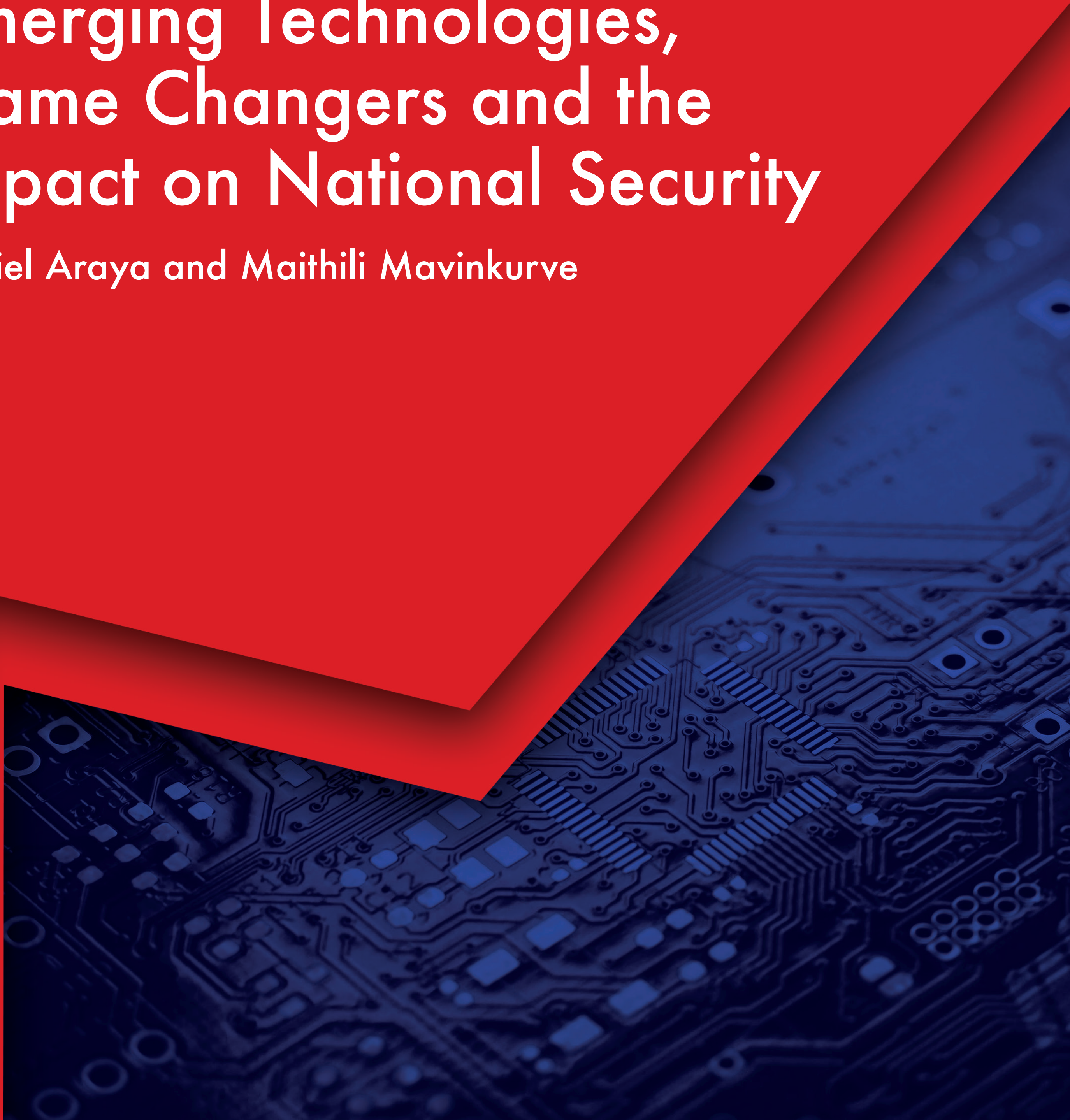
Centre for International
Governance Innovation

Reimagining a Canadian National Security Strategy | No. 9

Emerging Technologies, Game Changers and the Impact on National Security

Daniel Araya and Maithili Mavinkurve



Reimagining a Canadian National Security Strategy | No. 9

Emerging Technologies, Game Changers and the Impact on National Security

Daniel Araya and Maithili Mavinkurve

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
CIGI Senior Fellow and Project Co-Director Wesley Wark
Manager, Government Affairs and Partnerships Liliana Araujo
Publications Editor Susan Bubak
Publications Editor Lynn Schellenberg
Graphic Designer Sami Chouhdary

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

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

Centre for International Governance Innovation

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

Table of Contents

About the Project

Canada's approach to domestic and international security is at a profound moment of change. The shock wave of COVID-19 and its looming future effects highlight the urgent need for a new, coordinated and forward-looking Canadian national security strategy that identifies emerging and non-traditional threats and considers their interrelationships. Complex interactions between foreign policy, domestic innovation and intellectual property, data governance, cybersecurity and trade all have a significant impact on Canada's national security and intelligence activities.

Reimagining a Canadian National Security Strategy is an ambitious and unprecedented project undertaken by the Centre for International Governance Innovation (CIGI). It aims to generate new thinking on Canada's national security, inspire updated and innovative national security and intelligence practices, and identify ways that Canada can influence global policy and rulemaking to better protect future prosperity and enhance domestic security.

CIGI convened interdisciplinary working groups, which totalled more than 250 experts from government, industry, academia and civil society, to examine 10 thematic areas reflecting a new and broad definition of national security. Each thematic area was supported by senior officials from the Government of Canada, designated as "senior government liaisons." They provided input and ideas to the discussions of the working group and the drafting of thematic reports. Project advisers provided support and advice through specific lenses such as gender and human rights. This was critical to strengthening the project's commitment to human rights, equity, diversity and inclusion.

The project will publish 10 reports, authored independently by theme leaders chosen by the project's co-directors. The reports represent the views of their authors, are not designed as consensual documents and do not represent any official Government of Canada policy or position. The project was designed to provide latitude to the theme leaders to freely express new thinking about Canada's national security needs.

A special report by the project's co-directors, Aaron Shull and Wesley Wark, will analyze Canada's new national security outlook and propose a security strategy for 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.

Maithili (Mai) Mavinkurve is a CIGI senior fellow and the chief operating officer and a co-founder of Sightline Innovation, which created the world's first cloud-native data trust — a distributed artificial intelligence (AI) and data governance platform that enables control and sovereignty of data assets between trusted data partners.

Mai is an industry expert and adviser in applied AI and data governance. As a member of Innovation, Science and Economic Development Canada's Economic Strategy Table on digital industries, she led the subgroup that developed recommendations on national data strategy and intellectual property. She has also represented Canada at the Group of Seven ministerial meetings on AI and the future of work. Mai has advised on the Ontario Digital and Data Task Force, as well as co-chaired a data governance initiative with the Standards Council of Canada. Mai is an experienced engineer and executive leader with a focus on the practical enterprise applications and implications of AI and data. Mai was acknowledged as one of the 30 Most Influential Women in AI in Canada.

Acronyms and Abbreviations

5G	fifth generation
AEVs	autonomous and electric vehicles
AI	artificial intelligence
CADSI	Canadian Association of Defence and Security Industries
CARPA	Canada Advanced Research Projects Agency
CJEU	Court of Justice of the European Union
CTO	chief technology officer
DLTs	distributed ledger technologies
DND	Department of National Defence
EDTs	emerging and disruptive technologies
FPT	federal-provincial-territorial
GaaP	Government as a Platform
GDPR	General Data Protection Regulation
GPTs	general-purpose technologies
IDSA	International Data Spaces Association
IoT	Internet of Things
IP	intellectual property
ISED	Innovation, Science and Economic Development Canada
ML	machine learning
NATO	North Atlantic Treaty Organization
NSI	national system of innovation
PIPL	Personal Information Protection Law
WEF	World Economic Forum

Executive Summary

This report examines emerging and disruptive technologies (EDTs) and their impact on Canadian national security. These technologies include:

- artificial intelligence (AI) and machine learning (ML);
- data, computing and the Internet of Things (IoT);
- blockchain and distributed ledger technologies (DLTs);
- robotics and autonomous systems;
- quantum-enabled technologies;
- biotechnology and human enhancements;
- additive manufacturing;
- battery storage and renewables; and
- space-based applications.

The widespread application of EDTs to a vast array of industries and sectors defines many of these technologies as "general-purpose technologies" (GPTs) (Horowitz 2020). Broadly defined, GPTs are technologies with the capacity to reconfigure the shape and development of modern societies, dramatically altering their pace and structure. Historical examples of GPTs include the steam engine, the printing press, the railroad, electricity and the internal combustion engine (see Figure 1).

Much as mass electrification accelerated the rise of modern industrial societies in the twentieth century, so have technologies such as AI and ML begun transforming the contours of the global order (Araya and Nieto-Gómez 2020). Competition across a changing "geotechnological" landscape (Goodman and Khanna 2013) is inextricably linked to a rising great power rivalry between the United States and China. Areas of competition include cloud technologies, semiconductor chips, hypersonic and new missile technologies, space-based applications, quantum and biotechnologies, autonomous and electric vehicles (AEVs), battery storage and telecommunications.

Forecasting trends in this uncertain environment is daunting because timelines on various EDTs remain unclear. What is clear is that EDTs will confer transformational advantages to nations that incorporate these technologies into their security and intelligence organizations, military establishments and commercial industries. Over the coming decade, AI alone is expected to transform the nature of war, altering the speed and scope of military conflict. Indeed, the ongoing weaponization of AI and other frontier technologies is now fuelling a global arms race that promises to reshape the contours of Canadian national security strategy.

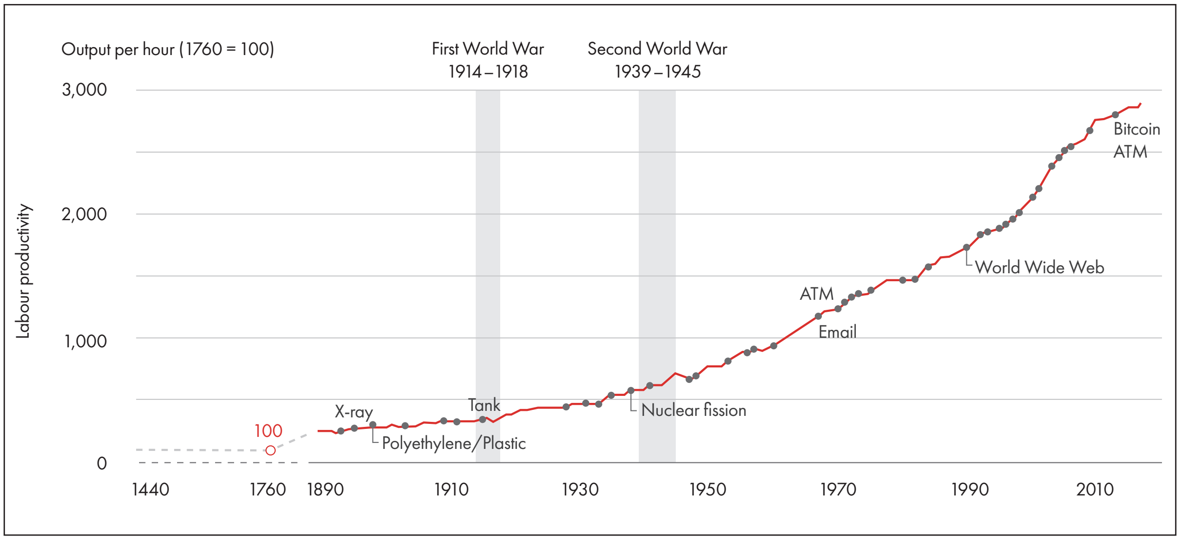
In fact, Canadian defence planning[1] has already begun incorporating many of these new technology platforms into Canada's national defence network (a "system of systems"). Together, remotely piloted drones, cyber technologies and space-based surveillance assets represent the emergence of a new generation of defence capabilities. In the decades ahead, spin-off technologies overlapping a global market in software and electronics will proliferate, resetting the conditions for interstate conflict (Roberts 2021).

Notwithstanding the fact that technological innovation has always shaped national security, the scale and velocity of contemporary technological change are unprecedented. Beyond an industrial era rooted in extractive production (coal, oil, livestock and scarce raw materials), we are now moving into a world that is highly dependent on systems of data-driven engineering and design. Together, protons, electrons, quantum bits, DNA and new materials have become basic building blocks in reshaping the fabric of industrialized societies (Schwab 2016).

Given the accelerating pace of innovation and the rise of Asia as the centre of global trade (Huiyao 2019), the impact of technologies from abroad could be substantial. Data-driven technologies are now so pervasive that they have become indispensable to modern transportation systems, water and power systems, electrical transmission grids, weapons systems, command-and-control systems and routine everyday communications (Adams 2016). In the decades ahead, frontier technologies including deep learning, quantum computing and genetic engineering will accelerate job losses (Lund et al. 2021), drive military transformation and introduce

[1] See www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html.

Figure 1: From the Printing Press to the Global Internet, Technology Has Evolved, and Human Societies with It



Source: Keller, Wieladek and Shelepko (2018).
Note: ATM = automated teller machine.

biotechnologies capable of fundamentally transforming our relationship to nature.

In the health-care sector, AI has already begun accelerating drug discovery and the development of new commercially viable biotechnologies.[2] Gene sequencing combined with AI represents a new era of genetic engineering that could alter existing organisms and synthesize entirely new organisms. In the banking and finance sectors, blockchain and DLT are beginning to transform asset management around distributed data networks (Ito, Narula and Ali 2017), while in the automotive and manufacturing sectors, AEVs are underwriting a long-term transformation of energy and mobility around zero-carbon “smart cities” (Conzade et al. 2021).

While Canadian planning has historically taken a “wait-and-see” approach, this may not be a strategic option. Revolutionary advancements in AI and other EDTs are now reshaping the global balance of power. Areas of discovery overlapping neuroscience, quantum computing and biotechnology are advancing quickly and represent uncharted territory in the evolution of “intelligence machines.” Indeed, prospects for developing fully autonomous weapons are no longer a matter of science fiction. Many nations around the world have already begun deploying automated personnel and equipment maintenance systems, autonomous surveillance and reconnaissance systems, and AI-powered drones and robotics (Congressional Research Service 2020).

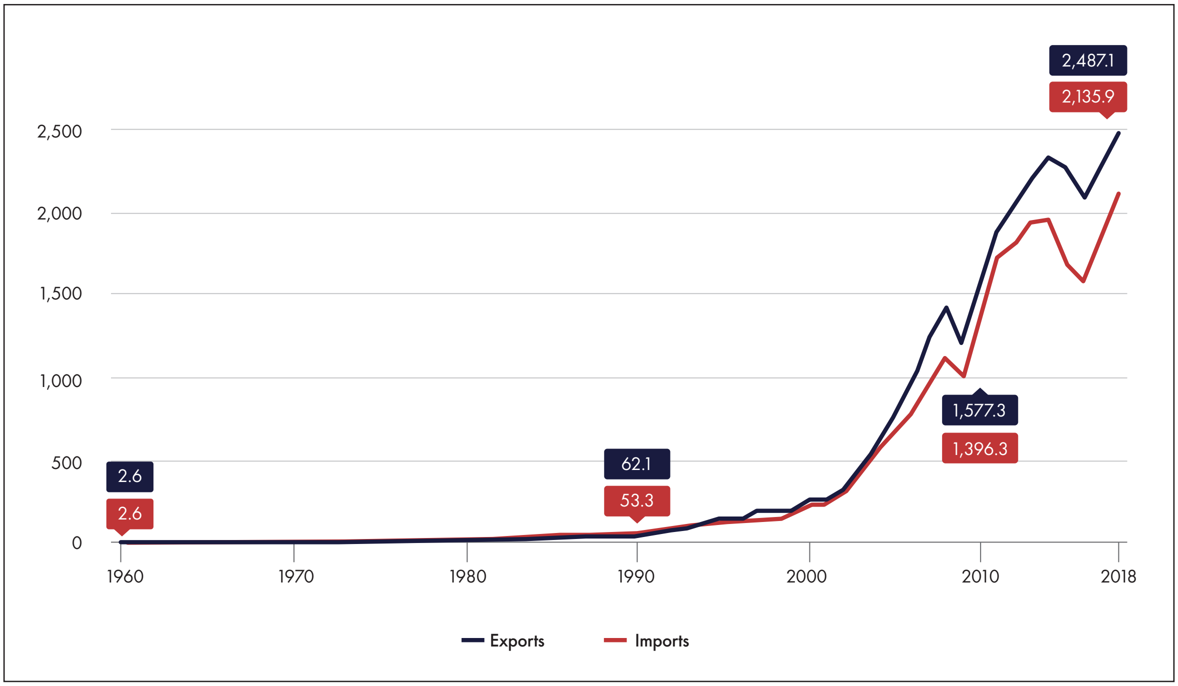
With the expanding economic heft of Asia and in particular China (see Figure 2), Canadian policy and planning will need to chart a pragmatic course. While this is a role familiar to Canadian policy makers, EDTs represent a unique challenge for national security because the bulk of research and development is happening in the commercial sector. For this reason, Canadian national security strategy will need to become better attuned to the needs of commercial industry. In this regard, the Liberal government’s recent proposal to establish a Canada Advanced Research Projects Agency (CARPA)[3] could be critical to advancing Canada’s frontier technologies for a new multipolar era.

While national security is often conflated with state security (i.e., protecting state institutions from threats foreign and domestic), this report argues that Canadian national security strategy should speak to a broad spectrum of concerns,

[2] In 2020, Massachusetts Institute of Technology researchers identified a powerful new antibiotic compound using an ML algorithm (Trafton 2020). This research was partially funded by the Canadian Institutes of Health Research, the Canadian Foundation for Innovation, the Canada Research Chairs Program and the Banting Postdoctoral Fellowships Program.

[3] See https://liberal.ca/our-platform/a-new-advanced-research-agency/.

Figure 2: China's Rise to Commercial Superpower (Annual Trade Values in US$ Billion)



Source: World Bank (cited in Buchholz 2019).

particularly core Canadian values applied to contemporary security challenges. Over the course of this decade, Canadian national security will face a unique geopolitical environment framed by great power competition, extreme climate events and accelerating technological disruption. In this report, the authors outline several policy proposals for managing Canadian national security strategy in this new era, looking specifically at the importance of data and data-driven technologies. These recommendations include:

- promoting the importance of data as a national asset;
- pursuing efforts to support both national and multilateral initiatives for data security and governance;
- supporting and promoting a sovereign Canadian cloud infrastructure and space-based internet;
- building a national data infrastructure; and
- establishing a cross-governmental unit to handle EDTs with an enhanced mandate for Canada's chief technology officer (CTO).

Introduction: Defining EDTs

The North Atlantic Treaty Organization and EDTs

What precisely is meant by EDTs in the context of Canadian national security strategy? While there are many definitions of EDT, for a technology to be classified as *emerging* and *disruptive*, it is generally characterized by rapid growth, radical novelty, wide-scale impact and a degree of ambiguity. North Atlantic Treaty Organization (NATO) Secretary General Jens Stoltenberg highlights five key areas in the development and adoption of EDT in the context of national security. These areas include:

- **AI and ML:** Their potential impact on innovation includes neuromorphic computing, generative adversarial neural networks and the capacity of AI to surface unexpected insights from data that has been, or has yet to be, gathered.
- **Quantum technologies**: These include 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:** This includes 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 in general.
- **Computing-enabled hardware:** This includes 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:** These include the design, synthesis and manipulation of materials at the atomic/molecular level for innovations at mesoscopic and macroscopic scales supporting bioengineering, chemical engineering, gene-level manipulation, additive manufacturing and AI-mediated generative design.

Data and National Security

As a 2021 publication by the United States' National Intelligence Council (2021) observes, technological breakthroughs in EDT now threaten to dissolve certain features of our national security architecture. Notwithstanding the fact that technological innovation has always shaped the nature of power, the scale and velocity of EDT and its impact on reshaping national security are unprecedented. Whether we focus on AI, DLTs, genetic engineering, space-based applications, quantum cryptography or IoT, data is now driving an extensive social, economic and cultural transformation.

Cascading global challenges ranging from migration and disease to climate change and technological disruption are buttressed by an expanding era of data networks and data-driven algorithms that are transforming traditional notions of power (political, economic and military). The rise of fifth-generation (5G) technology and cloud computing has amplified not only a range of security vulnerabilities overlapping technology proliferation, arms control and global governance, but also data privacy, social inequality and labour automation.

Taken as a whole, data-driven EDTs represent a rising security challenge impacting Canadian national security in unpredictable ways. These risks will grow in importance as a global market in digital technologies drives a tsunami of data connecting infrastructure, finance, communications and national defence to increasingly advanced AI systems. Underlying all of these challenges is the issue of data governance.

Data is now at the centre of the global economy. Indeed, the same data that unlocks the potential of ML is also transforming factory production, telecommunications, logistics, precision medicine, robotics and a myriad of other technologies that can be leveraged across sectors and industries. Moreover, intellectual property (IP) and the data it protects are now the world's most important commercial and national security assets. In 1976, 16 percent of the S&P 500 consisted of intangible assets (patents, trademarks and copyrights); today, those assets make up close to 90 percent (Asselin and Speer 2019, 25).

The capacity for data to reshape the national security landscape (Atlantic Council Geotech Center 2021) across increasingly contested commercial and military domains (air, land, maritime, cyber and space) is substantial. In its *National Cyber Threat Assessment 2018*, Canada's Communications Security Establishment observed that it is "now routinely blocking well over a billion malicious actions aimed every day at federal systems, databases and websites" and faces down "thousands of attempts to access and infiltrate government networks each day" (Canadian Centre for Cyber Security 2018). In fact, Canada's Department of National Defence (DND) networks have been attacked and compromised on several occasions (Waldie and Freeze 2020) over the past decade.

At the domestic level, data-driven social networks are catalyzing social and cultural fragmentation as concerns around social inequality and government capture erode the social contract. Growing pressure introduced by the platform economy is widening the gap between bureaucratic institutions and the digital services consumers now depend upon in the market. With the expanding influence of algorithms and the impact of disinformation in cyberspace, confidence in democratic societies and the rule of law has begun to wane. This portends greater social volatility across highly digitized societies alongside expanding demands for responsive government.

In addition to the risk of both intrastate and interstate conflict, we can also expect non-state actors to exploit Canadian data for financial and social gain. How Canadians use data and how the Canadian government safeguards that data will determine the ultimate success or failure of national security planning over the long term. Going forward, the most effective systems of governance in the digital era will likely be those that can build on political consensus and collective action in effectively resolving emerging social challenges. For a large federated society such as Canada, the challenges in achieving this consensus will be considerable.

Non-linear Dynamics

Conventional forecasts on technological change often make the common error of assuming that innovation simply replaces old technologies on a one-to-one basis. The reality is that GPTs tend to disproportionately replace old systems with dramatically new architectures, boundaries and capabilities. Much as the shift from wood to coal during the Industrial Revolution (Bazilian et al. 2019), the digital age represents a widespread economic and cultural transformation. This transformation may seem linear but reflects the non-linear[4] dynamics inherent in data-driven economies.

Across a disparate assortment of fields including computing, biology and machine automation, many of the challenges that we now face not only are facilitated by advances in EDT but also represent new risks in and of themselves. In fact, history is replete with examples of long periods of stability punctuated by abrupt technological and economic change. For the Austrian economist Joseph Schumpeter, this "creative destruction" (Schumpeter, quoted in Kopp 2021) reflects evolutionary cycles of social transformation within market economies.

What is clear is that the disruption of industry and the death of commercial giants punctuate an ongoing market restructuring that is driven by exponential feedback loops and accelerating innovation. As the death of Kodak, Motorola, Blockbuster, Sears, Circuit City and Compaq demonstrate, EDTs will continue to drive massive creative destruction. Indeed, even as economies of scale drive down the price of new technologies, increasing computing power, data storage and the expansion of the internet (Butler 2016) will drive up new capabilities, investment and market visibility and, ultimately, innovation itself.

Labour Automation

As old technologies give rise to new technologies, governments will be increasingly challenged by the pace of change over this decade (National Intelligence Council 2021). The impact of software and autonomous systems on industry remains difficult to predict, but the impact over the long term is certain: labour automation will displace routine work.

Research by PricewaterhouseCoopers LLP forecasts that as much as one-third of all jobs could be converted into software, robots and autonomous machines by the early 2030s (Hawksworth, Berriman and Goel 2018, 14). This includes a first wave of automation across data-driven sectors such as financial services, followed by a second wave impacting clerical support, decision making and robotics in semi-controlled environments. More conservatively, the World Economic Forum (WEF) (2020, 5) estimates that by 2025, 85 million jobs could be displaced and potentially replaced by 97 million new jobs across 26 countries.

The Rise of Fintech

Digital technologies have also begun disrupting global finance in the form of financial technologies (fintech). In the United States, the collective market value of fintech companies Square, Visa, PayPal and MasterCard is worth more than $1 trillion,[5] larger than that of even the "big six" banks (JPMorgan, Bank of America, Wells Fargo, Citigroup, Morgan Stanley and Goldman Sachs) (Delouya 2020). While in China, mobile payments in 2020 totalled an incredible 432 trillion yuan or $67 trillion (XinhuaNet 2021).

[4] See www.rethinkx.com/energy#energy-download.

[5] All dollar figures in US dollars unless otherwise noted.

Software and data have begun transforming the financial services and monetary sectors as cryptocurrencies and central bank digital currencies mark the arrival of new market actors, new industries and new regulatory challenges (Fay et al. 2021). Rather than relying on intermediaries such as banks and clearinghouses, the government and third-party institutions can make money transfers and payments directly. Fintech is also driving new channels for criminal activity by state and non-state actors alike. This includes the theft of IP and personal information, attacks on cyber infrastructure and a broad expansion of financial crimes across data-driven markets.

Autonomous Weapons

EDTs have also begun reshaping the contours of war, altering the speed, scope and automation of military technologies. Lethal autonomous weapon systems represent a new generation of technological weaponry with significant application to the battlefield. As the 2020 conflict between Armenia and Azerbaijan demonstrates (Shaikh and Rumbaugh 2020), 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.

The ongoing weaponization of AI also overlaps the weaponization of space (*The Economist* 2019) as low-Earth orbit increasingly becomes an operating base for military spacecraft and satellites for the purposes of surveillance, remote sensing,[6] communications, data processing (Tucker 2021) and ballistic weapons (Sevastopulo and Hille 2021). Russia, the European Union, India, Japan and China are all investing in advanced dual-use space programs. This integration of AI, space applications and robotics into warfighting is described by some Chinese military analysts as an evolving "battlefield singularity" (Kania 2017), that is, an environment in which machines largely displace human operators.

Canada in a Global Network Era

The challenges imposed by a new era of geotechnological rivalry mean rethinking Canadian national security. Unlike the case with past technological developments in atomic weapons or stealth aircraft, no country will have a monopoly in military AI. Most technological progress in the development of AI and other EDTs is driven by industry rather than by government. Alongside market-dominant technology companies, a wide range of network clusters around the world are incubating a new generation of commercial innovation (Li and Pauwels 2018).

Notwithstanding intense competition between states, it is important to recognize that extensive global cooperation among researchers and leading commercial enterprises means that advancements in AI and ML are likely to diffuse globally. As digitally networked technologies become cheaper and more widely available, they will diffuse to a broad range of actors, democratizing the capacity for both state and non-state actors to create and leverage force at scale. More problematically, it will mean the rise of asymmetrical security challenges.

Because they do not entail the substantial costs and planning needed to carry out conventional interstate conflict, cyberattacks can be launched against critical infrastructure by small groups of state and non-state actors alike with little more than personal computers, with devastating impact. The implications of this globally networked era are difficult to overstate. Networks are reshaping the means for both collaboration and competition as data scales laterally across digital platforms and open digital ecosystems.

The scope of this technological diffusion also means that the pace of innovation renders traditional policy and procurement cycles largely inadequate (Erwin 2021). In fact, we are living through a period of transition between two epochs: an industrial era characterized by vertically integrated bureaucracies, and a new computational era characterized by laterally networked platforms.

The move to decentralized networks means inevitable changes in the design of large bureaucracies (corporate, government, academic and military). Whereas centralized bureaucracies anchored human organization throughout the industrial era, the proliferation of algorithms and digital platforms are now becoming critical to managing resources and social interaction in the network era. In fact, this is the same logic driving the explosive evolution of the internet itself. In an era of highly scalable data-driven networks, centralized institutions of all kinds have now become extremely vulnerable to disruption.

[6] See https://earthdata.nasa.gov/learn/backgrounders/remote-sensing.

Government as a Platform

The use of digital platforms to deliver services at scale has become a common solution for breaking down organizational silos in digitizing commercial transactions. One obvious and compelling solution for evolving public services in the network era is the notion of “Government as a Platform” (GaaP). Originally coined by Tim O’Reilly (2010), the concept of GaaP is now a common reference point for reimagining government today.

In the United Kingdom, the Government Digital Service has used the term “government as a platform”[7] since 2015, while in Australia, the Digital Transformation Agency’s “whole-of-government” platforms strategy[8] was introduced in 2019 to support the country’s broader digitization efforts. Perhaps the most successful model of GaaP is Estonia’s X-Road platform,[9] launched in 2001. X-Road is now a global standard (Tambur 2021) in understanding the potential of GaaP and is often described as the future of digital democracies.

The concept of GaaP has had less impact in Canada but that may be changing. The Canadian Digital Exchange Platform (Treasury Board of Canada Secretariat 2019) could be the basis for developing a Canadian GaaP infrastructure. As Canada’s former chief information officer has warned (Benay 2019), the Canadian government needs to make much more progress on digitization. Indeed, much of this work simply involves reframing government platforms as core public infrastructure. Countries that invest in application programming interfaces, open data standards and modular software systems will have a huge opportunity to deliver government services at a much lower cost, while at the same time leveraging data for research and commercial purposes.

Data as the Basis for National Security

EDTs are ushering in a confluence of technological breakthroughs, from stacked neural nets that consume zettabytes of big data, to the application of massive cloud-computing infrastructure supporting smart mobile applications. Data is now the basis for training AI algorithms, which, in turn, drive advanced ML and autonomous systems. The current decade will be fuelled by data and will continue to drive the creation of ever-more data-driven technologies — especially AI. As AI is applied to augmented decision-support systems, the potential for serious and credible threats to Canadian national security will grow.

As a recent study from the Munk School of Global Affairs & Public Policy observes (White and Wolfe 2021), Canada faces multifaceted challenges overlapping EDTs, including software-driven automation and the transition to a carbon-neutral economy. In addition to defending Canada against foreign adversaries, Canadian national security strategy must also be calibrated to a data-driven economy.

The Need for Data Sovereignty

Given the fact that Canada’s digital infrastructure is almost exclusively owned by private firms, the threat of attacks in the cyber domain suggests the need for new security strategies. Data-driven EDTs will generate cascading ripple effects over the coming decade. With the rollout of 5G edge networks, it is anticipated that there will be an explosion of data created, collected, processed and stored. Measured in terms of bandwidth, cross-border data flows have already grown roughly 112 times between 2008 and 2020 (Slaughter and McCormick 2021).

While the world’s IoT infrastructure encompassed 10 billion devices in 2018, this global data ecosystem is projected to reach 64 billion devices by 2025 and possibly many trillions by 2040 (National Intelligence Council 2021, 2). The lack of oversight and accountability in how data is currently used, undermines public confidence in government. The Facebook-Cambridge Analytica scandal (Confessore 2018) highlights the abuse of power within commercial and political centres

[7] See https://gds.blog.gov.uk/category/government-as-a-platform/.

[8] See www.dta.gov.au/our-projects/digital-service-platforms-strategy.

[9] See https://e-estonia.com/solutions/interoperability-services/x-road/.

across the United States and around the world. The scandal showcased the importance of data in driving social change. Indeed, two aspects of data and data governance have become clear:

- The possession and control of data is leading to the accumulation of immense social, financial and geopolitical power. The misuse of this data poses a significant threat to public safety and to democratic society. In contrast, intelligent data governance could help drive mass economic security, democratic renewal and technological innovation.
- There are gaping holes in national, regional and international laws on data as well as regulations, norms and institutions around how data should be governed, collected, processed, monetized and used. Many of these holes are already being filled but much is left to be done.

In response to the challenges of data governance, many governments are now instituting virtual borders to control their data and protect "data sovereignty." The concept of data sovereignty or digital sovereignty refers to the idea that data is subject to the laws and governance structures within the nation in which it is collected.[10]

It is estimated that 92 percent of the Western world's data is stored in the United States (Propp 2019). Big tech companies such as Amazon, Google and Microsoft are now increasingly seen as enriching themselves at the expense of personal privacy. This includes personal data criss-crossing health care, finance, communications and entertainment.

To illustrate the dangers of data "hoarding," we need only consider the fact that US companies (as per the US Foreign Intelligence Surveillance Act[11] and the US Clarifying Lawful Overseas Use of Data Act[12]) can be compelled to hand over Canadian data to the US government without notifying Canadian authorities. These kinds of digital vulnerabilities represent substantial holes within the contemporary design of Canada's data infrastructure.

Resiliency and scalability of data systems are critical to any Canadian national security. Canada's national security strategy must safeguard data sovereignty while supporting the evolution of Canada's technology market. In response to the need for data governance, the Canadian government has embarked on a transformation plan to become a digital government. In fact, the Canadian government has clearly stated that "as long as a CSP [cloud service provider] that operates in Canada is subject to the laws of a foreign country, *Canada will not have full sovereignty over its data*. This is because there remains a risk that data stored in the cloud could be accessed by another country. The issue of data sovereignty is complex and continuously evolving as foreign laws are being tested in foreign courts" (Treasury Board of Canada Secretariat 2018, emphasis added).

This issue highlights the need for sovereign Canadian networks and data infrastructure (including 5G), data regulations and data laws to protect Canadian sovereignty. It also underscores the need for Canadian national security strategy to recognize that data supersedes economics and innovation (i.e., Innovation, Science and Economic Development Canada [ISED]) as a matter of national security because data and data-driven research now drive accelerating technological change.

The tools of war are changing. As an example, a foreign blockade in the digital realm could mean that a foreign power might restrict or suspend Canada from accessing critical data or services. Could a foreign power use this leverage to apply pressure on the Canadian government? Additionally, what if there is a scenario whereby, to protect itself, a foreign ally is forced to shut off its virtual borders? The impact to Canada in this scenario could be catastrophic.

A current example in which sovereignty is already compromised is Canadian domestic internet traffic. The internet is the underlying backbone network that enables the flow of traffic between servers. Data that is flowing across Canada is often routed through servers in the United States. This issue has been aptly called the "boomerang effect" (Clement and Obar 2015). Our dependency on US digital infrastructure could, under extreme cyberthreat scenarios, be especially detrimental to Canadians. Canadian national security measures should require that sensitive data in certain critical industries be stored, routed and

[10] See https://en.wikipedia.org/wiki/Data_sovereignty.

[11] See https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act.

[12] See https://en.wikipedia.org/wiki/CLOUD_Act.

processed within Canada. Canadian domestic internet traffic should remain within Canada.

As data regulations, laws and infrastructure evolve, countries will need to balance their national security concerns with economic and political considerations. Ensuring sovereignty over data and key cyber-infrastructure is now increasingly critical to protecting citizens. Citizen data and sensitive corporate data are at the centre of a struggle between national security and economic growth.[13] This is challenging because data must flow across borders as well as within them.

Data is now a form of capital. Accumulating and monetizing Canadian data is critical to future economic growth. To offer one compelling example, the genetic testing company 23andMe collects vast amounts of genetic data from ordinary Canadians through the use of home-based saliva collection kits. The company's current market cap is $3.2 billion, with 2020 revenues at $475 million. Even as Canadian genomic data freely transits the Canadian border with little or no oversight, the decision to simply "give up" this data undermines Canadian sovereignty and future prosperity.

The asymmetry at play between large data platform companies and individual consumers means that ordinary Canadians are at a substantial disadvantage. Without public oversight, platform companies can act in ways that are harmful to Canada and Canadians. As Facebook whistle-blower Frances Haugen observed, "Until we bring in a counterweight, these [platforms] will be operated for the shareholders' interest and not the public interest" (Haugen, quoted in Waterson and Milmo 2021).

Data Governance

What we require today are governing systems that provide new data standards, new regulatory systems and a new legal infrastructure for guiding the evolution of data-driven technologies. Given Canada's history, economy and values, it is clear that Canadian national security strategy should provide appropriate interoperability and governance standards to support a globally articulated data economy. This approach requires a national security strategy that supports collaboration across departments (i.e., ISED, Global Affairs Canada) and across domestic and international fronts on matters related to data and data-driven EDT. The public service will also require education in developing a uniquely Canadian model of data governance even as Canadian policy makers learn from other countries.

Data governance remains a daunting challenge. There are at least three broad models for data governance practised across the world's largest economies today, in the European Union, China and the United States. Despite these varying approaches, many countries are now requiring that data on their citizens be stored or processed within their borders. This rapidly changing global regulatory landscape around data places a particular burden on industry. Chief information security officers and legal and compliance teams are now required to carry the weight of these global regulatory challenges, even as their businesses aim to capitalize on revenue from data.[14]

The European Union: Data for the Purpose of Citizen Advancement

In 2018, the European Union released a data sovereignty regulation known as the General Data Protection Regulation (GDPR), which has quickly become a global standard. The GDPR prioritizes data privacy and places EU citizens squarely in control of their own data. Ursula von der Leyen, president of the European Commission, has pledged

[13] Cross-border data transfers have been recently challenged between the European Union and the United States are proving to be a growing problem both for economic growth and security. The Court of Justice of the European Union (CJEU) issued a verdict on July 16, 2020, ruling that the EU-US Privacy Shield was invalid. This shield allowed companies to transfer data between the United States and the European Union; however, the CJEU invalidated it due to concerns around surveillance by the US government. This case is known as Schrems II (see https://en.wikipedia.org/wiki/Max_Schrems#Schrems_II). Due to national security concerns, cross-border data flows are under heavy scrutiny. There is also concern that the ruling could put an excessive burden on companies with respect to managing the data of EU citizens when there are cross-border transfers required.

[14] These teams must verify that data exists only where it is allowed as well as show the lineage of data. This task is already monumental, but coupled with digital transformation efforts to move data to the cloud, it becomes expensive as well. Until best practices are established or new tools made available, we can expect many industries to invest heavily in data protection and compliance.

that the European Union will attain "technological sovereignty" in critical areas of the digital economy. For many EU member states, concern is growing that countries are slowly losing both sovereignty and control over their data, inhibiting the ability of nation-states to innovate and/or shape democratic norms and values in the digital arena.[15]

China: Data for the Purpose of State Advancement

In early 2021, China passed its Data Security Law (Bloomberg News 2021). This law strengthens the control that the Chinese government has over data collected within China.[16] Protection of the state and its governance is China's top priority, effectively giving the Chinese government the power to fine or close firms that mishandle "core state data." As such, the law requires that major decisions involving data security are to be made by national security officials. In November 2021, China put into effect its data protection law, the Personal Information Protection Law (PIPL) (Bagchi 2021), overseeing the collection of citizen data by private businesses. Widely regarded as China's version of the GDPR, the PIPL provides rules overseeing how businesses can collect, process and transfer the personal information of Chinese citizens.

The United States: Data for the Purpose of Economic Advancement

The United States currently has no federal-level data protection laws. Certain states are crafting their own consumer data privacy regulations, such as the California Consumer Privacy Act.[17] Consequently, the US government has struggled to constrain the accumulating wealth and power of its big tech firms. By building tools that enable a form of "surveillance capitalism," US tech firms have deliberately commoditized the personal data of users to drive enormous profits. The United States is home to the world's largest cloud providers (for example, Amazon Web Services, Microsoft and Google); therefore, the US government faces a significant challenge with regard to protecting citizen data, maintaining trust in its democracy and holding technology firms accountable while also ensuring a thriving technology industry.

Canada's Approach to Digital Trust, Data Sovereignty and EDT

The real value of data is found in its quantity and quality for driving innovation. Data is the "operational exhaust" of digital systems running at scale today. For this reason, the proliferation of surveillance systems deployed by governments and the private sector to monitor populations is now a routine feature of a data-driven society.

In November 2020, the Canadian government proposed the Digital Charter Implementation Act (part of Bill C-11) (ISED 2020), signalling that it is taking some steps to establish data protection rights for Canadians. In particular, the Consumer Privacy Protection Act, an update to the Personal Information Protection and Electronic Documents Act, focuses on individuals having more control over their personal information. Canada is aiming to build a foundation of "trust" in the digital age. Critics of Bill C-11 (Kenyon 2021; Cofone 2020; Scassa 2021) argue that the legislation does not represent human rights principles in the digital era, due to its lack of clarity in the areas of de-identification, meaningful consent or data mobility.

With regard to AI, Canada has released a Directive on Automated Decision-Making[18] with the purpose of ensuring that deployed AI-based technology reduces harm to Canada and to Canadians. The objective is to ensure that such technology is deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent and

[15] Although the promotion of democratic values is at the forefront of EU data and digital messaging, its foundation is underpinned by the potential for building economic strength. A core feature of the European Union's Digital Strategy is the concept of a Digital Single Market (see www.europarl.europa.eu/factsheets/en/sheet/43/the-ubiquitous-digital-single-market), introduced in 2019. The Digital Single Market is intended to promote e-commerce across the European Union's digital economy. It requires that data flows freely across the European Union, thus forcing a regulatory framework around data connectivity, safeguarding privacy, cybersecurity and cross-border data access. It also offers a window into what needs to come across international markets.

[16] Additionally, the Cyberspace Administration of China has released a draft of regulations on data classification as it relates to national security.

[17] See https://oag.ca.gov/privacy/ccpa.

[18] See www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

interpretable decisions. Interestingly, national security systems are exempt from this directive.

Even as the federal government has begun taking steps to protect Canadians, there is much more to do. The global "data arms race" and great power competition between China and the United States mean that Canada will need to update its national security strategy. In particular, national security should play a larger role in both innovation policy and economic development. More to the point, there is a need to ensure that:

- Canadian technology supports a global standard with respect to our values and principles, while being interoperable with our allies, our trade partners and the broader UN community; and
- Canada has the capacity to appropriately create, sustain and protect its digital and data resources and the rights of its citizens.

Traditional notions of Canadian sovereignty are understood in terms of the protection of land, natural resources and freedoms. Today, the issue of sovereignty also directly overlaps Canada's digital infrastructure, which includes data, software, interoperability standards, and Canadian rights and freedoms[19] in the digital domain.

Data as a National Asset

Given the changing nature of national security, Canada must elevate data to the level of a national asset. This move is critical to both economic growth and technological innovation but also to Canadian national security. Data is one of the most strategic assets in driving sustainability, autonomy and economic prosperity in the network era. Similar to natural resources, data can fuel immense economic growth and innovation for Canadians. But this data must be appropriately secured and regulated through a proper digital trust infrastructure.

Data is the key to unlocking EDTs. Protecting and harnessing data as a national asset will mean rethinking the large centralized digital infrastructure that now constitutes our data architectures. Securing critical data means exploring public infrastructure and interoperability mechanisms that are flexible, modular and resilient. Data security in the network era should be decentralized, distributed and federated in order to avoid the vulnerabilities of centralized systems.

Data as a national asset means:

- recognizing that Canadian data is an asset to Canadian society and the Canadian economy;
- recognizing that protecting Canadian data means protecting Canadians;
- recognizing that Canadian data has tangible financial value — it is a capital resource asset;
- prioritizing certain data as a public utility to drive innovation;
- restricting certain data sharing and access for national security purposes;
- ensuring data collectors and processors adhere to specific rules to protect national security interests;
- classifying certain data and digital systems as critical infrastructure having national security implications;
- recognizing the need for sovereign Canadian digital and data infrastructure; and
- recognizing that economic prosperity with data and EDT intersects Canadian democracy, sovereignty and national security.

Realizing the vision of "data as a national asset" is a massive undertaking that requires educating the public, taking a whole-of-government approach to data, and understanding its economic and national security implications, while bridging collaboration between the public and private sectors. The hard lesson we have learned from the pandemic is how unprepared the government has been to share data and health information across provinces and territories in a timely manner (Wolfson 2021).

Focusing on Data Supply Chain Sovereignty

Sovereignty over data means having authority over data assets as well as authority over data access, production and distribution. The hardware and cloud systems that store Canadian data, the

[19] See www.canada.ca/en/canadian-heritage/services/how-rights-protected/guide-canadian-charter-rights-freedoms.html.

network and routing systems that enable the flow of Canadian data, and the software systems that process and mediate access to Canadian data are all parties in the overall data supply chain.[20] The sovereignty of each must be considered when developing overall sovereignty of our national data assets. The safety and prosperity of our future digital nation depends on the ability of our democracy and our government to exert sufficient oversight over the flow of data through our national digital infrastructure.

National Security Strategies for the Digital Age

For Canada to advance a national security posture tailored to the digital age, government, industry and academia will need to collaborate in a more integrated fashion. Given that so much technology innovation is industry-led, advancing public-private partnerships is critical to Canadian national security strategy. Additionally, government processes and planning will need to adapt to accelerated innovation cycles alongside new and different knowledge, resources and expertise.

National Systems of Innovation

The pace of innovation today places a premium on the continuous reskilling, training and knowledge exchange between government, industry and academia. This overlaps needed investments in advancing a Canadian GaaP model that matches EDT's aggressive obsolescence cycles and cross-platform integration challenges. This also builds on the need for more extensive collaboration between industry, academia and government.

National innovation necessarily depends upon institutional actors collaborating toward a shared goal. For this reason, Canadian national security strategy must stress the need for coordinated flows of technology and information among people and institutions in driving long-term innovation. This kind of multi-domain collaboration has historically been defined in terms of a national system of innovation (NSI) (Organisation for Economic Co-operation and Development 1997).

NSI policy and planning can take many forms. These range 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.

The Liberal government's proposal to establish CARPA[21] — a public-private intermediary in high-impact areas — could be critical to advancing Canada's frontier technologies. Canada's cyber industry alone generates more than CDN$1 billion in annual export revenues. Despite this success, the federal government procures approximately 90 percent of its cyber technology from large foreign suppliers (CADSI 2019).[22] This must change. Like the Defense Advanced Research Projects Agency in the United States, CARPA could harness the next generation of Canadian EDT while simultaneously advancing related government initiatives (for example, the Pan-Canadian Artificial Intelligence Strategy,[23] the National Research Council's Canadian Photonics Fabrication Centre,[24] Canada's Innovation Superclusters Initiative[25] and a future National Quantum Strategy[26]).

[20] When moving from strategy to execution of the Canadian data supply chain, we need to have a better shared understanding of the stages data goes through. Although traditionally, data is conceptualized as "moving" from one physical location to another, new technologies and standards today are promoting the concept of "zero-copy" or "data in place." This again transforms the linear view of the data supply chain into a mesh of interconnected nodes. Each "node" is a silo of information connecting to the network. The transition of systems from centralized banks of information, where linear workflows are performed, to decentralized and distributed systems, which perform atomic functions and services, is also the direction in which software technology architecture and cybersecurity are heading.

[21] See https://liberal.ca/our-platform/a-new-advanced-research-agency/.

[22] As a CADSI (2021) review on military procurement makes clear, Canada's industrial-era acquisition system will need to be redesigned.

[23] See https://cifar.ca/ai/.

[24] See https://nrc.canada.ca/en/research-development/nrc-facilities/canadian-photonics-fabrication-centre.

[25] See www.ic.gc.ca/eic/site/093.nsf/eng/home.

[26] See www.ic.gc.ca/eic/site/154.nsf/eng/home.

Opportunities for Canada

What should be the role of nation-states in managing EDTs for the purposes of national security in a multipolar era? EDTs such as AI, 5G and IoT are simultaneously transforming communication, health care, trade, finance, labour markets and value chains across a wide range of industries and geographies, blurring traditional regulatory boundaries. Indeed, the speed with which data-driven EDT now converges and diffuses to shape the global economy and the nature of organizations is unprecedented.

Unfortunately, governments working in isolation simply cannot hope to manage the escalating pace of threats and/or opportunities across the spectrum of EDT. AI systems alone offer a range of challenges overlapping automation, algorithmic bias, labour automation, cyberespionage, fintech, "surveillance capitalism" and personal privacy that will need to be addressed through various forms of regulation. The lack of policy coordination and regulatory systems among nation-states at the global level remains a substantial problem.

Canadian Multilateralism

As a 2021 white paper from the WEF (2021) makes clear, global governance of EDT is a patchwork. As a global middle power, Canada should look to align more closely with its allies in the United States, Europe, Asia and the UN community more broadly to help in supporting democratic values and norms in the development and regulation of EDT. The European Union, in particular, provides a strong model for developing systems that enable and govern citizen data.

Europe's International Data Spaces Association[27] (IDSA) offers a promising example. The IDSA has a membership base of 130 companies representing 20 different countries across the European Union. Founded in 2016 by the Fraunhofer Institute in Germany, the IDSA provides a distributed network of data nodes or end points that enable the exchange of data while guaranteeing data sovereignty. The IDSA holds data sovereignty as a paramount principle and defines data sovereignty as "the ability of a natural or legal person to ensure exclusive self-determination regarding their data assets."[28]

In collaboration with Gaia-X,[29] the IDSA provides a technical reference model, standards and infrastructure that enable federated, secure and trustworthy data sharing. The aim of Gaia-X is to develop common requirements for a European data infrastructure, providing both economic development as well as national security and sovereignty in the data era. This supports the EU vision of a Digital Single Market across its member nations.

Estonia is perhaps the best example of data governance anywhere in the world. Most of Estonia's public services are digitally enabled and anchored to citizen digital identification cards. Often described as the first "digital republic" (Khan and Shahaab 2020), Estonia has even created the first "digital embassies" (Rice 2019), providing a digital backup in the event of any loss of autonomy or sovereignty.

At the same time, Estonia is not Canada. With a population of 1.3 million and a unique history, Estonia may not perfectly mirror Canada's needs. Given that Canada is a federation with provinces and territories rather than a small unitary state, a distinct federal-provincial-territorial (FPT) framework will be key.

A critical approach to developing a Canadian security framework will be the use of DLTs or blockchain. Designed to support an entirely new peer-to-peer architecture for managing data, blockchain eliminates the need for centralized controls while tracking and recording transactional data without error. Through the use of software-driven smart contracts, blockchain allows for law to become code. And through decentralized finance, it enables digital and non-digital assets to become tangible financial assets.

DLTs are foundational to powerful new tools driving economic and military development around the world, and Canada should be innovating in this space. China's government, for example, is already heavily invested in the development of an "advanced blockchain industrial system" (Feng and Borak 2021). With the goal of

[27] See https://internationaldataspaces.org.

[28] See www.dataspaces.fraunhofer.de/en/faq.html.

[29] See www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

becoming a global leader by 2025 (*Global Times* 2021), China plans to deploy the world's largest blockchain infrastructure to enhance global cooperation under its Belt and Road Initiative.[30]

Policy Proposals

The following are recommendations for shaping a Canadian response to a changing geopolitical landscape. As these proposals make clear, Canada needs to expand its digital infrastructure with respect to both modernization and its operational capacity, scale and resiliency. This approach will require a robust Canadian NSI in which government, industry and academia collaborate toward a common purpose. In all the proposed recommendations, Canadian national security leadership must be involved in some capacity.

Promote the importance of data as a national asset: In the data economy, data is a national asset. Canada must foster a data culture and educate both the public and the private sectors about the importance of data in strengthening and securing Canada's digital resources. In a data culture, data is woven into the operations, mindset and identity of a community and its leadership.[31] In May 2020, Canada announced CDN$80 million (Scott 2021) for a new national cybersecurity network. This initiative could be leveraged to promote the importance of data education, particularly around data security.

Pursue efforts to support both national and multilateral initiatives for data security and governance: Canada should pursue solutions to security challenges in the digital era through multilateral institutions and mechanisms that straddle security divides. At the very least, this means working with UN partners in developing comprehensive and multilateral regulatory frameworks for governing EDT and data.

Support and promote a sovereign Canadian cloud infrastructure and space-based internet: Canadian cloud infrastructure is a critical cyber infrastructure for the EDT era. Canada's reliance on foreign cloud-computing providers poses a threat to national security as our organizations and our governments adopt the cloud to harness data and leverage EDT. Canadian policy makers should ensure that Canada has a sovereign cloud provider ecosystem[32] as an alternative to foreign technology firms.[33] This ecosystem includes space-based satellite telecommunications. Promoting a sovereign cloud infrastructure does not necessarily equate to forced data localization. Rather, it provides feasible alternatives to foreign cloud providers in cases where such infrastructure is needed for sensitive public/private data.

Build a national data infrastructure: Data is a critical national asset. As the basis for EDT, data unlocks innovation and should be protected for the purposes of national security. To ensure this data protection, Canada requires public data infrastructure that is distributed, trusted and interoperable. Government could leverage existing investments in the current innovation infrastructure[34] (i.e., national superclusters, Pan-Canadian AI Strategy) to foster a more robust

[30] See www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative.

[31] See www.tableau.com/why-tableau/data-culture.

[32] While Starlink leads the way in space-based broadband internet, a Canadian company, Telesat, is working to provide such services, and support for its operations in Canada could help secure Canadian data privacy and security. There are other domestic traditional cloud compute providers available as well.

[33] Foreign "hyperscalers" have dominated the Canadian cloud ecosystem, creating increased dependency and risk to our network sovereignty and national security. Additional foreign firms are participating in key elements of the data supply chain/cyberinfrastructure, including web hosting, content distribution, internet services at competitive prices and so forth. These firms can end up creating a significant barrier to entry for local firms to compete. However, one policy element to consider is whether Canada should create equivalent cloud providers in Canada or ensure that the rules and regulations enable more equal competition.

[34] In the context of infrastructure, data as an asset cannot be separated from the underlying software, hardware and network systems that enable data production, access, storage and transmissions. This infrastructure includes the standards around data interoperability, access, governance and so forth. Any national data infrastructure will need to consider the security and sovereignty elements for the entire technology stack that data depends on. Additionally, this trusted data infrastructure would need to provide a sovereign network with sufficient scale and computational power to produce, process and access sovereign data. This could be done in an interoperable fashion with the appropriate standards or application programming interfaces to connect to data and services.

Canadian NSI.[35] This would mean an FPT data framework that recognizes the national security aspects of data sharing. This approach could build on provincial projects such as the Ontario "Data Authority" (Government of Ontario 2021) announced in April 2021.[36] Data standards[37] are key to the development of a national data infrastructure. Building on provincial investments, the federal government will need to establish federal data standards that serve the national interest.

Establish a cross-governmental unit to handle EDTs with an enhanced mandate for Canada's CTO: Technology leadership within the Canadian government is in "catch-up" mode. Canada has been slow to move forward on many digital government initiatives. For this reason, Canada needs enhanced leadership within the federal government to navigate the EDT era. Canada's CTO should be given a horizontal function and an enhanced mandate. Similar to the role of the CTO within commercial industry, Canada's CTO should be responsible for overseeing the selection, implementation and application of technology across government, including technology procurement and process organization across departments. In the context of national security strategy, national security leadership should work in collaboration with the office of the CTO to ensure appropriate national security concerns are addressed in technology strategy and implementation.

Redefine critical infrastructure in the era of EDT: Critical infrastructure and supply chains have become increasingly complex, global and interconnected. This evolving landscape inherently makes security more complicated across a broad range of existing and emerging systems and processes. At the national level, the defence and security of critical infrastructure — particularly cyber infrastructure — means protection from a wide array of malicious activities perpetrated by both state and non-state actors across a range of criminal, political, economic and/or military activities. The category of critical infrastructure today must include software and hardware systems as well as space-based applications and infrastructure. Cloud and data-sharing infrastructure in specific industries should be explicitly classified as critical infrastructure. Taken as a whole, the data supply chain that supports the digital fuel for EDT should now be seen as national security assets.

Provide public support for innovation in the form of direct procurement across key EDT sectors: Increase direct procurement in key sectors for EDT including data infrastructure, cybersecurity, cloud, applied AI, blockchain and quantum technologies. As the 2019 CADSI (2019, 17) annual report indicates, 60 percent of DND purchases went to foreign suppliers and rose to 94 percent foreign purchases in the area of ICT security. This poses a critical risk to the Canadian economy and to Canadian national security. All levels of government should work together in supporting strategic EDT sectors.

Develop homegrown talent in critical capacities for EDT: Capacity building within Canada's technology industry is critical to its future resiliency and safety in the digital domain. Collaboration between government, universities and the private sector is an imperative. In addition to improving procurement practices and investing in research and commercialization, Canada

[35] Canada has the opportunity to encode democratic values and norms within the digital domain through such a build out, ensuring that businesses and governments can connect and apply Canadian data in a privacy-preserving manner. The Gaia-X initiative as part of the European data strategy is a good example of such a data infrastructure. Here in Canada, there are examples of a new type of data infrastructure being built, called data trusts. Data trusts have emerged as a potential digital infrastructure model. Data is a fundamental building block of a prosperous and resilient innovation economy. To offer one example, Innovate Cities (see https://innovatecities.com), a Canadian not-for-profit, is building a data trust. The Innovate Cities data trust will operate as a not-for-profit utility to boost the data innovation ecosystem. It will also abide by the highest governance and privacy standards. In the digital age, the right to privacy is a human right that needs to be both protected and nurtured. A data trust that operates in accordance with these principles will play an important role in helping to protect both the privacy rights of Canadians and to advance Canada's economic and national security interests. Through appropriate investment and collaboration, Canada can easily utilize its existing assets and set the bar for digital cooperation, digital democracy governance standards (for example, the Standards Council of Canada's *Canadian Data Governance Standardization Roadmap* [see www.scc.ca/en/system/files/publications/SCC_Data_Gov_Roadmap_EN.pdf], the CIO Strategy Council's data governance standards [see https://ciostrategycouncil.com/standards/]) and responsible use of emerging technologies.

[36] This concept is the first of its kind in Canada. It would be responsible for building out data infrastructure to enable economic growth while ensuring privacy. It is still unclear exactly how this data authority would operate or how it will be accepted by the citizens of Ontario. However, it is important that federal leadership builds an interoperable national data infrastructure that will benefit and protect all Canadians. A crucial element to this will, however, be that all Canadians have access to proper network connectivity (see Canadian Internet Registration Authority, n.d.).

[37] Such an infrastructure must be compatible with standards that are globally recognized. Standards around data sharing and data governance are a critical foundation for the data economy. The CIO Strategy Council in Canada has developed standards and specifications regarding approaches and architectures for the secure collection and exchange of data.

should directly nurture, develop and retain its human talent across domains of EDT, including cyber, digital identity, privacy and security, and experimental research. This means nurturing our talent at home as well as attracting foreign talent from abroad. As Canada's Minister of Innovation, Science and Industry François-Philippe Champagne pointed out, "Strong cyber security expertise and innovations are key to protecting Canada's data and intellectual property and to maintaining the competitiveness of Canada's businesses" (Scott 2021). This means bridging Canada's private sector talent with Canada's national security workforce. Most importantly, Canadian national security strategy must be clear in its mandates and vision for responsible and ethical innovation in order to attract high-calibre talent.

Create an innovation ecosystem around national security technology with appropriate public investment: In the United States, In-Q-Tel,[38] a non-profit venture capital firm developed by the Central Intelligence Agency, actively invests in high-tech start-ups that are directly focused on building out US intelligence capabilities. The federal government could consider this as a potential model for building an innovation ecosystem around national security. Building on initiatives such as Innovation for Defence Excellence and Security,[39] Mobilizing Insights in Defence and Security[40] and the Cyber Innovation Network,[41] Canada could directly grow its national security capabilities by investing in frontier technologies. The Liberal government's recent proposal to establish CARPA[42] could support this recommendation. Despite the fact that the cybersecurity industry in Canada remains distributed and fragmented, local accelerator programs such as the Rogers Cybersecure Catalyst[43] in Ontario could be recruited by the government to help identify innovative start-ups and scale-ups that have high-growth potential in the cybersecurity industry.

Establish a national security institution in the form of a digital and data academy: Canada needs to develop knowledge and talent within the Canadian national security ecosystem through continuing education — particularly with regard to digital technologies and data. This could take the form of a digital or data academy. This institution could be independent of the Canada School of Public Service or in collaboration with it. However, it must focus on deep technical expertise in cyber, AI, data, blockchain, quantum technologies and their national security implications. National security teams would need to have their own curated digital and data education track and course list supported by state-of-the-art advancements within industry. This is another area where a network of private sector experts could support such an initiative as well as provide deep technical training. The general public service could benefit from national security education with respect to decisions being made around data and EDT.

Define a data strategy for Canadian national security leadership: Canadian national security leaders should establish an innovation and data strategy to ensure preparedness in the EDT era. As an example, Canada's Directive on Automated Decision-Making[44] exempts national security. This leaves behind a gap in understanding how Canadian national security leadership should harness data and EDT. In September 2020, the US Department of Defense (2020) announced a data strategy titled "Unleashing Data to Advance the National Defense Strategy." In it, they defined eight key strategic areas:

→ data as a strategic asset;

→ collective data stewardship;

→ data ethics;

→ data collection;

→ enterprise-wide data access and availability;

→ data for AI training;

→ data fit for purpose; and

→ design for compliance.

[38] See www.iqt.org.

[39] See www.canada.ca/en/department-national-defence/programs/defence-ideas/understanding-ideas.html.

[40] See www.canada.ca/en/department-national-defence/programs/minds.html.

[41] See https://ised-isde.canada.ca/site/cyber-security-innovation-network/en.

[42] See https://liberal.ca/our-platform/a-new-advanced-research-agency/.

[43] See www.cybersecurecatalyst.ca.

[44] See www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

The Canadian national security data strategy should also be appropriately integrated with an update to its defence ethics[45] in a digital world.

Build public-private partnerships in the fields of AI, data, blockchain, cyber and quantum: Canada has a strong AI, cyber, blockchain and quantum ecosystem. These industries provide the nation with key strengths going into the EDT era. Canadian national security strategy must deploy these strengths in strategic ways, encouraging cross-collaboration through public-private partnerships. There continues to be a gap in how the government collaborates with Canadian small and medium-sized enterprises, for example. In response to this, a network of private sector experts could be called upon to develop a plan that builds better connectivity between government, university researchers and commercial industry in key areas of EDT.

Educate the Canadian public on the changing landscape of emerging technologies and what it means for them: The Canadian public needs education and guidance around the importance of personal data. This includes guidance on legal protections (or lack thereof) governing personal information both within and outside of Canada. The Canadian government should work to educate Canadians on the controls available to identify threats or bad actors. Building on this education process, Canadian planners could help support and equip Canadians with basic tools for the digital era.

Conclusion

As NATO's (2020) annual report on EDT makes clear, keeping pace with technological change necessitates agility and rapid iteration with respect to the development, experimentation and application of technology. Leveraging technological innovation as part of Canadian national security must be part of a wider innovation ecosystem that effectively integrates research and implementation.

Even as the industrial era winds down (Araya 2020), technological innovation is speeding up. A substantial challenge for Canadian national security strategy over this decade will be appreciating the development and convergence of EDTs in new forms. Technology is transforming the nature of national security across a changing geopolitical landscape. Much as in the past, emerging technologies will trigger widespread social and economic development beyond their initial application.

Data is now the basis for EDTs, and Canadian national security will need to be recalibrated to reflect this reality. The current decade will be fuelled by data and will continue to drive the creation of ever-more data-driven technologies — especially AI. Alongside the global rollout of 5G edge networks, it is anticipated that there will be an explosion of data created, collected, processed and stored across highly robust global information networks.

Even as modern security regimes rely on conventional forms of technological superiority to maintain military readiness, the rapid development and proliferation of highly accessible data-driven technologies are now reshaping the global balance of power. Technological advantage has been a key pillar of NATO countries, but other countries are quickly catching up. China's technology sector is reaching a critical mass of expertise, talent and capital that is realigning the commanding heights (Lucas and Waters 2018) of the global economy.

Given that so much technology innovation is now industry-led, advancing public-private partnerships is critical to Canadian national security strategy. Unfortunately, the same digital networks driving commercial innovation and economic growth are also driving social fragmentation and new forms of criminal activity. More problematically, Canada's critical digital infrastructure is almost exclusively owned by private firms, undermining the capacities of any government-led data security strategy.

For Canada to advance a national security posture tailored to the digital age, government, industry and academia will need to collaborate as an organic whole. Part of the answer to resolving this challenge will involve the development of public infrastructure that can secure and govern a data-driven society. Upgrading governance platforms around decentralized networks will be important to transforming the single points of failure inherent to industrial-era bureaucracies. Government processes and planning will also need to adapt to accelerated innovation cycles alongside new and different knowledge, resources and expertise.

[45] See www.canada.ca/en/department-national-defence/services/benefits-military/defence-ethics.html.

What we require today are governing systems that provide new data standards, new regulatory systems and a new legal infrastructure for guiding the evolution of data-driven technologies. Given Canada's unique history, economy and values, it is clear that Canadian strategy should provide appropriate interoperability and governance standards to support a globally articulated data economy. To be sure, the continued evolution of Canadian national security strategy will require education within the public service in developing a uniquely Canadian model of data governance even as Canadian policy makers learn from other countries.

In an era defined by existential threats (digital, biological and ecological), the current "rules-based order" appears to be fraying. Canada's reputation as a nation that supports multilateralism and the rule of law is an important basis upon which to promote responsible data governance. Indeed, some analysts have proposed a World Data Organization (Bailey 2019) or a Digital Stability Board (Fay, quoted in Emanuele 2021) as new institutions for a digital era. These kinds of multilateral data governance institutions could provide the needed guardrails in guiding the evolution of EDT — particularly the responsible use of AI. As AI is increasingly applied to both public and private domains, the potential for serious and credible threats to Canadian national security strategy will grow.

Canadian policy and planning now face a unique geopolitical environment framed by great power competition, extreme climate events and accelerating technological disruption. Canada could play a strong role in shaping the rules for this new era, particularly in terms of data governance and the regulation of EDT. Given the inherent challenges of governing technologies with global reach, Canadian national security strategy should focus on supporting and partnering with like-minded nations and transnational organizations such as the European Union, the Association of Southeast Asian Nations and the United Nations in promoting digital democracy and multilateral governance. In the face of a rapidly evolving digital era, international cooperation will be critical to ensuring sustained peace and security.

Works Cited

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

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=6b4a61ed2c57.

Araya, Daniel and Rodrigo Nieto-Gómez. 2020. "Renewing Multilateral Governance in the Age of AI." Modern Conflict and Artificial Intelligence Essay Series, Centre for International Governance Innovation, November 9. www.cigionline.org/articles/renewing-multilateral-governance-age-ai/.

Asselin, Robert and Sean Speer. 2019. *A New North Star: Canadian Competitiveness in an Intangibles Economy*. Ottawa, ON: Public Policy Forum. https://ppforum.ca/wp-content/uploads/2019/04/PPF-NewNorthStar-EN4.pdf.

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

Atlantic Council Geotech Center. 2021. *Report of the Commission on the Geopolitical Impacts of New Technologies and Data*. Atlantic Council, May. www.atlanticcouncil.org/wp-content/uploads/2021/05/GeoTech-Commission-Report-Full.pdf.

Bagchi, Rounak. 2021. "Explained: China's new data privacy laws and its impact on the tech industry." *The Indian Express*, August 22. https://indianexpress.com/article/explained/china-new-data-privacy-law-7463166/.

Bailey, Ronald. 2019. "Do We Need a World Data Organization?" Reason, November 22. https://reason.com/2019/11/22/do-we-need-a-world-data-organization/.

Bazilian, Morgan, Michael Bradshaw, Andreas Goldthau and Kirsten Westphal. 2019. "Model and manage the changing geopolitics of energy." *Nature* 569: 29–31.

Benay, Alex. 2019. "Canada needs to assert its digital identity." *The Globe and Mail*, October 3. www.theglobeandmail.com/business/commentary/article-canada-needs-to-assert-its-digital-identity/.

Bloomberg News. 2021. "China's New Data Law Gives Xi the Power to Shut Down Tech Firms." Bloomberg News, June 10. www.bloomberg.com/news/articles/2021-06-10/china-passes-law-to-strengthen-control-over-tech-firms-data.

Buchholz, Katharina. 2019. "China's rise to commercial superpower." Statista, October 2. www.statista.com/chart/19535/exports-and-imports-china/.

Butler, Declan. 2016. "Tomorrow's World." *Nature* 530: 398–401. www.nature.com/news/polopoly_fs/1.19431!/menu/main/topColumns/topLeftColumn/pdf/530398a.pdf.

CADSI. 2019. *From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence.* Ottawa, ON: CADSI. www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-24.pdf.

———. 2021. *Procurement at Cyber Speed.* Ottawa, ON: CADSI. www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-37.pdf.

Canadian Centre for Cyber Security. 2018. *National Cyber Threat Assessment 2018*. Ottawa, ON: Communications Security Establishment. https://cyber.gc.ca/sites/default/files/publications/national-cyber-threat-assessment-2018-e_1.pdf.

Canadian Internet Registration Authority. n.d. *Unconnected: Funding Shortfalls, Policy Imbalances and How They Are Contributing to Canada's Digital Underdevelopment.* Ottawa, ON: Canadian Internet Registration Authority. www.cira.ca/resources/state-internet/report/unconnected.

Clement, Andrew and Jonathan A. Obar. 2015. "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges." In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 13–44. Ottawa, ON: University of Ottawa Press.

Cofone, Ignacio. 2020. "Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report." Office of the Privacy Commissioner of Canada, November. www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/.

Confessore, Nicholas. 2018. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *The New York Times*, April 4. www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

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

Conzade, Julian, Andreas Cornet, Patrick Hertzke, Russell Hensley, Ruth Heuss, Timo Möller, Patrick Schaufuss, Stephanie Schenk, Andreas Tschiesner and Karsten von Laufenberg. 2021. "Why the automotive future is electric." McKinsey & Company, September 7. www.mckinsey.com/industries/automotive-and-assembly/our-insights/why-the-automotive-future-is-electric.

Delouya, Samantha. 2020. "Market value of big fintech companies rises to $1 trillion, more than the largest banks." CNBC, September 16. www.cnbc.com/2020/09/16/market-value-of-big-fintech-companies-rises-to-1-trillion-more-than-the-largest-banks.html.

Department of Defense. 2020. "DoD Data Strategy." Department of Defense, September 20. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

Emanuele, Marco. 2021. "Towards the Digital Stability Board for a digital Bretton Woods." *The Science of Where Magazine*, February 1. www.thescienceofwheremagazine.it/2021/02/01/towards-the-digital-stability-board-for-a-digital-bretton-woods/.

Erwin, Sandra. 2021. "Hyten blasts 'unbelievably' slow DoD bureaucracy as China advances space weapons." Space News, October 28. https://spacenews.com/hyten-blasts-unbelievably-slow-dod-bureaucracy-as-china-advances-space-weapons/.

Fay, Robert, David Dodge, Serge Dupont, Mark Jewett and John Murray. 2021. *Canada and the Digitalization of Money: Key Takeaways from a Virtual Workshop of International and Canadian Experts*. Conference Report, Centre for International Governance Innovation, October 21. www.cigionline.org/publications/canada-and-the-digitalization-of-money-key-takeaways-from-a-virtual-workshop-of-international-and-canadian-experts/.

Feng, Coco and Masha Borak. 2021. "China plans to accelerate blockchain development and adoption in push to become a world leader in the technology by 2025." *South China Morning Post*, June 9. www.scmp.com/tech/tech-trends/article/3136515/china-plans-accelerate-blockchain-development-and-adoption-push.

Global Times. 2021. "China takes steps to boost blockchain industry into world-leading position by 2025." *Global Times*, June 7. www.globaltimes.cn/page/202106/1225636.shtml.

Goodman, Marc and Parag Khanna. 2013. "The Power of Moore's Law in a World of Geotechnology." *The National Interest*, January 2. https://nationalinterest.org/article/the-power-moores-law-world-geotechnology-7888?nopaging=1.

Government of Ontario. 2021. "Ontario Moves One Step Closer to Becoming a World-Leading Digital Jurisdiction." News release, April 30. https://news.ontario.ca/en/release/1000039/ontario-moves-one-step-closer-to-becoming-a-world-leading-digital-jurisdiction.

Hawksworth, John, Richard Berriman and Saloni Goel. 2018. "Will robots really steal our jobs? An international analysis of the potential long term impact of automation." PricewaterhouseCoopers LLP. www.pwc.com/hu/hu/kiadvanyok/assets/pdf/impact_of_automation_on_jobs.pdf.

Horowitz, Michael C. 2020. "AI and the Diffusion of Global Power." Modern Conflict and Artificial Intelligence Essay Series, Centre for International Governance Innovation, November 16. www.cigionline.org/articles/ai-and-diffusion-global-power/.

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

ISED. 2020. "New proposed law to better protect Canadians' privacy and increase their control over their data and personal information." News release, November 17. www.canada.ca/en/innovation-science-economic-development/news/2020/11/new-proposed-law-to-better-protect-canadians-privacy-and-increase-their-control-over-their-data-and-personal-information.html.

Ito, Joichi, Neha Narula and Robleh Ali. 2017. "The Blockchain Will Do to the Financial System What the Internet Did to Media." *Harvard Business Review,* March 9. https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media.

Kania, Elsa B. 2017. "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's 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.

Keller, Christian, Tomasz Wieladek and Iaroslav Shelepko. 2018. "Macroeconomics of the machines." Barclays, April 10. www.fullertreacymoney.com/system/data/files/PDFs/2018/April/27th/Barclays_Macroeconomics_of_the_machines.pdf.

Kenyon, Miles. 2021. "Bill C-11 Explained." Citizen Lab, April 23. https://citizenlab.ca/2021/04/bill-c-11-explained/.

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

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

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

Lund, Susan, Anu Madgavkar, James Manyika, Sven Smit, Kweilin Ellingrud, Mary Meaney and Olivia Robinson. 2021. *The future of work after COVID-19*. McKinsey Global Institute, February 18. www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19.

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

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

O'Hanlon, Michael E. 2018. "The role of AI in future warfare." Brookings, November 29. www.brookings.edu/research/ai-and-future-warfare/.

O'Reilly, Tim. 2010. "Government as a Platform." *Innovations* 6 (1): 13–40.

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

Propp, Kenneth. 2019. "Waving the flag of digital sovereignty." *New Atlanticist* (blog), December 11. www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty.

Public-Private Analytic Exchange Program. 2019. "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar." https://nsiteam.com/social/wp-content/uploads/2019/11/191119-AEP_Commodification-of-Cyber-Capabilities-Paper.pdf.

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

Roberts, Megan M. 2021. "The UN Security Council Tackles Emerging Technologies." *Net Politics* (blog), May 28. www.cfr.org/blog/un-security-council-tackles-emerging-technologies.

Scassa, Teresa. 2021. "Bill C-11's Treatment of Cross-Border Transfers of Personal Information." Office of the Privacy Commissioner of Canada, May. www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_scassa_2105/.

Schwab, Klaus. 2016. "The Fourth Industrial Revolution: what it means, how to respond." WEF, January 14. www. weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

Scott, Josh. 2021. "Canada Earmarks $80 Million for New National Cybersecurity Network." Betakit, May 6. https://betakit.com/canada-earmarks-80-million-for-new-national-cybersecurity-network/.

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 & International Studies, December 8. www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

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

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

Tambur, Silver. 2021. "Estonia's X-Road solution launched in Mexico." *Estonian World*, February 2. https://estonianworld.com/technology/estonias-x-road-solution-launched-in-mexico/.

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

Trafton, Anne. 2020. "Artificial intelligence yields new antibiotic." *MIT News*, February 20. https://news.mit.edu/2020/artificial-intelligence-identifies-new-antibiotic-0220.

Treasury Board of Canada Secretariat. 2018. "Government of Canada White Paper: Data Sovereignty and Public Cloud." www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html.

———. 2019. “The Canadian Digital Exchange Platform (CDXP): Canada’s Digital Backbone.” https://ciostrategycouncil.com/wp-content/uploads/2019/02/Canadas-Digital-Backbone-EN-Teresa.pdf.

Tucker, 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/.

Waldie, Paul and Colin Freeze. 2020. “Four Canadian military schools affected by cyber attack.” *The Globe and Mail*, July 7. www.theglobeandmail.com/canada/article-four-canadian-military-schools-affected-by-cyberattack/.

Waterson, Jim and Dan Milmo. 2021. “Facebook whistleblower Frances Haugen calls for urgent external regulation.” *The Guardian*, October 25. www.theguardian.com/technology/2021/oct/25/facebook-whistleblower-frances-haugen-calls-for-urgent-external-regulation.

WEF. 2020. *The Future of Jobs Report 2020*. Geneva, Switzerland: WEF. www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf.

———. 2021. “Data for Common Purpose: Leveraging Consent to Build Trust.” White Paper, November. www3.weforum.org/docs/WEF_Data_for_Common_Purpose_Leveraging_Consent_to_Build_Trust_2021.pdf.

White, Tracy M. and David A. Wolfe. 2021. “Canada as a Learning Economy: Education and Training in an Age of Machines: Policy Challenges and Policy Responses.” Munk School of Global Affairs and Public Policy, Innovation Policy Lab Working Paper Series 2021-04. https://munkschool.utoronto.ca/ipl/files/2021/08/IPL-Working-Paper-2021-04-White-and-Wolfe.pdf.

Wirkierman, Ariel L., Tommaso Ciarli and Maria Savona. 2018. “Varieties of European National Innovation Systems.” Working Paper 13/2018 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.

Wolfson, Michael. 2021. “What’s preventing Canada from creating a robust health data infrastructure?” *Policy Options*, May 4. https://policyoptions.irpp.org/magazines/may-2021/whats-preventing-canada-from-creating-a-robust-health-data-infrastructure/.

XinhuaNet. 2021. “China’s non-cash payments top 4,000 trln yuan in 2020.” XinhuaNet, March 27. www.xinhuanet.com/english/2021-03/27/c_139840050.htm.

Acknowledgements

The Reimagining a Canadian National Security Strategy project wishes to acknowledge the valuable engagement we have enjoyed with senior officials during working group discussions and the drafting of the report. The senior government liaisons who took part in discussions about the Emerging Technologies, Game Changers and Impacts on National Security theme and who consent to be acknowledged are:

- Stephen Burt, Assistant Deputy Minister, Data, Innovation, Analytics
- Martin Fontaine, Chief Research Officer, Communications Security Establishment, Government of Canada
- Scott Jones, Federal Lead, Proof of Vaccine Credentials, and Associate Deputy Minister of Immigration, Refugees and Citizenship Canada

Their involvement with the project does not in any way indicate their agreement in whole or in part with the theme report and their participation does not reflect any official Government of Canada policy or position.

The project wishes to acknowledge the valuable contributions made by working group members during discussions and the drafting of the report. The working group members who took part in discussions about the Emerging Technologies, Game Changers and Impacts on National Security theme and who consent to be acknowledged are:

- David Connell, Defence Scientist/Analyst, Concept Development and Experimentation, Canadian Forces Joint Warfare Centre, Centre for Operational Research and Analysis, DRDC
- Ian Gallagher, Vice President, Smart Transit and Infrastructure, BAI Canada
- Keith Jansa, Executive Director, CIO Strategy Council
- Meg King, Director of the Science and Technology Innovation Program, Wilson Center
- Jean Le Bouthillier, Founder and CEO, Qohash
- Annette Ryan, Deputy Director and Chief Financial Officer, Enterprise Policy, Research and Programs, Financial Transactions and Reports Analysis Centre of Canada
- Tony Seba, Co-Founder, RethinkX, and Author of *Clean Disruption of Energy and Transportation: How Silicon Valley Will Make Oil, Nuclear, Natural Gas, Coal, Electric Utilities and Conventional Cars Obsolete by 2030*
- Peter Suma, Chairman and co-CEO, Applied Brain Research -AI + Robotics
- Graham Taylor, Professor of Engineering, University of Guelph; Interim Research Director and Faculty Member at the Vector Institute
- Eytan Tepper, Research Coordinator and Adjunct Professor, Space Governance at the Graduate School of International Studies, Université Laval
- Davide Venturelli, Associate Director, Quantum Computing, Universities Space Research Association

Their involvement with the project does not in any way indicate their agreement in whole or in part with the theme report.

Centre for International
Governance Innovation

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