	observe, orient, decide and act
OSINT	open source intelligence
SSE	Strong, Secure, Engaged
UAVs	unmanned aerial vehicles

Executive Summary

This paper explores the development of military-specific capabilities in the context of artificial intelligence (AI) and machine learning. Building on Canadian defence policy, the paper outlines the military applications of AI and the resources needed to manage next-generation military operations, including multilateral engagement and technology governance.

Prospects for sustaining advanced military capabilities are now directly tied to the weaponization of AI. As a general-purpose technology, AI represents a force multiplier with a capacity to reshape the rules of war. Indeed, where nuclear warheads remain a singular application of technology, AI is capable of underwriting many different types of weapons and systems. As guidance from the North Atlantic Treaty Organization (NATO) observes, AI and other "smart" technologies are now fundamental to the future security of Canada and its allies.

New technologies have a long history of transforming the nature of war. From the use of horses and armour to the introduction of aircraft carriers and fighter jets, AI and robotics represent only the latest phase in the evolution of military technologies. Together, the fusion of conventional weapons with AI and machine learning is set to reshape the nature of decision making and the application of force in the transformation of military strategy.

Even as the capabilities of contemporary AI systems are limited to the narrow scope of machine-learning algorithms, this limitation will likely not be true for long. Areas of discovery overlapping neuroscience, quantum computing and biotechnology are advancing quickly and represent uncharted territory in the evolution of "intelligent machines." Scientific and technological discoveries in these new research domains promise significant risk to Canadian national defence but represent significant opportunities as well.

What is clear is that emerging technologies have become the basis for a highly charged geopolitical competition that overlaps a range of commercial industries and technology platforms. China, Russia, the United States and other state and non-state actors are aggressively pursuing the military application of AI and other frontier technologies. Areas of competition include cloud technologies, hypersonic and new missile technologies, space applications, quantum and biotechnologies, and human augmentation.

Notwithstanding the fact that technological innovation has always shaped the nature of interstate conflict, the scale and velocity of emerging and disruptive technologies (EDT) is unprecedented. Canada's defence policy reflects this concern in its call to adapt the Canadian Armed Forces (CAF) to a changing geopolitical landscape. Canadian defence planning has set out to expand and evolve the CAF by incorporating next-generation surveillance aircraft, remotely piloted systems and space-based assets in the integration of new military platforms.

Grounded in a broad assessment of a shifting technology landscape, Canada's Department of National Defence (DND) recognizes that this new era is marked by changes in the global balance of power. This includes changes in the nature of great power competition across a rapidly evolving innovation economy. Much as oil and steel set the terms for the industrial age, so AI and machine learning could now set the terms for the digital age.

Disruptions of this magnitude are driven by the convergence of technological and institutional changes that can trigger complex feedback loops in new and unpredictable ways. In this new environment, AI technologies will force-multiply the capacity of the world's militaries to project power. Determining the guardrails in the evolution of military AI will be critical to avoiding future crises. The application of risk-reduction measures to identify and mitigate the spectrum of risks that may stem from military AI will be key. Indeed, it may be easier to govern AI before these capabilities become fully embedded into the world's current and future militaries.

Taken as a whole, this transition portends a dramatic shift away from rudimentary machines and toward data-driven technologies and precision electronics. This accelerating convergence of physical, digital and biological technologies represents the early stages of an enormous technological revolution. Governing these emerging and disruptive technologies at the global level will be critical to reducing the risk of future conflict.

Introduction

From AI and robotics to battery storage, distributed ledger technologies (DLT) and the Internet of Things (IoT), EDT are now provoking a new era in commercial innovation. This vast landscape of technological change is fomenting a social and economic transformation that has enormous implications for the evolution of the CAF. As a recent report from NATO observes (NATO Advisory Group on Emerging and Disruptive Technologies 2020), these technologies include:

- **AI and machine learning:** The development of AI/machine learning and their potential impact on innovation. This includes neuromorphic computing, generative adversarial networks, and the capacities of AI to reveal unexpected insights from data that has been gathered or is yet to be gathered.
- **Quantum technologies:** The ongoing translation of knowledge gained from the study of quantum processes to the application of quantum-enabled technologies including quantum computing, quantum sensing, quantum cryptographic systems, and the manipulation and development of material at the quantum scale.
- **Data security:** The design of algorithms and systems for securing and compromising the security of communications, data transactions and data storage, including quantum proof encryption methods, blockchain and distributed ledger architectures, and the field of cybersecurity more broadly.
- **Computing-enabled hardware:** Advances in miniaturization, power harvesting and energy storage, encompassing the physical systems necessary to deliver digitally enabled critical infrastructure on a global scale (IoT) and the widespread use of robotics and their ongoing impact on global systems and processes.
- **Biological and synthetic materials:** The design, synthesis and manipulation of materials at the atomic/molecular level to innovations at mesoscopic and macroscopic scales supporting bioengineering, chemical engineering, gene-level manipulation, additive manufacturing and AI-mediated generative design.

Just as the steam engine and the printing press galvanized the Industrial Revolution, so AI and robotics are now provoking a vast transformation in the nature of military technologies and the global balance of power. The rise of AI is not without historical precedent, but the changes accompanying AI suggest the need for national defence planning that is more precisely calibrated to a data-driven era.

Against the backdrop of great power rivalry and a multipolar system, AI has emerged as a particular focus of competition. China, Russia, the United States and many other nations are aggressively pursuing AI capabilities with a significant focus on defence and security. China's government, for example, hopes to lead the world in AI by 2030 and expects to widen its lead in the industrialization of AI by leveraging the country's massive abundance of data (Lucas and Feng 2017).

In fact, data and data-driven technologies now occupy the commanding heights of the global economy. Competition across a global data economy has become inextricably linked to great power rivalry (Mearsheimer 2021). Notwithstanding the fact that the US and Chinese economies are deeply interdependent, China's expanding investments across Eurasia will soon make it the centre of world trade.

Technological advantage remains a key pillar of NATO countries but China is quickly catching up. Even as the United States has established a strong lead in AI discovery, it is increasingly likely that China will dominate the industrialization of AI-driven applications. Not only does China have advanced commercial capabilities, but it also has a coherent national strategy. China's technology sector is reaching a critical mass of expertise, talent and capital that is realigning the commanding heights of the global economy (Lucas and Waters 2018) (see Figure 1).

Much of the technological innovation deployed by Chinese industries has been "incremental" rather than "disruptive" but this is now changing. Gathering emerging markets in its orbit, China's unprecedented economic expansion now exerts a gravitational pull on the world economy (*The Economist* 2018). President Xi Jinping's signature project, the multi-trillion-dollar Belt and Road Initiative (The World Bank 2018) offers a global platform for a broad strategic shift around electric vehicles,

telecommunications, robotics, semiconductors, rail infrastructure, maritime engineering and, ultimately, AI (McBride and Chatzky 2019).

Not surprisingly, China is already the world leader in international patent applications with broad ambitions to become an innovation superpower (World Intellectual Property Organization 2020). As autonomous machines (Etzioni and Etzioni 2017), renewable energy infrastructure,[1] quantum communication (Šiljak 2020), augmented brain-machine interfaces (Putze et al. 2020) and space-based weapons (Etherington 2020) come to the fore, pressure is growing to rethink the nature of Canadian national security and, in particular, Canadian national defence. Given the accelerating pace of technological innovation and the rise of Asia as the centre of world trade (Huiyao 2019), the impact of technologies from abroad could be substantial.

AI and Military Defence

Defining AI

The concept of AI has been much discussed, but the precise definition of the term remains a moving target. Rather than a specific technology or a particular innovation, AI is more akin to a collection of materials. In truth, AI remains an aspirational goal even as AI technologies have become the basis for a wide range of mainstream commercial applications, including web search, medical diagnosis, algorithmic trading, factory automation, ridesharing and autonomous vehicles.

Notwithstanding the fact that the field of AI research began in the 1940s, the explosion of interest in AI has gathered pace over the past decade as improvements to machine learning and computer processing power have converged. Ongoing advancements in AI are analogized with the multi-scale learning and reasoning abilities found in the human brain. When combined with big data and cloud computing, AI is predicted to "cognitize" digital technologies by connecting "smart" AI and machine-learning systems to a vast universe of networked devices across fifth-generation (5G) telecommunications networks (i.e., the IoT).

As a subset of AI, machine learning represents the most prominent application of AI (see Figure 2). Machine learning uses statistical techniques to enable machines to "learn" without explicit instruction, driving many applications and services that improve automation across a range of analytical and physical tasks. Automatically improving performance through the use of data, this process is known as "training" a "model." Using an algorithm to improve performance on a specific task, machine-learning systems analyze large training data sets in order to do what comes naturally to human beings: learn by example.

The most common application of machine learning today is deep learning. As part of the broader family of machine learning, deep learning leverages layers of artificial neural networks to replicate human intelligence. Deep-learning architectures such as deep neural networks, recurrent neural networks and convolutional neural networks support a wide array of research fields, including computer vision, speech recognition, machine translation, natural language processing and drug design.

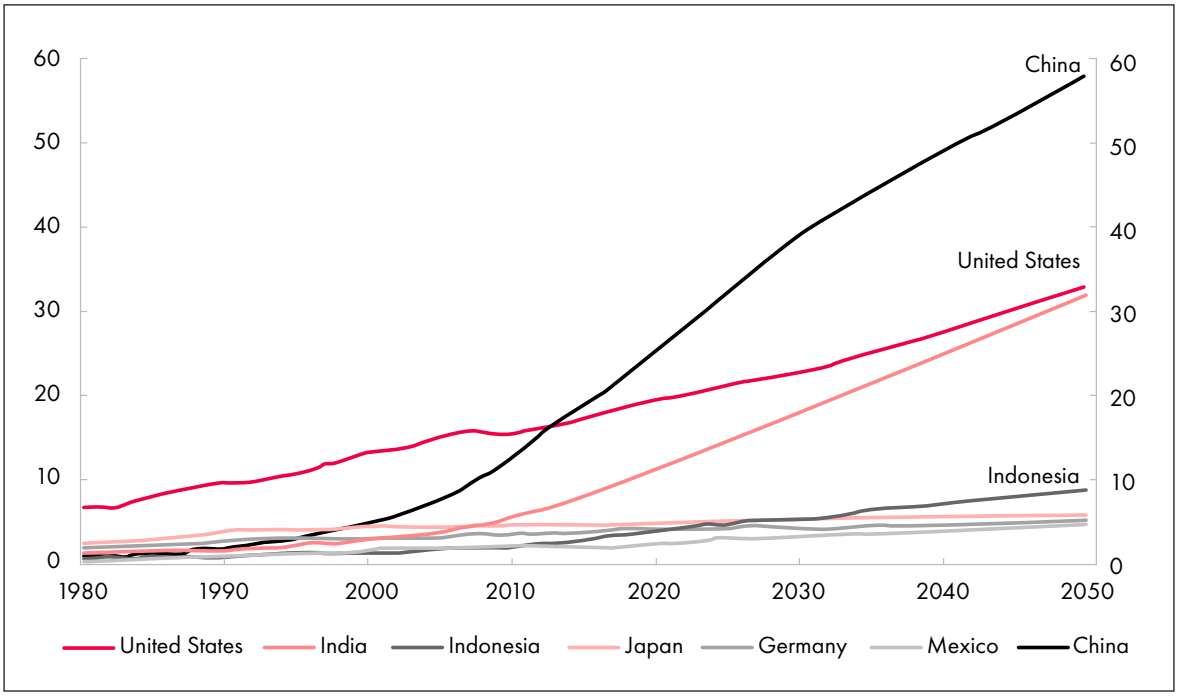
Canadian National Defence: Applying AI to National Security

AI sits at the centre of a constellation of EDT that includes robotics, genomics, battery storage, blockchain, 3D printing, quantum computing and 5G telecommunications. At the research level, the United States remains the global leader in AI. The National Science Foundation currently invests more than US$100 million each year in AI research (National Science Foundation 2018). The Defense Advanced Research Projects Agency (DARPA) recently announced a US$2 billion investment in an initiative called AI Next, whose goal is advancing contextual and adaptive reasoning (DARPA 2018).

Unlike past technological development in atomic weapons or stealth aircraft, no country will have a monopoly on military AI. Extensive global cooperation among researchers and leading commercial enterprises means that advancements in AI and machine learning are likely to diffuse globally. In fact, most technological progress in the development of AI is driven by industry rather than government. Alongside market-dominant technology companies, a wide range of network clusters around the world are incubating

1 See www.blackrock.com/institutions/en-us/strategies/alternatives/real-assets/infrastructure/global-renewable-power.

Figure 1: Projected GDP in Purchasing Power Parity (in trillions of US dollars)



Source: https://en.wikipedia.org/wiki/Asian_Century.

a new generation of commercial innovation (Li and Pauwels 2018). As a result, many future military applications will likely be adaptations of technologies developed for commercial industry.

Fortunately, Canada has been a leader at the forefront of AI research and continues to nurture a strong AI ecosystem through several programs under the Pan-Canadian AI Strategy introduced in 2017.[2] The Canadian government is active in the Advisory Council on AI[3] and various international partnerships including the Global Partnership on AI, launched in 2020;[4] the AI Partnership for Defense, whose second dialogue took place in 2021;[5] and multilateral agreements overlapping AI-driven security and planning (the Five Eyes, NATO). Indeed, Canada's national defence policy, "Strong, Secure, Engaged" (SSE), reflects the Government of Canada's commitment to growing annual defence spending with a critical focus on technology.

The current federal budget includes a substantial commitment to AI development, with $443.8 million promised over 10 years (Silcoff 2021). From the government's 2021 budget, $185 million will support the commercialization of AI research; $162.2 million will go toward recruiting top academic talent across the country; $48 million will be for the Canadian Institute for Advanced Research; $40 million over five years will aim to bolster computing capacity for researchers at national AI institutes in Edmonton, Toronto and Montreal; and $8.6 million over five years will help advance the development and adoption of standards related to AI (Government of Canada 2021, 148).

Augmenting Canadian Intelligence

AI is a fuzzy area affecting a broad range of commercial and military technologies. Like electricity or fossil fuels, the widespread application of AI means that AI and other general-use technologies have a capacity to reconfigure the pace and organization of modern militaries (Bresnahan and Trajtenberg 1995). Taken as a whole, AI represents a structural transformation in the nature of national security. For this reason, SSE envisions

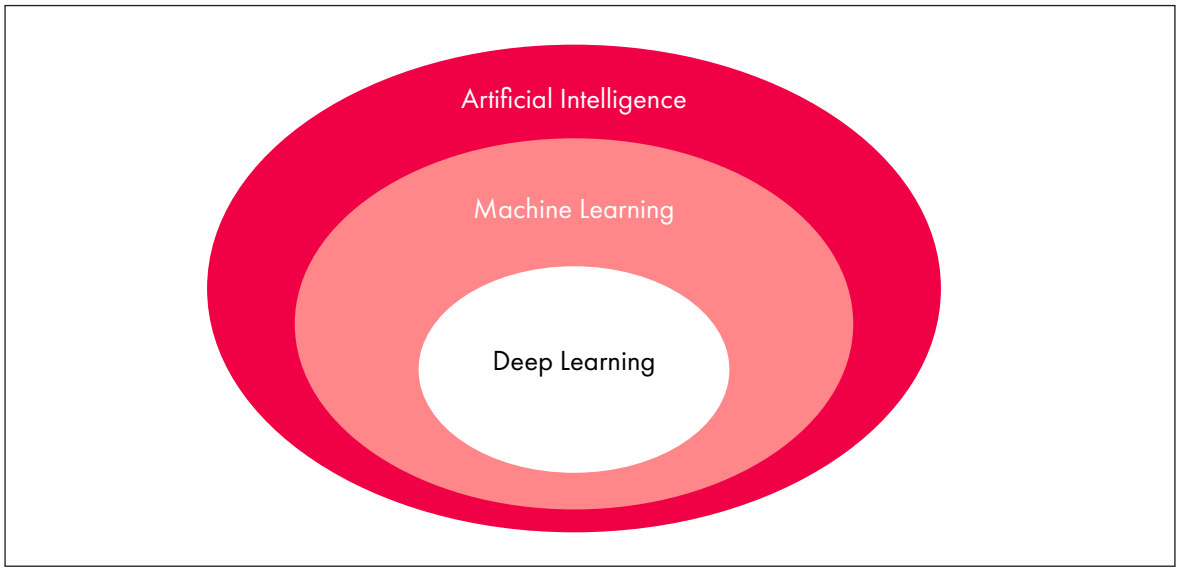
2 See https://cifar.ca/ai/.

3 See https://ised-isde.canada.ca/site/advisory-council-artificial-intelligence/en.

4 See https://gpai.ai/.

5 See www.ai.mil/news_01_27_21-dod_joint_ai_center_facilitates_second_international_ai_dialogue_for_defense.html.

Figure 2: The Layers of AI



Source: Authors.

a future military posture with a greater focus on developing, acquiring and integrating advanced and transformative technologies, including cyber networks and autonomous systems.

Even as Canada's continued role in traditional alliances (NORAD, NATO and the Five Eyes community) remains the basis for national security, EDT is fundamentally changing the nature of conflict. As Greg Fyffe (2021) observes, the rise of AI as a tool of war overlaps a growing need to upgrade Canada's national security architecture, particularly Canadian intelligence. Compounding cycles of technological change and the explosion of information, new skill sets and new strategies for analyzing data are becoming critical to the evolution of national defence planning.

In the digital age, war is increasingly becoming knowledge based. As conflict moves into the information arena, military planning is beginning to refocus on information/disinformation operations, cyber operations, intelligence operations and political or economic influence operations. In fact, this hybrid warfare has a long history as a tool of war with the goal of using propaganda, sabotage, deception and other non-kinetic military operations to undermine adversaries from within (Bilal 2021).

Cyber continues to be a key target for potential adversaries, state proxies, criminal organizations and non-state actors alike. This includes embedded surveillance and reconnaissance of communications, intelligence and sensitive information. As Amy Zegart (2021) explains, technology is democratizing the nature of intelligence by dramatically expanding access to data and information. Indeed, the majority of information driving strategic intelligence today is actually open source intelligence (OSINT) or in the public domain.

Modern militaries are becoming critically dependent on secure, timely and accurate data. As data expands exponentially, digesting it becomes impossible. This data explosion is driving the need for new modes of analysis and new kinds of cyber tools. In the digital age, security and intelligence personnel require new platforms, new tools and new OSINT agencies that work across domains. AI can be particularly helpful in this regard.

As data grows in importance, so does adversarial competition across a vast digital landscape. AI and machine learning can vastly improve Canada's national intelligence capabilities by sifting through enormous troves of data. AI is not a silver bullet. AI systems cannot generate meaning or provide causal analysis. However, AI and machine learning can dramatically augment human intelligence capabilities in managing data and data-driven analytics.

Augmenting the CAF

AI is expected to change the established paradigm of military conflict as decision makers adjust their security posture for a data-driven world. One of the key challenges confronting DND/CAF is the speed at which data-driven networks reshape command-and-control systems (Thatcher 2020). The advantage of centralized systems is their efficiency in coordinating human activity. In command systems, personnel and sensors drive threat detection, moving information up the decision stack so that decision makers may properly respond. Digital technologies profoundly accelerate this process.

Applications of AI to the military domain could prove challenging to conventional command-and-control systems. In the United States, for example, the Pentagon's first chief software officer recently resigned in protest at the slow pace of technological transformation. In an interview after leaving his post at the Department of Defense, Nicolas Chaillan told the *Financial Times* that the failure of the United States to respond to technological change and other threats had put the country's future at risk (Manson 2021).

In addition to the slow pace of change, the centralized nature of military command-and-control systems means that single points of failure provide vulnerable points of attack. Command authorities and automated or human controllers are often prone to adversarial techniques that leverage bad or deceptive information, even as top-down decision-making can be slow to adapt to complex emergent challenges.

New innovations in neuromorphic computing, generative adversarial networks (GANs), AI decision support, data analytics and intelligence analysis could have enormous impact in augmenting the structure and processes of military operations. Rapid advancements in machine-learning algorithms have already sparked a wave of investment across commercial and military sectors.[6] Integrated across a variety of platforms, technologies and applications, AI and machine learning could prove critical to augmenting DND/CAF for a digital era.

Moving beyond a conventional focus on attrition and kinetic attack to new methods based on accelerating speed and adaptation, data-driven technologies may be key to fomenting a radical shift in the nature of national security. AI is not a single technology. Rather, it is a class of technologies that can be integrated across a range of military and commercial applications. Underlying the ongoing evolution of these technologies is data.

Digital technologies are now fuelled by data and will continue to drive the creation of ever-more data-driven technologies — especially AI. Data is the basis for training AI and advanced machine-learning algorithms. As both the "operational exhaust" generated by digital systems running at scale and a process by which machines respond to data inputs, data now drives machine "autonomy."

Data-driven technologies underpin core social and economic functions of modern societies overlapping infrastructure, energy, health care, finance, trade, transportation and defence. With the global rollout of 5G networks, it is anticipated that there will be an explosion of data created, collected, processed and stored across highly robust global information networks. According to the market research firm IDC, global data is now growing at an annual rate of 61 percent (Patrizio 2018). Data is expected to reach 175 zettabytes by 2025 (a trillion gigabytes), transforming the nature and scale of the digital economy (ibid.).

For this reason, it would be wise for DND/CAF to elevate data to the level of a national asset. This is critical to both economic growth and Canadian national defence. Protecting and harnessing data as a national asset will mean rethinking the large centralized digital infrastructure that now constitutes contemporary data architectures. To be sure, data security in the network era should be decentralized and federated in order to avoid the vulnerabilities of centralized systems.

Weaponizing AI: Lethal Autonomous Systems

Conventional forecasts on technological disruption often make the mistake of assuming that system changes of this magnitude simply

6 The goal of general AI or "strong AI" is to enable a machine to apply knowledge and skills across different contexts without the need of human intervention. This more closely mirrors human intelligence by providing opportunities for autonomous learning and problem solving across a broad range of tasks. However, experts broadly agree that it will be many decades before the field advances to develop general AI.

replace old technologies on a one-to-one basis. In reality, disruptions on this scale tend to disproportionately replace old systems with dramatically new architectures, boundaries and capabilities (Arbib and Seba 2020).

The ongoing weaponization of AI is fuelling a global arms race that promises to reshape the contours of Canadian defence strategy. In fact, many states around the world are already far advanced in automating personnel systems, equipment maintenance, surveillance systems, and the deployment of drones and robotics (Stanley Center for Peace and Security, United Nations Office of Disarmament Affairs and the Stimson Center 2019). From the United States to Russia to Israel to China, military researchers are embedding AI into cybersecurity initiatives and robotic systems that support remote surgery, combat simulations and data processing.

The application of AI to military operations in the form of advanced logistics, semi-autonomous convoys, smart supply-chain management and predictive maintenance systems represents near-term applications of AI (Perry 2021). However, the evolution of autonomous weapons that can target individuals across land, sea, air, space and cyber domains (with or without the need for human intervention) represents the likely future of military conflict (see Figure 3). In fact, close to 100 militaries currently have some level of armed or unarmed drone capability (Gettinger 2019).

The expansion of commercial drone technologies criss-crossing mining, agriculture and energy is fuelling a broad proliferation of drone technologies. As the recent conflict between Armenia and Azerbaijan demonstrates, a swarm of relatively cheap autonomous and semi-autonomous drones can be leveraged to overwhelm conventional military systems, rendering a range of contemporary platforms obsolete (Shaikh and Rumbaugh 2020). Lightweight, reusable armed drones such as China's Blowfish A3 (Xuanzun 2019) and Turkey's Songar (Uyanık 2021) can be equipped with a range of payloads including mortars, grenades and light machine guns. Recent attacks on Saudi Arabia's Abqaiq oil processing facility (Rapier 2019) and the Russian airbase in Khmeimim (Hambling 2018) reflect the growing application of military drones to varied battlefield environments.

Defined as weapons that can select and engage targets without human authorization, lethal autonomous weapons systems (LAWS) are designed to loiter in designated areas of operations for long periods before independently identifying a target. Multiple drones or robots can function in parallel to overcome an opponent's defences or destroy a specific target. Developers tend to sort LAWS into three broad categories relative to the observe, orient, decide and act (OODA) loop[7] (see Figure 4). These categories include: "humans-in-the-loop," "humans-on-the-loop" and "humans-out-of-the-loop." This distinction is also framed as "semi-autonomous," "supervised autonomous" and "fully autonomous" technological systems. Unfortunately, the distinction between LAWS that are supervised and LAWS that are fully autonomous can be little more than a software patch or a regulatory procedure.

As LAWS and other data-driven technologies become cheaper and more widespread, they will likely provide a broad range of state and non-state actors with platforms and tools to leverage AI and machine learning in new and disruptive ways. In addition to tightening the OODA loop, military personnel will need to understand the ramifications of AI in accelerating the OODA loop in order to determine which mode is most appropriate in given situations.

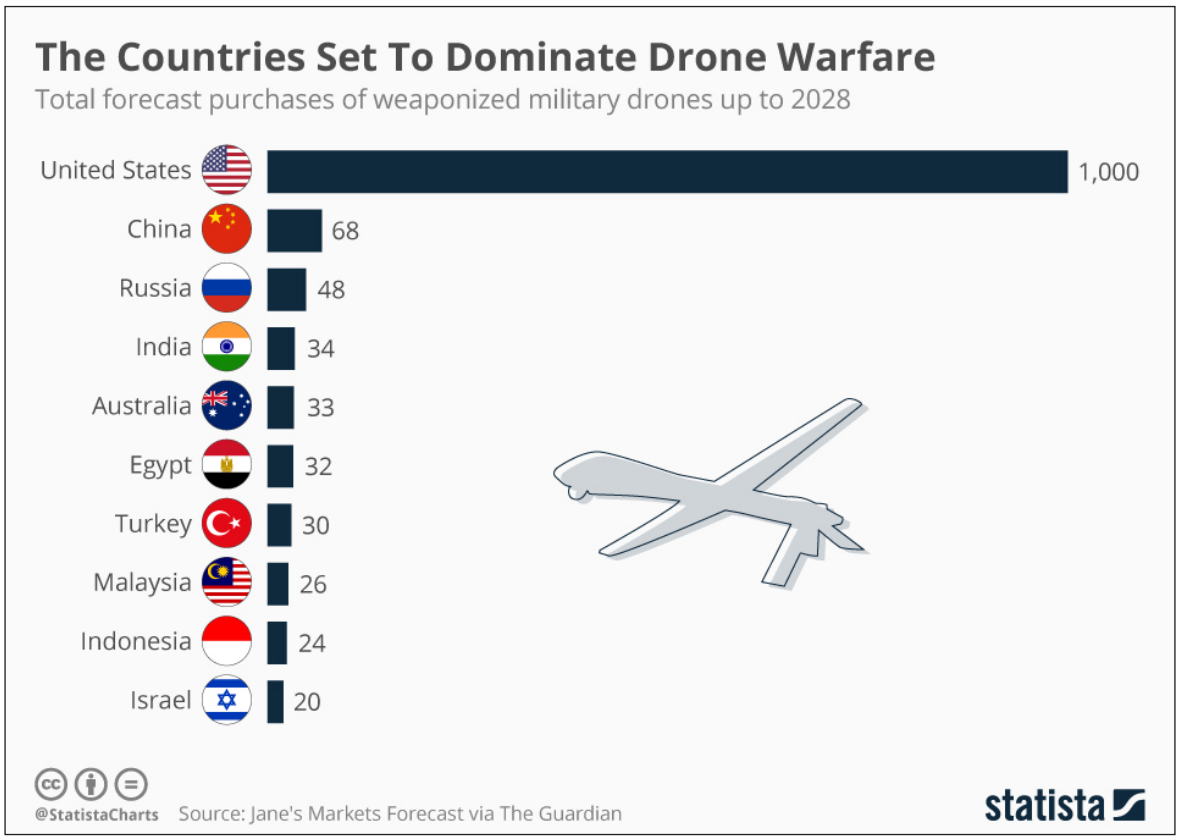
Network Platforms

Given the scope and scale of EDT, it would be wrong to assume that we can simply maintain systems and practices inherited from a previous century. As a 2018 report by Britain's Chatham House has warned, US, British and other nuclear weapons systems are becoming increasingly vulnerable to cyberattacks (Unal and Lewis 2018). These concerns are well founded. Together, AI and the proliferation of EDT will almost certainly advantage small states and non-state actors by capitalizing on the scaling effects of AI and autonomous systems.

For many NATO countries, networked platforms have become critical to multi-domain operations — sea, air, land, cyber and space. Enterprise-scale networks make it possible to visualize and coordinate vast resources across complex environments. Building on 5G telecommunications and cloud computing, information systems can now efficiently collect, transmit and

7 The objective of the OODA loop is to "get inside the enemy's decision cycle" and eliminate enemy combatants before they can complete their own OODA loop.

Figure 3: Global Drone Proliferation



Source: www.statista.com/chart/20005/total-forecast-purchases-of-weaponized-military-drones/.

process massive amounts of battlefield data, providing real-time data analysis.

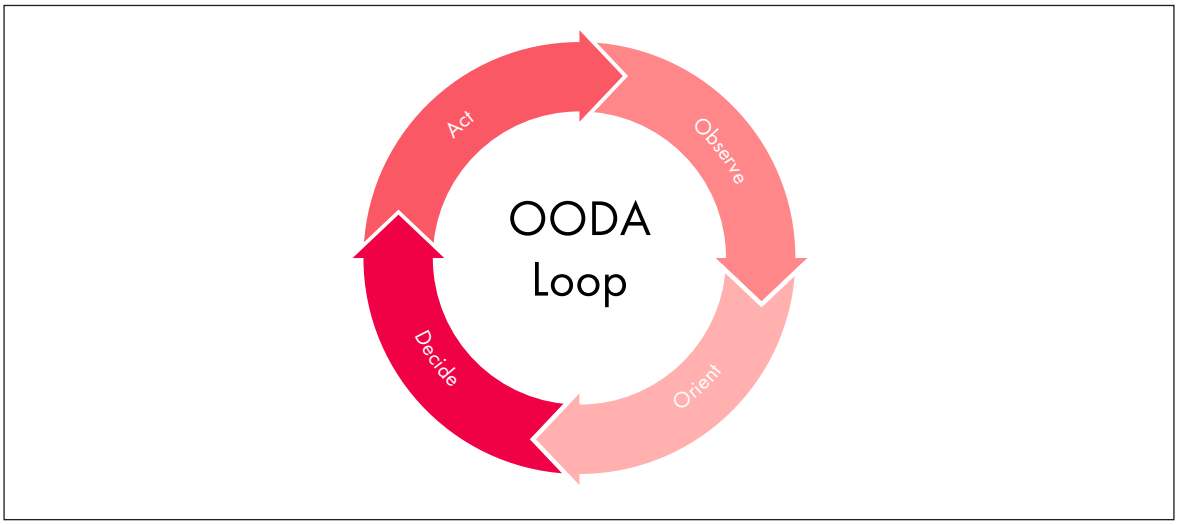
Connected devices are becoming critical to coordinating air strikes, piloting drones, digesting real-time video of the battle space and managing highly complex supply chains. In Britain, the Defence Data Framework provides a structure to address the challenges in aligning military organizations with the needs of a data-driven enterprise (Ministry of Defence 2021). From strategy to communications to logistics to intelligence, digital platforms are now fundamental to orchestrating complex military operations. Data is now the lifeblood of all operational domains.

In a digitized battlespace, every soldier, platform and resource is now a node within a complex military network. Beginning with network-centric US military operations in the 1990s, digital technologies have become the basis for advanced weapons, tactics and strategy. From battlefield situational awareness and autonomous drones to precision-guided munitions and machine-driven psychological operations, cyber is moving war into the network era.

Where centralized institutions were critical to the industrial era, platforms and networks are becoming critical to the digital era. AI is essentially a "bottom-up" technology that relies on the constant "feed" of massive amounts of data in support of machine learning as a "learning engine." As digital ecosystems proliferate, the network platforms and the data management systems they depend on become critical to managing an expanding range of resources and personnel.

Like the financial sector, DND should look to DLTs such as blockchain to accelerate the Canadian military's digital transformation. By distributing data laterally across decentralized networks, a CAF blockchain could help reduce the limitations and vulnerabilities inherent to bureaucratized systems. DLTs provide a highly decentralized validation system that can ensure all communication and data transfer are protected from adversaries while eliminating the potential failure of centralized nodes.

Figure 4: The OODA Loop



Source: Boyd (1976).

Drone Swarms and Robotics

The application of AI to military planning is advancing quickly, with many states already far advanced in the deployment of drones and robotics. Indeed, the global proliferation of drone technologies is well under way.

Militaries around the world are developing or procuring attack drones at an accelerating pace (see Figure 5). Together, Russia's Lightning (BulgarianMilitary.com 2021), Spain's Rapaz,[8] and various drone projects across Britain,[9] the United States[10] and Israel[11] represent the early stages of a new era in military technologies. Unlike industrial-era military technologies, drones can be acquired at low cost and require relatively little technical skill.[12]

Drone swarm technology involves groups of micro/mini drones/unmanned aerial vehicles, or UAVs, leveraging autonomous decision making based on shared information. In fact, contemporary military drones can already be designed to locate, identify and attack targets without a human in/on the loop. Using swarm techniques, hundreds of unarmed drones can collect information from the field while guiding thousands more with various weapons (i.e., firearms, artillery and/or munitions).

As the short video "Slaughterbots"[13] dramatizes, fully autonomous weapons will make it significantly easier and cheaper to target and kill unique individuals. Building on facial recognition and decision-making algorithms, LAWS are becoming widely available to state and non-state actors alike. Thousands of relatively inexpensive drones armed with explosive warheads could potentially overwhelm air defences to attack infrastructure, cities, military bases and so forth.

Mosaic Warfare

The threat of drone swarms overwhelming Canadian military installations alongside cyberattacks on critical infrastructure or hypersonic missiles that automatically launch when satellite sensors detect threats represent a disturbing but increasingly likely future. Emerging from complexity science and research on insects, the use of drones to

8 See https://scrdrones.com/en/success-stories/rapaz-project/.

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

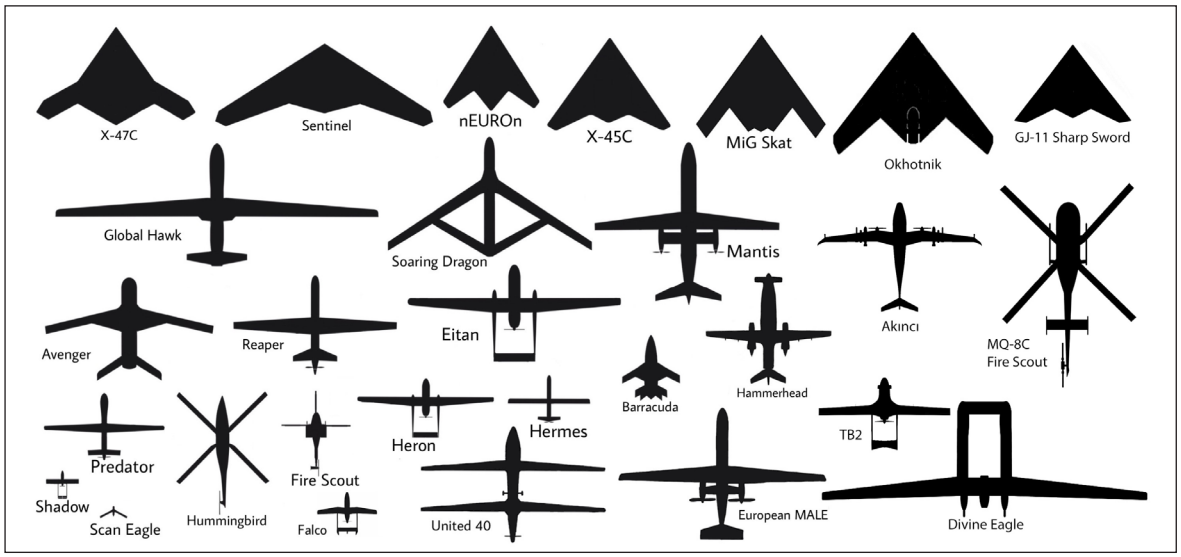
10 See https://dod.defense.gov/UAS/.

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

12 See www.newamerica.org/international-security/reports/world-drones/introduction-how-we-became-a-world-of-drones/.

13 "Slaughterbots" was produced in 2017 by the Future of Life Institute, promoting arms control. The video presents a dramatized near-future scenario where swarms of inexpensive microdrones use AI and facial recognition to assassinate political opponents based on preprogrammed criteria.

Figure 5: UAV Comparison



Source: https://commons.wikimedia.org/wiki/File:UAV_Comparison.jpg.

support "swarm intelligence"[14] represents a new toolset for accelerating the tempo of war.

In response to this changing environment, DARPA has developed the concept of Mosaic Warfare. The central idea behind Mosaic Warfare is that modular systems can be cheap, flexible and highly scalable tools for responding to highly networked environments. Like the ceramic tiles in mosaics, individual warfighting platforms can be designed to be highly configurable. Formations leverage decentralized agents reconfigured across a "kill web." The goal of kill webs is to avoid the structural rigidity of "monolithic systems."

Unlike the complex chess moves required in conventional warfighting, Mosaic Warfare leverages digital networks to accelerate dynamic response time using modular flexibility and augmented decision making (time compression). Like complex systems in nature, kill webs use algorithms to eliminate single points of failure, accelerating response time through a modular design.

Moving away from dominance (forecasting) and toward accelerating reaction (adaptation), Mosaic Warfare is designed to support hybrid military units that leverage lateral networks up and down a "decision-making stack." Together, AI, drones, sensors, data and personnel are combined to support operational commanders on the ground, making intelligence, resources and logistics assets available to small formations at an accelerated pace.

Modular systems such as Mosaic Warfare suggest that the future of warfare will increasingly leverage the computing, data analytics and algorithms that now drive wargaming and simulations. Driving highly fluid, gamified and unpredictable environments, future AI systems could accelerate war to a pace and tempo that becomes extremely computationally intensive as the range of outcomes expands.

DARPA's recent AlphaDogfight (2019–2020) provides a window into this new reality. Using a sophisticated F-16 flight simulator to pit computers against an experienced human pilot, trials were designed to advance AI developers for DARPA's Air Combat Evolution program.[15] Not surprisingly, the F-16 AI agent defeated a human pilot five games to zero through aggressive and precise manoeuvres that the human pilot simply could not match.

14 True swarm behaviour is self-organizing and emergent: a simple set of rules followed by independent agents generates "collective intelligence." This behaviour, seen in the murmuration of starlings, enables a kind of collective intelligence from the simple behaviour of local agents. Working as a "hive mind," individual agents can be networked together in support of "stigmergic" improvement.

15 See www.darpa.mil/program/air-combat-evolution.

Adversarial Attacks

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

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

Attacking the Data

Attackers may seek to modify training data or testing data. This is accomplished by creating adversarial examples that are intentionally "perturbed" or altered and provided to a model, which causes error. For example, by just changing the resolution of the image of a washing machine, researchers were able to trick a model into classifying the machine as a "safe" or a "loudspeaker" (Kurakin, Goodfellow and Bengio 2017). To the human eye, the adversarial images look nearly identical.

In the national security context, an adversary might try to use the same technique to suggest a weapon system is really a community centre. If this occurs in isolation, the problem can likely be identified and addressed. If adversarial examples are used at scale over time, this could become a significant challenge and impact trust in intelligence collection systems.

Additionally, some adversaries might not be precise — or have the skill to be — and could attempt to force a model to misclassify an entire class rather than a specific class. As we increasingly rely on computer imagery in the national security environment and are not always able to verify in real-time or in contested spaces, the risk of miscalculation during this kind of attack is significant.

High-consequence AI systems are not the only targets for adversarial attacks. AI systems affected by adversarial examples can include biometric recognition in which fake biometric traits can be exploited to impersonate legitimate users, speech recognition in which an attacker adds low-magnitude noise to confuse the system (Zelasko et al. 2021) and computer security (including obfuscating malware code within network packets).

As DND/CAF seeks to improve efficiencies through the deployment of AI systems — such as voice assistants on warships (McLeod 2019) — the risk of adversarial use must be assessed and countermeasures developed before deployment.

Attacking the Model

In addition to altering inputs, another attack method can be used to reverse-engineer models to access training data (Heaven 2021). Because machine-learning models perform better against training data than new inputs, adversaries can recognize differences in a target model's predictions and match against known data including personally identifiable information (Shokri et al. 2017). With machine-learning-as-a-service becoming increasingly available — and, in many cases, used as a base to develop more sophisticated capabilities — DND will need to carefully review the risk of data leakage from national security systems. This applies to even seemingly innocuous systems such as voice assistants.

Examples of weaknesses in AI systems are extensive (Hadfield-Menell et al. 2017). These include a vacuum cleaner that ejects collected dust back onto a space it just cleaned so that it can collect even more dust or a racing boat in a digital game looping in place to collect points instead of pursuing the main purpose of winning the race. While these examples are not life threatening, the same technique — known as reward hacking (when a model is instructed to maximize its objective function but does so in a way that is unintended) — can be used to far more serious effect.

The transition from machine learning designed to solve "single-step decision-making problems" with fixed training data to deep machine learning solving "sequential decision-making problems"

and much broader data sets will make adversarial attacks even harder to detect. This threat is so significant that the US Intelligence Advanced Research Projects Activity is funding a project to detect trojan AI attacks on a completed system.[16] The concern is that governments could unknowingly operate an AI system that produces "correct" behaviour until a scenario presents in which a "trigger" is present. During deployment, for example, an adversary could attack a system and only cause a catastrophic failure to occur at a much later time. These kinds of attacks could impact image, text, audio and game-playing AI systems.

Defence and Countermeasures

Just as adversarial examples can be used to fool AI systems, they can be included in the training process to make them more robust against attacks. By training the most important national security AI systems on clean and adversarial data — either by labelling them that way or by instructing a model to separate them out — greater defence is possible. But sophisticated adversaries could likely evade this defence method on its own, and a defence in depth will be necessary using additional tactics.

GANs have a wide variety of use cases from creating deepfakes to cancer prognosis (Kim, Oh and Ahn 2018). They may also be used to defend against adversarial attacks (Short, Le Pay and Ghandi 2019), using a generator to create adversarial examples and a discriminator to determine if it is real or fake. An added benefit is that using GANs as a defence may also actually improve the original model's performance by normalizing data and preventing "overfitting" (IBM Cloud Education 2021).

Benchmarking adversarial attacks and defence models — such as the use of GANs — is a comprehensive countermeasure against which AI systems can be compared. This method provides a quantitative measure for developing and meeting security standards and allows for assessment of capabilities and limits of AI systems. As part of this testing and evaluation process, game theory may be useful in modelling behaviour of adversaries in order to identify possible defence strategies.

As AI systems cannot be "patched" in the traditional information security sense, the risk of adversarial attack against national security AI systems should be meticulously analyzed before deployment and regularly reviewed. Additionally, trained models — especially those on classified data and with the most sensitive application — should be carefully protected

16 See www.iarpa.gov/index.php/research-programs/trojai.

Global Governance on AI

The speed and scope of data-driven warfare suggest that we are entering a new era in which the potential for LAWS — with or without humans in the loop — could dramatically alter the global balance of power. From killer drones and human-machine teaming to augmented military decision making (Slayer 2020), AI technologies will force-multiply the capacity of the world's militaries to project power. The ongoing weaponization of AI also overlaps the weaponization of space (*The Economist* 2019) as low-Earth orbit (LEO) increasingly becomes an operating environment for military surveillance, remote sensing,[17] communications, data processing (Turner 2021) and ballistic weapons (Sevastopulo and Hille 2021).[18]

The rise of AI in conjunction with LEO and LAWS represents a critical turning point in the nature of global security. For this reason, academic researchers, technology entrepreneurs and citizens around the world have raised concerns about the dangers associated with militarizing AI. As they rightly point out, the lack of international consensus on the norms and laws regulating the responsible development and use of AI risks future crises.

Laws of War

Beyond the exaggerations of AI we often see in science fiction, it is important to establish the appropriate checks and balances for limiting the concentration of power that AI technologies could provide. Common international rules and

17 See https://earthdata.nasa.gov/learn/backgrounders/remote-sensing.

18 In 2019, the United States introduced Space Force (see www.airforce.com/spaceforce), a new branch of the US military, with the purpose of securing US interests in space. Alongside the United States, Russia, the European Union, India, Japan and China are all investing in advanced space programs with military applications. In 2007, China successfully tested a ballistic missile-launched anti-satellite weapon; while, more recently, India shot down a satellite in LEO using an anti-satellite weapon during an operation code-named Mission Shakti (Still, Ledur and Levine 2019).

regulations on managing AI and other digital technologies will shape the contours of war and conflict over the coming decades. Developing guardrails in the evolution of military AI will be critical to reducing the potential for future conflict.

Active engagement by Canada and other NATO countries in this discussion could be key to the future of global peace and security. The laws of war regulating the use of AI both in terms of the conditions for initiating wars (*jus ad bellum*) and the conduct of AI in war (*jus in bello*) remain to be determined. Given the expanding rivalry between the United States and China, the need for treaties governing the use of LAWS and their proliferation could not be more timely.

As NATO observes, Canada and its allies should seek to promote, participate in and establish collaborative opportunities that support a broad, comprehensive architecture for the development and application of AI and other EDT (NATO Advisory Group on Emerging and Disruptive Technologies 2020). Notwithstanding the daunting challenges ahead, global governance has an important role to play in regulating military AI. Despite divergent views on AI and its weaponization, past negotiations can serve as a basis for future treaties, particularly in defining the rules of war. This includes treaties on conventional weapons, nuclear arms control, biological and chemical weapons, landmines, outer space and civilian protection (see Figure 6).[19]

Thus far, the United Nations Convention on Certain Conventional Weapons (CCW) has overseen a process to discuss options for addressing the humanitarian and international security challenges posed by autonomous weapons.[20] A range of potential options for the regulation of LAWS has been introduced, including an international treaty under CCW, a non-binding code of conduct declaring states' commitment to the responsible development and use of LAWS. Outside the United Nations, the Stop Killer Robots campaign was launched in 2013 with the goal of banning LAWS altogether.[21]

UN Secretary-General António Guterres has highlighted the risks and opportunities of AI and other digital technologies (United Nations 2020) and has called for a ban on LAWS (Guterres 2021). Unfortunately, the views of UN member states and, in particular, the UN Security Council diverge, with some states viewing regulation as the exclusive purview of nation-states and others focusing on a more multisectoral approach. In addition to the weaponization of AI, broad differences exist with regard to issues around human rights, algorithmic bias, surveillance (both public and private) and state-sponsored or state-enabled cyberattacks.

For the major military powers of the world, a lack of mutual trust remains a substantial hurdle to pursuing collective arms control agreements on AI. Even as a significant number of countries support the provision of new legally binding treaties that would ban the development and use of LAWS, most of the world's major military powers see significant value in weaponizing AI. Given these divides, multilateral governance on LAWS will require confidence-building measures as a means to open politically deadlocked arms control processes.

Toward Mundane Regulation

Perhaps the most challenging aspect of developing policy and regulatory regimes for governing AI is the difficulty in pinpointing exactly what these regimes are supposed to regulate. Unlike biological and chemical weapons, AI is mostly software. Indeed, AI is a moving target: what was defined as AI 40 years ago is simply conventional software today.

AI is a fuzzy technological area affecting a broad range of commercial and military applications. Machine-learning algorithms, for example, serve as ingredients in search engines (algorithmic ranking), military drones (robotics and decision making) and cybersecurity software (algorithmic optimization). But they also underwrite mundane industries and even children's toys (semantic analysis, visual analysis and robotics), financial software and social media networks (trend analysis and predictive analytics).

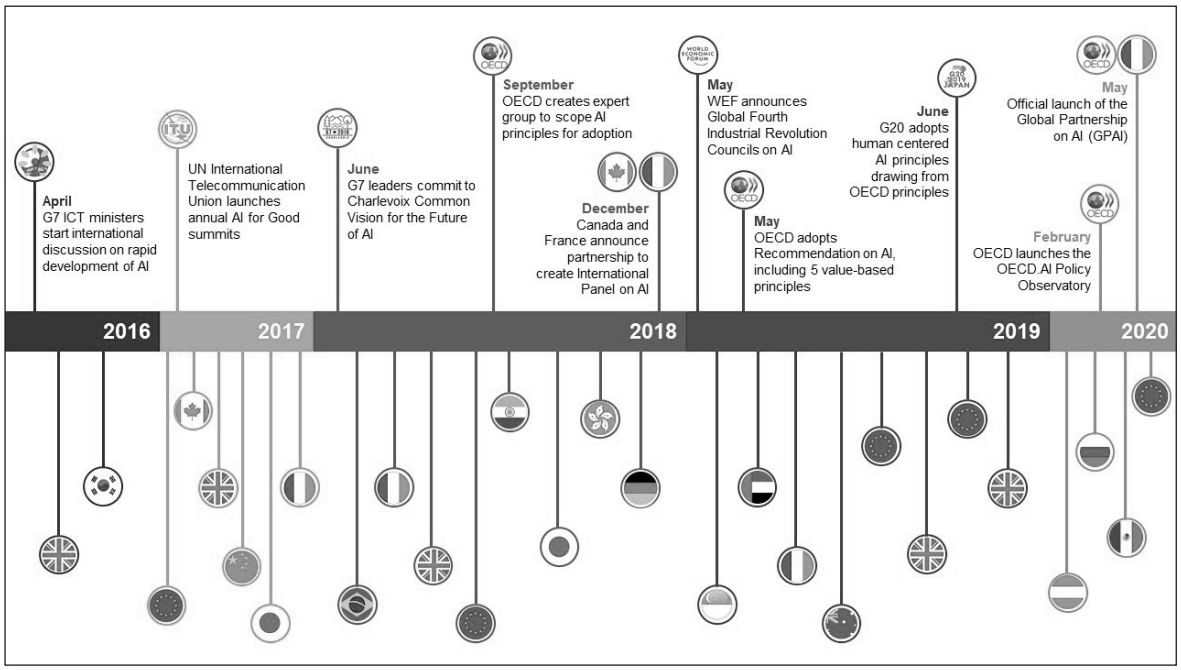
Much like the products and processes falling within these mundane regulatory domains, AI technologies are designed not as final entities, but as ingredients or components to be used within a wide range of products, services and systems. A "killer robot," for example, is not

19 See www.armscontrol.org/treaties.

20 See www.un.org/disarmament/the-convention-on-certain-conventional-weapons/.

21 See www.stopkillerrobots.org/.

Figure 6: Global Governance on AI



Source: Giardino (2020).

the outcome of a specific kind of technology. Rather, it is the outcome of the recombination of AI "ingredients," many of which are also used to detect cancers or increase driver safety.

While the temptation is to use an exclusive non-proliferation lens to regulate AI, the dual-use challenge remains. Unlike nuclear proliferation or genetically modified pathogens, AI is not a specific technology. Rather, it is more akin to a collection of materials or software ingredients. Instead of the mostly binary nuclear non-proliferation lens, inspiration for a more relevant (albeit less exciting) model of regulation can be found in food regulation, specifically, food safety and material standards (Araya and Nieto-Gómez 2020).

Governing AI

Given the significant conceptual and political hurdles in pursuing blanket regulation on AI, governance remains a daunting challenge. On the one hand, if we understand AI as a series of technological practices that replicate human activities, then there is simply no single field to regulate. Instead, AI governance overlaps almost every kind of product or service that uses computation to perform a task. On the other hand, if we understand AI as the basis for dramatically altering the balance of power among peoples and nations, then we have significant challenges ahead.

Fortunately, this is not the first time that nation-states have been confronted with new technologies impacting global security. In the aftermath of the Second World War, the world's most powerful countries — the United States, the United Kingdom, the Soviet Union, China, France, Germany and Japan — oversaw global governance on nuclear weapons, chemical agents and biological warfare. Then, as now, the world must act collectively to govern AI.

Like the Cold War, confidence-building measures including regular dialogue, scientific cooperation and shared scholarship could help in reducing geopolitical tensions. The development of a common vocabulary for managing the risks posed by military AI could provide the basis for more robust multilateral treaties on AI over time.

In this regard, the Organisation for Economic Co-operation and Development (OECD) has published its Recommendation on AI as a set of intergovernmental standards, launching the AI Policy Observatory in February 2020. Together, the Canadian and French governments are also leading a Global Partnership on Artificial Intelligence (GPAI) in conjunction with the OECD, which aims to be an

international forum for AI policy.[22] Members of GPAI are focused on the responsible development of AI grounded in "principles of human rights, inclusion, diversity, innovation and economic growth."[23]

In addition to GPAI, several European countries have called for EU members to begin a strategic process on the responsible use of new technologies — in particular AI.[24] The United States has invited allies to discuss the ethical use of AI (JAIC Public Affairs 2020). NATO has initiated a process to encourage member states to agree on a series of ethical principles and an agenda for international arms control in key areas of EDT with military application (Christie 2020; NATO 2020). Acknowledging the profound impact of EDT on global security, NATO launched the EDT road map in December 2019 (NATO Science & Technology Organization 2020).

Taken as a whole, the very real potential of a twenty-first-century cold war between the United States and China signals the need for formal oversight in negotiating a normative path toward multilateral governance. Over the long term, this will likely include the pursuit of treaties on AI that mirror the ban on biological weapons, chemical weapons and anti-personnel landmines. However, given the pace of innovation in AI and the growing divide between the world's superpowers, the window of opportunity for negotiating global governance on AI may be closing.

Conclusion: Toward a National System of Innovation

Even as the industrial era winds down, technological innovation is speeding up (Araya 2020). Since its inception some 80 years ago, AI has evolved from an arcane academic field into a powerful driver of social and economic transformation. The integration of AI in warfighting has been described by some Chinese military analysts as an evolving "battlefield singularity" (Kania 2017). Building on notions of a "technological singularity" (Schulze-Makuch 2020), speculation is growing that AI and robotics will outstrip the capacities of human beings to effectively respond to algorithm-driven warfare.

The evolution of AI and other EDT is bringing together advanced data, algorithms and computing power to "cognify" military technologies. In this new environment, modern militaries are becoming critically dependent on networks that provision secure, timely and accurate data. Data has become the "operational exhaust" of digital systems and the feedstock for driving "intelligent machines." As data grows in importance, so does adversarial competition across a vast digital landscape. Indeed, the real value of data is found in its quantity and quality for driving innovation.

As NATO's annual report on EDT (NATO Advisory Group on Emerging and Disruptive Technologies 2020) makes clear, keeping pace with technological change necessitates agility and rapid iteration with respect to the development, experimentation and application of technology. The capacity for innovation across the CAF must be part of a wider innovation ecosystem that effectively integrates research and implementation across a public-private ecosystem. This includes clear objectives for harnessing dual-use GPT in partnership with Canadian industry in order to capitalize on already-existing technology.

This kind of multi-domain collaboration has historically been defined in terms of a national system of innovation (NSI) (OECD 1997). In fact, NSI policy and planning can take many forms, ranging from loose coordination to highly integrated partnerships. The varied NSI planning models applied in the United States (Atkinson 2020), China (Song 2013) and Europe (Wirkierman, Ciarli and Savona 2018) demonstrate the substantial economic and social return to be found in maximizing government-industry-research partnerships. Government should work to build out Canadian technological capacity through tax incentives, procurement and research funding, and strategic planning. But it cannot act alone.

National innovation necessarily depends on institutional actors collaborating across a shared ecosystem. For this reason, a coordinated Canadian NSI will require reciprocal flows of technology

22 See https://gpai.ai/.

23 See https://gpai.ai/about/.

24 See https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

and information among people and institutions in driving long-term innovation. Given that so much innovation in EDT is industry-led, advancing public-private partnerships is critical to the evolution of the Canadian military. For DND/CAF to advance a military tailored to the digital age, government, industry and academia will need to collaborate in a more integrated fashion.

Building a robust Canadian innovation ecosystem will mean much more extensive public-private collaboration and the continuous reskilling, training and incubation of knowledge and resources. Notwithstanding the human capital investments required to develop cutting-edge AI, most AI applications can now be obtained via open-source licensing even as core learning algorithms are available on public platforms and across academic ecosystems. The impact of this "open everything" environment represents a substantial challenge to closed hierarchies and ponderous bureaucracies.

Government processes and planning will need to adapt to accelerated innovation life cycles in order to match EDT's aggressive cycles of obsolescence. Alongside the enormous asymmetrical security risks associated with network technologies, the move to a data-driven military will require a substantial focus on data security and data governance. Unlike the substantial costs and planning needed to carry out conventional interstate conflict, the devastating impact of cyberattacks can be launched against critical infrastructure by small groups with little more than a personal computer. Given the proliferating challenges ahead, changes in the design of large bureaucracies (corporate, government, academic and military) are inevitable.

Alongside the need for new and different knowledge, resources and expertise, the Canadian government and the CAF will need to balance a capacity for hard power with the needs of a changing geopolitical landscape. Beyond the era of US predominance, the twenty-first century is now being shaped by a multipolar system characterized by techno-nationalism and a post-Bretton Woods order. In the face of a rapidly evolving digital era, international cooperation will be critical to ensuring peace and security. Information sharing, expert conferences and multilateral dialogue can help the world's nation-states and their militaries develop a better understanding of one another's capabilities and intentions. As a global middle power, Canada could be a major partner in driving this effort.

Works Cited

Araya, Daniel. 2020. "Is America's Fossil Fuel Empire Collapsing?" *Forbes*, January 28. www.forbes.com/sites/danielaraya/2020/01/28/is-americas-fossil-fuel-empire-collapsing/?sh=6a41db572c57.

Araya, Daniel and Rodrigo Nieto-Gómez. 2020. "Renewing Multilateral Governance in the Age of AI." In *Modern Conflict and Artificial Intelligence*, 6–12. Waterloo, ON: CIGI. www.cigionline.org/publications/modern-conflict-and-artificial-intelligence/.

Arbib, James and Tony Seba. 2020. *Rethinking Humanity: Five Foundational Sector Disruptions, the Lifecycle of Civilizations, and the Coming Age of Freedom*. RethinkX, June. https://static1.squarespace.com/static/585c3439be65942f022bbf9b/t/5f436dfe85783706be4a315a/1598254621881/RethinkX+Humanity+Report.pdf.

Atkinson, Robert D. 2020. "Understanding the U.S. National Innovation System, 2020." Information Technology & Innovation Foundation. November 2. https://itif.org/publications/2020/11/02/understanding-us-national-innovation-system-2020.

Bilal, Arsalan. 2021. "Hybrid Warfare — New Threats, Complexity, and 'Trust' as the Antidote." *NATO Review*, November 30. www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

Boyd, John R. 1976. "Destruction and Creation." US Army Command and General Staff College, September 3. https://upload.wikimedia.org/wikipedia/commons/a/a6/Destruction_%26_Creation.pdf.

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

BulgarianMilitary.com. 2021. "'Lightning' — the new Russian military supersonic drone." March 1. https://bulgarianmilitary.com/2021/03/01/lightning-the-new-russian-military-supersonic-drone/.

Christie, Edward Hunter. 2020. "Artificial Intelligence at NATO: dynamic adoption, responsible use." *NATO Review*, November 24. www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html.

DARPA. 2018. "DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies." September 7. www.darpa.mil/news-events/2018-09-07.

Etherington, Darrell. 2020. "More evidence of increasing militarization of space as US claims Russia satellite weapon test." TechCrunch, July 23. https://techcrunch.com/2020/07/23/more-evidence-of-increasing-militarization-of-space-as-u-s-claims-russia-satellite-weapon-test/.

Etzioni, Amitai and Oren Etzioni. 2017. "Pros and Cons of Autonomous Weapons Systems." *Military Review* (May-June). www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/.

Fyffe, Greg. 2021. *Prepared: Canadian Intelligence for the Dangerous Decades.* Reimagining a Canadian National Security Strategy Report No. 6. Waterloo, ON: CIGI. www.cigionline.org/publications/prepared-canadian-intelligence-for-the-dangerous-decades/.

Gettinger, Dan. 2019. *The Drone Handbook.* The Center for the Study of the Drone at Bard College. https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf.

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

Government of Canada. 2021. *A Recovery Plan for Jobs, Growth, and Resilience.* www.budget.gc.ca/2021/home-accueil-en.html.

Guterres, António. 2021. "Secretary-General's remarks to Member States on Priorities for 2021." January 28. www.un.org/sg/en/content/sg/statement/2021-01-28/secretary-generals-remarks-member-states-priorities-for-2021-bilingual-delivered-scroll-down-for-all-english-version.

Hadfield-Menell, Dylan, Smitha Milli, Pieter Abbeel, Stuart Russell and Anca D. Dragan. 2017. "Inverse Reward Design." Conference Paper, 31st Conference on Neural Information Processing Systems. https://people.eecs.berkeley.edu/~russell/papers/nips17-ird.pdf.

Hambling, David. 2018. "A swarm of home-made drones has bombed a Russian airbase." *New Scientist*, January 10. www.newscientist.com/article/2158289-a-swarm-of-home-made-drones-has-bombed-a-russian-airbase/.

Heaven, Will Douglas. 2021. "AI fake-face generators can be rewound to reveal the real faces they trained on." *MIT Technology Review*, October 12. www.technologyreview.com/2021/10/12/1036844/ai-gan-fake-faces-data-privacy-security-leak/.

Huiyao, Wang. 2019. "In 2020, Asian economies will become larger than the rest of the world combined — here's how." World Economic Forum, July 25. www.weforum.org/agenda/2019/07/the-dawn-of-the-asian-century/.

IBM Cloud Education. 2021. "Overfitting." March 3. www.ibm.com/cloud/learn/overfitting.

JAIC Public Affairs. 2020. "JAIC facilitates first-ever International AI Dialogue for Defense." September 16. https://www.ai.mil/news_09_16_20-jaic_facilitates_first-ever_international_ai_dialogue_for_defense_.html.

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

Kim, Minseon, Ilhwan Oh and Jaegyoon Ahn. 2018. "An Improved Method for Prediction of Cancer Prognosis by Network Learning." *Genes* 9 (10). doi:10.3390/genes9100478.

Kurakin, Alexey, Ian J. Goodfellow and Samy Bengio. 2017. "Adversarial Examples in the Physical World." Workshop paper, February 11. https://arxiv.org/pdf/1607.02533.pdf.

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

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

Lucas, Louise and Richard Waters. 2018. "China and US compete to dominate big data." *Financial Times*, May 1. www.ft.com/content/e33a6994-447e-11e8-93cf-67ac3a6482fd.

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

McBride, James and Andrew Chatzky. 2019. "Is 'Made in China 2025' a Threat to Global Trade?" Backgrounder. May 13. Council on Foreign Relations. www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

McLeod, James. 2019. "Canada's navy is developing an AI voice assistant for warships, but don't worry: It won't control the weapons." *Financial Post*, May 1. https://financialpost.com/technology/canadas-navy-is-developing-an-ai-voice-assistant-for-warships-but-dont-worry-it-wont-control-the-weapons.

Mearsheimer, John J. 2021. "The Inevitable Rivalry: America, China, and the Tragedy of Great-Power Politics." *Foreign Affairs*, November/December. www.foreignaffairs.com/articles/china/2021-10-19/inevitable-rivalry-cold-war#author-info.

Ministry of Defence. 2021. *Data Strategy for Defence*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020553/Data_Strategy_for_Defence.pdf.

National Science Foundation. 2018. "Statement on Artificial Intelligence for American Industry." May 10. www.nsf.gov/news/news_summ.jsp?cntn_id=245418.

NATO. 2020. *NATO 2030: United for a New Era*. November 25. www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

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

NATO Science & Technology Organization. 2020. *Science & Technology Trends 2020–2040: Exploring the S&T Edge*. www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

OECD. 1997. *National Innovation Systems*. Paris, France: OECD.

Patrizio, Andy. 2018. "IDC: Expect 175 zettabytes of data worldwide by 2025." Network World, December 3. www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html.

Perry, Bradley. 2021. "Autonomous Convoys." JCSP 47 Service Paper. Canadian Forces College. www.cfc.forces.gc.ca/259/290/23/192/Perry.pdf.

Putze, Felix, Athanasios Vourvopoulos, Anatole Lécuyer, Dean Krusienski, Sergi Bermúdez i Badia, Timothy Mullen and Christian Herff. 2020. "Editorial: Brain-Computer Interfaces and Augmented/Virtual Reality." *Frontiers in Human Neuroscience*, May 12. www.frontiersin.org/articles/10.3389/fnhum.2020.00144/full.

Rapier, Robert. 2019. "Why the Attacks In Saudi Arabia Are A Really Big Deal." *Forbes*, September 16. www.forbes.com/sites/rrapier/2019/09/16/why-the-attacks-in-saudi-arabia-are-a-really-big-deal/?sh=1f301d7dde1a.

Schulze-Makuch, Dirk. 2020. "Reaching the Singularity May be Humanity's Greatest and Last Accomplishment." *Smithsonian Magazine*, March 27. www.smithsonianmag.com/air-space-magazine/reaching-singularity-may-be-humanitys-greatest-and-last-accomplishment-180974528/.

Sevastopulo, Demetri and Kathrin Hille. 2021. "China tests new space capability with hypersonic missile." *Financial Times*, October 16. www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb.

Shaikh, Shaan and Wes Rumbaugh. 2020. "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense." Center for Strategic and International Studies. December 8. www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

Shokri, Reza, Marco Stronati, Congzheng Song and Vitaly Shmatikov. 2017. "Membership Inference Attacks Against Machine Learning Models." Conference Paper, IEEE Symposium on Security and Privacy. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7958568.

Short, Austin, Trevor Le Pay and Apurva Ghandi. 2019. "Defending Against Adversarial Examples." Sandia National Laboratories Report. September. www.osti.gov/servlets/purl/1569514.

Silcoff, Sean. 2021. "Federal budget promises more funding for innovative technologies, including artificial intelligence, genomics research and quantum computing." *The Globe and Mail*, April 20. www.theglobeandmail.com/business/article-budget-promises-more-funding-for-innovative-technologies-including/.

Šiljak, Harun. 2020. "China's quantum satellite enables first totally secure long-range messages." The Conversation, June 16. https://theconversation.com/chinas-quantum-satellite-enables-first-totally-secure-long-range-messages-140803.

Slayer, Kelley M. 2020. *Artificial Intelligence and National Security*. Congressional Research Service. https://sgp.fas.org/crs/natsec/R45178.pdf.

Song, Hefa. 2013. "China's National Innovation System." In *Encyclopedia of Creativity, Invention, Innovation and Entrepreneurship*, edited by E. G. Carayannis. New York, NY: Springer. doi:10.1007/978-1-4614-3858-8_497.

Stanley Center for Peace and Security, United Nations Office of Disarmament Affairs and the Stimson Center. 2019. *The Militarization of Artificial Intelligence*. August. New York, NY: United Nations. https://reliefweb.int/sites/reliefweb.int/files/resources/TheMilitarization-ArtificialIntelligence.pdf.

Still, Ashlyn, Júlia Ledur and Ally J. Levine 2019. "India shoots down own satellite." Reuters Graphics, March 27. https://graphics.reuters.com/INDIA-SATELLITE-WEAPON/0100918Q1RV/index.html.

Thatcher, Chris. 2020. "Artificial intelligence: Overcoming the barriers to adoption." *Canadian Army Today*, April 2. https://canadianarmytoday.com/artificial-intelligence-overcoming-the-barriers-to-adoption/.

The Economist. 2018. "The Chinese century is well under way." *The Economist,* October 27. www.economist.com/graphic-detail/2018/10/27/the-chinese-century-is-well-under-way.

———. 2019. "America's military relationship with China needs rules." *The Economist,* May 18. www.economist.com/special-report/2019/05/16/americas-military-relationship-with-china-needs-rules.

The World Bank. 2018. "Belt and Road Initiative." Brief. March 29. www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative.

Turner, Patrick. 2021. "Military Eyes AI, Cloud Computing in Space in a Decade." Defense One, January 27. www.defenseone.com/technology/2021/01/military-eyes-ai-cloud-computing-space-decade/171692/.

Unal, Beyza and Patricia Lewis. 2018. "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences." Chatham House Research Paper. January. www.chathamhouse.org/2018/01/cybersecurity-nuclear-weapons-systems/cyber-vulnerabilities.

United Nations. 2020. "Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation." Report of the Secretary-General. United Nations General Assembly, May 29. https://undocs.org/A/74/821.

Uyanık, Saffet. 2021. "SONGAR Armed Drone System Integrated into an Armored Vehicle for the First Time." Defence Turkey, January 16. www.defenceturkey.com/en/content/songar-armed-drone-system-integrated-into-an-armored-vehicle-for-the-first-time-4328.

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

World Intellectual Property Organization. 2020. *World Intellectual Property Indicators 2020.* Geneva, Switzerland: World Intellectual Property Organization. www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2020.pdf.

Xuanzun, Liu. 2019. "Chinese helicopter drones capable of intelligent swarm attacks." *Global Times,* May 9. www.globaltimes.cn/page/201905/1149168.shtml.

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

Żelasko, Piotr, Sonal Joshi, Yiwen Shao, Jesus Villalba, Jan Trmal, Najim Dehak and Sanjeev Khudanpur. 2021. "Adversarial Attacks and Defenses for Speech Recognition Systems." March 31. https://arxiv.org/pdf/2103.17122.pdf.

Centre for International
Governance Innovation

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

@cigionline