Centre for International
Governance Innovation

CIGI Papers No. 316 — March 2025

Artificial Intelligence and National Defence: A Strategic Foresight Analysis

Alex Wilner and Ryan Atkinson

Centre for International
Governance Innovation

CIGI Papers No. 316 — March 2025

Artificial Intelligence and National Defence: A Strategic Foresight Analysis

Alex Wilner and Ryan Atkinson

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
Director, Program Management Dianna English
Program Manager and Research Associate Kailee Hilt
Senior Publications Editor Jennifer Goyder
Publications Editor Christine Robertson
Graphic Designer Sepideh Shomali

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

Table of Contents

About the Authors

Alex Wilner is an associate professor at the Norman Paterson School of International Affairs (NPSIA), Carleton University, Ottawa, Canada. He is a leading scholar of contemporary deterrence theory and practice. His research — which explores the nexus between deterrence theory and emerging security considerations, domains and environments — has shaped the fourth, and now fifth, generation of deterrence scholarship. Among his more than two dozen journal publications, his articles on the subject of deterring terrorism and cyber deterrence have been published in top-ranked international relations journals, including *International Security, Journal of Strategic Studies, Security Studies* and *Studies in Conflict & Terrorism*. His books include *Deterrence by Denial: Theory and Practice* (eds., Cambria Press, 2021), *Deterring Rational Fanatics* (University of Pennsylvania Press, 2015) and *Deterring Terrorism: Theory and Practice* (eds., Stanford University Press, 2012).

Since joining NPSIA in 2015, his broader scholarship has been awarded more than $1.7 million in external research funding. Alex teaches classes on terrorism and violent radicalization, intelligence in international affairs, strategic foresight in international affairs and a capstone course on Canadian security policy. Besides his academic teaching, since 2017 he has trained more than 1,200 Canadian public servants in strategic foresight, having provided more than 45 multi-day training workshops to numerous government departments and agencies.

Ryan Atkinson is a post-doctoral fellow at Carleton University, supported by the Canadian Defence and Security Network. His research focuses on emerging technologies and defence policy. Ryan's career combines in-depth academic knowledge with hands-on experience in defence and security, including working alongside the international staff at the North Atlantic Treaty Organization (NATO). He previously managed the cybersecurity program for the NATO Association of Canada, where he worked on enhancing awareness and resilience initiatives. Additionally, Ryan has conducted cybersecurity assessments as a consultant on engagements with various organizations. He holds a Ph.D. in political science from Western University and an M.A. in the same field from the University of Toronto.

Acronyms and Abbreviations

1/33	January 2033
AAFC	Agriculture and Agri-Food Canada
ADF	Australian Defence Force
AFSPC	Air Force Space Program Command (US)
AGI	artificial general intelligence
AI	artificial intelligence
ANI	artificial narrow intelligence
ASI	artificial super intelligence
CBSA	Canada Border Services Agency
CFO	chief financial officer
CSIS	Canadian Security Intelligence Service
DDoS	distributed denial of service
DND	Department of National Defence (Canada)
DCDC	Development, Concepts and Doctrine Centre (UK)
DIY	do-it-yourself
DoJ	Department of Justice (Canada)
DPMC	Department of the Prime Minister and Cabinet (New Zealand)
DRDC	Defence Research and Development Canada
LLMs	large language models
MOD	Ministry of Defence (UK)
N-DAIC	North Dakota AI Control Framework
NATO	North Atlantic Treaty Organization
NIC	National Intelligence Council (US)
NPSIA	Norman Paterson School of International Affairs
NRCan	Natural Resources Canada
PHAC	Public Health Agency of Canada
RCMP	Royal Canadian Mounted Police
UASs	uncrewed aerial systems

Executive Summary

Strategic foresight can help address long-term uncertainties by offering insights into the potential impact of artificial intelligence (AI) on national security. This analysis highlights the value of qualitative tools in exploring a variety of future scenarios related to breakthroughs in AI. This investigation examines how strategic foresight is changing in Canada and other Five Eyes (plus one) nations — the United States, the United Kingdom, Australia, New Zealand and the Netherlands — using horizon scanning and scenario planning to improve security policies. Important observations centre on the dual nature of AI, exploring the difficulties presented by deepfake technology and cyberthreats while emphasizing the need for preventative regulatory actions to protect democratic institutions and national security. Various illustrative scenarios highlight the risks associated with unbridled AI capabilities, including the problem of incremental approaches, showcasing different degrees of AI integration for defence. Robust legislative frameworks and international cooperation are essential to control AI's impact, and strategic foresight provides a critical instrument to navigate upcoming possibilities and challenges in defence and security.

Introduction: Foresight, the Future of AI and National Defence

Strategic foresight is the systematic study of the future. It is both loved and misunderstood by casual observers and experts alike. It is loved because, at its core, foresight's very ethos rests on the simple truth that strategic surprise is a dangerous position in which to find oneself. Foresight's structured approach to thinking about medium- and long-term change and uncertainty can provide a solution to understanding and avoiding adverse developments. As a methodology with dozens of research tools and techniques, foresight promises us forward-leaning insights beneficial to our long-term survival and growth. The process allows for the systemic exploration of possibilities and trends that shape the future. Weak signals are identified as early indicators of potentially significant change, which inform multiple future scenarios covering a range of possibilities and reduce the risk of being surprised by unexpected events.

Foresight is often incorrectly conflated with forecasting, a related methodology with deep and well-regarded ties to economics and political science, mathematics and physics, computer and data sciences, management and business administration, Earth and climate sciences, and other disciplines. Forecasting, using the terminology of "prediction," promises insights on the near-term future — often from minutes to weeks to months ahead — anchored to quantifiable data, statistics, simulations and structured modelling. Foresight, by contrast, speaks of "anticipation," with promises of insights on the far future — usually years to decades to generations ahead — driven by qualitative observations, systems dynamics, informed intuition and a speculative and grounded accounting of change. A central difference is that prediction focuses on calculating and estimating likely future events given the current relevant data, whereas anticipation involves the preparation for a range of future scenarios with an emphasis on adaptability to uncertain futures.

If forecasting is admired as a methodology with a long and improving track record of success across various disciplines, foresight is famous despite itself.[1] Foresight proponents need to better explain themselves to more traditional scholars, as the approach still rests well outside the traditional bounds of the social scientific establishment (Fergnani and Chermack 2021). It can be challenging to learn and apply foresight quickly and efficiently (Webb 2024). Foresight is likewise agnostic at best, about the feasibility, desire and meaning of "success" when it comes to getting the future right (Bishop 2001). The point of foresight is to open our aperture, to become more aware of how change might unfold, rather than to accurately identify what will happen to whom on a particular date 15 years from now. Plausible criticisms target foresight's notion of data, given that there is no data from (or of) the future. Thus, the observations that animate foresight analysis are informed interpretations of contemporary dynamics, creatively and thoughtfully extrapolated into the future through imagination (Spaniol

1 See https://goodjudgment.com/about/.

and Rowland 2018). Recreating this type of data and analysis — as per the scientific method — can be a challenge, as can peer review.

Today, the medium- and long-term future of crisis, conflict and war will likely be marked by advancements in AI. AI introduces significant uncertainty, given the lack of understanding of the unintended consequences of such applications. The lack of established norms and regulations increases the risk of miscalculations or unforeseen escalations, making the threat landscape unpredictable. Recent classifications of AI suggest three broad categories: artificial narrow intelligence (ANI), artificial general intelligence (AGI) and artificial super intelligence (ASI) (IBM 2023). ANI is designed to accomplish specific tasks, such as identifying and cataloguing objects in pictures, playing complex, multi-player computer and strategy games, writing computer code and text, and directing swarming robotic platforms. Moreover, while AI outperforms humans at some well-defined and structured tasks, it does not yet have the capability for general problem solving, something still reserved for human intelligence (Larkin 2022). ANI systems cannot complete a task they are not programmed to "think" about. Still, current ANI impresses nonetheless. Generative AI systems, including large language models (LLMs) such as ChatGPT and content generators such as DALL-E, Kling or Sora, are a subset of ANI (Metz 2024a; Tobin and Metz 2024). Their algorithms identify patterns in reams of data, recognizing and building words, sounds and images around structured prompts. Deep-learning architecture enables the ability to generate outputs in various kinds of generation, including text, pictures and videos, among others. Leaping from one domain to another, the same technology might soon provide robotic systems with the ability to manipulate objects in physical space, as has been the observable case in manufacturing (Metz 2024b).

By contrast, AGI and ASI still live in the realm of science fiction and of a plausible (if not yet probable) near-distant future (Kuusi and Heinonen 2022). They refer to machines with human-like attributes in intelligence and reasoning, which are applicable across a wide range of tasks and domains with or without human prompts (Bostrom 2014). Over the coming years and decades, achieving either or both AGI and ASI constitutes the field's holy grail and nightmare scenarios, depending on your interpretation of the future, simplified as a spectrum regarding AGI and ASI to make sense of central debates within this space despite some mutually exclusive traits. Techno-optimists, who sometimes refer to themselves as "effective accelerationists," provide an idealist future of AGI and ASI that allows for civilization's next great leap across all domains at once. Techno-pessimists, those who refer to themselves as "doomers," warn otherwise, calculating that any AGI or ASI has a non-zero probability of purposefully or accidentally annihilating the planet, and everybody and everything living on it (Marantz 2024; Altman 2023). For most observers, AGI and ASI are still a long way off. Clearly, among opponents and proponents of AGI and ASI, fact meets fiction. This is the perfect environment in which strategic foresight shines.

Foresight Methodology: Weak Signals, Insights and Scenarios

Foresight is more art than science (Policy Horizons Canada 2018). Gut feelings matter to inquiry, despite such sentiments not sitting well with some critics (Mizsei 2023). Imperfect as it is, strategic foresight is nonetheless an essential tool kit for identifying, anticipating and responding to future change. Forecasting is a powerful tool for short-term projections. However, it suffers further into the distant future when the assumptions underpinning our understanding of change unravel. Forecasting needs to be equipped to identify or anticipate hidden shocks. Take the COVID-19 pandemic, for example. All the world's forecasts — from national inflation and housing stocks to women's employment rates and the happiness index — were proven suspect or inaccurate by early 2020 once the total weight of the global public health emergency became clear. We had entered underexplored territory where existing forecasts and frameworks told us little about the world we would eventually inherit.

By design, foresight is much better able to grasp and speculate about the importance of surprising developments. Foresight begins where forecasting ends, challenging contemporary assumptions about our future environment and our response to it by way of a series of tools, techniques and methods,

which provide a better appreciation of how over-the-horizon changes still years and decades in the making might unfold. It does so with an eye on identifying weak signals of change — contemporary events or developments that are weakly felt, weakly understood or both, that nonetheless portend a possible and plausible alternative future. Insights are assessed about the future against our understanding of the system dynamics that are in play. Foresight might not have anticipated the exact contours of the COVID-19 pandemic, but it certainly could have developed scenarios for what might be expected under these conditions of change (Policy Horizons Canada 2021; Global Affairs Canada 2018; Van Der Meer 2023; Cairns and Wright 2020).

As a formal analysis process, strategic foresight is usually punctuated by different and cascading research steps.[2] Most foresight projects start with a table-setting exercise, such as a domain map or framing process, that helps define and delineate the topic under study (Wilner and Stein 2025). Scanning for data by identifying weak signals and insights and developing change drivers of future change usually follows (Cuhls 2020; Honda et al. 2017). Data scanning involves actively finding information from numerous sources to identify early warning signs of change, also considered weak signals, which are trends or anomalies that can all signal future developments. The indicators of possible future change are then used to learn about potential future trends, disruptions or opportunities. Change drivers are then created from the weak signals and insights that depict underlying dynamics that influence future events. These gathered materials are analyzed and projected into the future using several different research tools so that foresight analysts can identify logical but surprising ways that contemporary developments might unfold in the medium and far future.

Analysts project a weak signal, insight or change driver into the future to capture how it might grow in importance and clout and affect change within (and beyond) the system under study. Finally, most foresight projects conclude by constructing alternative scenarios of the future — informed fictionalized accounts of our probable, possible, plausible and preferred futures — based on scanning material and its thorough analysis (Bishop, Hines and Collins 2007). Scenarios let us imagine how our organizations might respond to various competing future states, assisting our strategic planning and long-term policy making. Now, foresight's speculative and rigorous halves meet, inviting users to explore their institutional and decision-making assumptions, expectations and responses to emerging opportunities and challenges.

The strength of strategic foresight rests in its ability to help us think about the unthinkable (Urban and Kahn 1971).Its open and inquisitive acceptance of the many quirky and uncertain ways our future trajectories might shift, unravel or head off a cliff provides us with a means to question the continued truths and strengths underpinning our planning and operating assumptions. Set in the context of national defence policy against the backdrop of the emerging Cold War, American mathematician and think tank maverick Herman Kahn argued in his still-controversial bestseller, *Thinking About the Unthinkable* (1962), that governments had an obligation — in fact, a moral duty — to explore futures beyond the most probable, however horrible those futures might appear. With nuclear weapons proliferating among antagonist states, Kahn asserted that exploring "how a war might be fought" and won was a necessity for ultimately shaping our preferred future short of nuclear holocaust. Kahn's willingness to develop plausible, fictionalized scenarios about the future of war was tied to his belief in our collective ability to prevent undesirable developments while supporting and cultivating desirable ones.

This contribution has two purposes: to introduce readers to the promises (and pitfalls) of strategic foresight as it relates to the study of distant, alternative futures; and to provide a synopsis of the future of AI as it relates to democracy, geopolitics, conflict and warfare. The paper is structured in seven sections. These introductory sections situate the study of strategic foresight and introduces the topic of AI. The following section offers a summary of where and how the Government of Canada is currently applying foresight, providing a backdrop for better appreciating contemporary policy-driven foresight in the country. The third and fourth sections then summarize some recent foresight-related research on the future of defence, security and intelligence with an eye on emerging technology, produced by Canada's Five Eyes (plus one) partners in the United States, the United Kingdom, Australia,

2 The following description of the foresight process is built from the original, as presented in Marcovitch and Wilner (2024).

New Zealand and the Netherlands. The fifth section dives into the foresight process, offering several insights on the future of AI that were collated and curated using an original scanning process and by conducting two influence diagram workshops. That foresight analysis reappears in the sixth section, in which three alternative scenarios on the future of AI in defence are animated. Using a version of the archetype scenario construction method, numerous scenarios are given from which lessons are drawn, and the conclusion presents the next steps for thinking and responding to the future of AI in defence.

Foresight is a well-established methodology for medium- and long-term analysis to anticipate challenges and opportunities applied to AI in defence. The research puzzle concerns how to prepare for AI's unpredictable potential transformative impact in future defence scenario planning related to uncertainties surrounding AI advancement. To address this puzzle, this paper answers a research question on how strategic foresight methodologically can be applied to anticipate future impacts of AI on national defence with insights and scenario planning. This paper argues that strategic foresight offers a crucial yet underutilized methodology to understand the uncertainties posed by AI in national defence. Foresight provides a broader, more flexible framework to explore possible and plausible futures. The approach to identify weak signals and construct alternative scenarios provides policy makers with the tools to better prepare for and adapt to profound changes that AI brings to enhance situational awareness and reduce risks of miscalculation and escalation.

Highlights from Canada's Policy Foresight Ecosystem

Within Canada, where our research on public policy foresight is primarily based, strategic foresight is currently being applied across the federal public service by several government departments, institutions and agencies.[3] In fact, since 2015, Canada's foresight landscape has expanded a great deal (Wilner and Roy 2020; Prityi, Docherty and Lavery 2022; Calof and Colton 2024). The pace of experimentation quickened significantly starting in 2020, the result of the combined disruptive effects of the COVID-19 global pandemic, open hostilities in Eastern Europe and the Middle East, and the concomitant risks increased conflict and geopolitical uncertainty have had on global trade, energy and food security, counter-proliferation and the rules-based international order. Renewed interests in the long-term effects of climate change, diminishing biodiversity and ecosystem degradation have also played a role in rising foresight's profile.

At the centre of Canada's foresight ecosystem lies Policy Horizons Canada (referred to as Horizons), the government's foresight centre of excellence. Horizons has the mandate and means to think big over decades, untethered from the everyday challenges of Canadian policy making. It has a large and robust team of foresight experts, publishes regular pieces on various futures across all domains and has an international reputation Canadians should be proud of. Besides Horizons, several government foresight units and groups have likewise been created since 2015. Pre-eminent among them include the units at Global Affairs Canada, Defence Research and Development Canada (DRDC), the Standards Council of Canada (Marcovitch and Wilner 2024), Canadian Security Intelligence Service (CSIS), Canada Border Services Agency (CBSA), the Department of National Defence (DND), the Canadian Armed Forces, the Department of Justice (DoJ), the Public Health Agency of Canada (PHAC), Royal Canadian Mounted Police (RCMP), the Canada Mortgage and Housing Corporation, the International Development Research Centre (Reilly-King, Duggan and Wilner 2024), the Canada Revenue Agency, and Agriculture and Agri-Food Canada (AAFC).

Unlike Horizons, these foresight teams are usually relatively small, constituting between two and four foresight analysts. Most of their foresight efforts are specifically and narrowly tied to their

3 The following description of Canada's foresight ecosystem expands on the original published in Wilner and Roy (2020). The information herein is derived from Alex Wilner's personal and professional experience working with and supporting individuals and groups associated with these organizations since 2016. Other foresight initiatives may exist within the Government of Canada.

department's core mandates: the DoJ runs a project on the future of justice provision, AAFC on the future of agriculture, DRDC on the future of defence-adjacent technology, and so forth. Often, their foresight activities explore the near term, between five and 10 years out into the future, rooted in experiential research approaches, brainstorming sessions and stakeholder workshops, combining both foresight capacity-building and research efforts. These organizations seek to develop lasting foresight capabilities that will continuously feed specific departmental needs in medium- and long-term planning. Less structured foresight initiatives comprised of one-off foresight reports, pilot studies, training and experimentation have likewise emerged at several other Canadian government organizations, including the Canadian Foreign Service Institute, Environment and Climate Change Canada, Immigration, Refugees, and Citizenship Canada, the RCMP, Women and Gender Equality Canada, PHAC, Communications Security Establishment and at Cyber and Energy Security Policy and Outreach within Natural Resources Canada (NRCan).

These disparate units and teams often collaborate across the government through shared foresight training and scanning initiatives, other capacity-building efforts and information-sharing workshops, symposia and conferences, and have occasionally established more formal, pan-government thematic scan clubs. For illustration, the newly minted Centre for Surveillance, Integrated Insights and Risk Assessment, within the Data, Surveillance and Foresight Branch at PHAC, launched a foresight community of practice for all public servants interested in public health and pandemic preparedness. In 2023, CBSA launched a similar, cross-government thematic scan club on border and national security that attracts participants from Public Safety, DND, NRCan and Canada's intelligence community. Both initiatives meet semi-regularly (several times a year) and generate foresight-related material and empirical data useful for in-house foresight research. Canada's emerging web of public policy foresight has helped build a culture of future awareness and excellence across socio-cultural, political, economic and technological contexts (School of International Futures 2021).

The Five Eyes (Plus One) Defence Foresight: Observations and Lessons

National defence and security establishments worldwide use foresight to model joint operations, understand organizational challenges, project long-term goals and inform strategic decision making.[4] This literature review illustrates how the United States, the United Kingdom, Australia, New Zealand and the Netherlands use foresight to test, explore and guide national defence strategies while identifying possible future security risks, emerging geopolitical trends and operational requirements. Each report within this scope presents a range of future scenarios, from the worst-case outcome of strategic failure combined with nuclear proliferation and use, to the revitalization of international norms. The literature review captures how each national defence report implements foresight techniques to inform emerging security trends and implications, long-term strategic goals, possible future scenarios and policy recommendations. The reports stem from national security and defence organizations that occupy different roles within their respective national defence establishments, including the US Air Force Space Program Command (AFSPC) and US National Intelligence Council (NIC), the UK Ministry of Defence, the Australian Defence Force, the New Zealand Ministry of Foreign Affairs and the Dutch Ministry of Defence.

The United States

In 2019, the AFSPC published *The Future of Space 2060 & Implications for U.S. Strategy: Report on the Space Futures Workshop* (Office of the Chief Scientist 2019). Expert participants from the US Department of Defense, the National Aeronautics and Space Administration, the commercial sector, and academia contributed to this report. The workshop used the North Atlantic Treaty Organization's (NATO's) Strategic Foresight Analysis framework to understand how political, economic and technological trends could influence the future of US interests within the space domain. The workshop

4 The following section was supported by research produced by Talya Stein, Alex Wilner's student research assistant, while working on a larger comparative study of foresight efforts, techniques and tools from January to August 2024.

developed eight possible future scenarios as shaped by the upper and lower bounds of space power, human presence, potential commercial activity and US coalition leadership in space. The positive, negative and transformative future scenarios of space illuminate critical nodes of decision making the US government might consider in securing strategic space interests by 2060. The workshop report recommends that the United States develop a long-term national space strategy that addresses resourcing and securitization considerations for future strategic space missions. Furthermore, the report found that the government must support increased science and technological investments, craft policy and regulatory strategies to ensure that essential space technologies produce positive future outcomes in line with core US national defence and security interests.

The Future of Space 2060 includes eight distinct scenarios: Star Trek, Garden Earth and Elysium sit within the optimistic and expansive camp, exemplified by more US military leadership and commercial gains across the space domain. The pessimistic future scenarios are described in Zheng He, Wild Frontier and Xi's Dream, in which an alternate power, such as China, dominates the space domain in commerce, technology and defence. The last two scenarios explore futures informed by the military dominance of space. Space Today captures an optimistic future scenario wherein the US military coalition is the dominant power, and space itself serves as an arena for conflict and an essential component of integrated warfare. Dark Skies is the reverse, where another state and its allies dominate space to benefit their own (and competing) interests.

Every four years, the US NIC likewise publishes a lengthy foresight report that provides trends assessments and insights into the uncertainties that will shape the American strategic environment over the coming decades. NIC pairs its foresight practitioners and civil society consultation with a vast data set of scanning material to produce the report, which is regularly titled *Global Trends*. From a governance and policy-making perspective, each *Global Trends* report is usually published at the beginning of a new or incoming presidential administration, such that foresight is used to inform a new administration's strategic vision vis-à-vis emerging geopolitical uncertainty and security, defence and intelligence challenges.

The latest report, published in 2021, *Global Trends 2040: A More Contested World,* analyzes how structural forces are shaping demographic and human development, the environment, economics, and technology and suggests, in turn, their impact on US national interests and the prevailing international order. The report's scanning sections establish a baseline of the primary structural forces and plausible changes, subsequently informing the report's future scenarios. The report uses its structural trends analysis to illustrate future visions at the societal, state and international levels. Future scenarios are explored along the power axes of resurging open democracies, volatility in the international system, competitive coexistence, fragmented security blocs, and large-scale and innovative international cooperation. *Global Trends 2040* includes novel thoughts on shifting strategic alliances, US-China power competition, advancements in disruptive technology, non-kinetic warfare and influence, nuclear proliferation and other key change drivers shaping the future of conflict.

The latest *Global Trends* report includes five future scenarios, circa 2040, each guided by three key questions: "How severe are the looming global challenges? How do states and nonstate actors engage in the world, including focus and type of engagement? Finally, what do states prioritize for the future?" (NIC 2021, 108). In exploring these guiding questions, three of *Global Trends*' five future scenarios exist along a backdrop of worsening US-China relations. The most volatile and hostile scenario, Competitive Coexistence, depicts a world where the United States and China compete head-to-head to lead a bifurcated and highly divisive world. The other two scenarios in the set explore radical future changes that challenge the NIC's core assumptions about the functioning of the international system. In Separate Silos, economic, regional and security blocs emerge, ad hoc, out of the remnants of globalization to protect states from external shocks and threats. In Tragedy and Mobilization, the report's transformative scenario, revolutionary geopolitical change occurs because of a catastrophic global "food catastrophe" spurred on by climate change and ecological degradation. The remaining two scenarios provide a more hopeful outlook: The Renaissance of Democracies occupies the most optimistic position, with the United States leading a global resurgence of democratic countries, allies, partners and institutions. A World Adrift offers a future scenario in which China remains a leading state but fails to become a global and disruptive hegemon.

The United Kingdom

The Development, Concepts and Doctrine Centre (DCDC) within the UK Ministry of Defence (MOD) uses evidence-based strategic foresight to inform governments and international organizations about emerging military insights and possible security implications. The DCDC's report, *Global Strategic Trends: The Future Starts Today*, published in 2018, provides the UK government with a systematic exploration into possible futures, potential disruptions and strategic imperatives using a variety of foresight methods, in-depth academic literature review, stakeholder workshops, interviews with subject-matter experts and research papers from across 42 institutions. *Global Strategic Trends* analyzes emerging thematic disruptions across various domains, including the environment and resources, human development, economics, industry and information, governance and law, and conflict and security. Each thematic trend offers a snapshot of plausible alternative outcomes through a future lens. The report identifies indicators of weak signals, called "watch points," and change drivers, called "discontinuities." The report identifies influential weak signals shaping the future of conflict and security by analyzing levels of cooperation in conflict prevention and disaster relief, legal constraints on the use of novel technologies, adherence to arms control treaties, the rise in confrontational nationalistic policy positions, global defence spending and the emergence of unregulated and privatized security providers. *Global Strategic Trends* outlines 10 detailed security implications and considerations for the MOD, including discontinuities such as global conflict, the collapse of critical multilateral organizations, a decline of US military pre-eminence and the rapid proliferation of weapons of mass destruction that pose as transformative flashpoints for future conflict, national defence and security.

Unlike the American foresight examples above, the MOD report uses a two-by-two scenario matrix to develop plausible alternative future scenarios as influenced by the distribution of power, level of cooperation, powerful states and level of competition. Each scenario dissects the state of the trending structural themes analyzed in the horizon scan. The variable matrix produces different future scenarios in each of its four quadrants, including Multilateralism, Multipolarity, Network of Actors and Fragmentation. Resting within the upper quadrant of powerful states and cooperation, Multilateralism offers a future scenario in which states are the key actors and cooperate to address global challenges through multilateral institutions and channels for global governance. Conversely, in a competitive future ruled by powerful states, Multipolarity organizes blocs of cooperation and competition for global power and leadership. Moving down the scenario matrix, the Network of Actors is at the intersection of cooperation and diffusion of power, where non-state actors address global governance and challenges. The last scenario, Fragmentation, explores a future dictated by the diffusion of power and competition, in which "states, corporations, megacities and other non-state actors, including organized criminal and dissident groups, compete for power" (DCDC 2018).

Australia

The Australian Defence Force (ADF) uses strategic foresight to inform national security decision making and the military's operational needs. The ADF report, *Future Operating Environment 2035*, outlines a regional scope for its horizon scanning, accounting for Southeast Asia, Papua New Guinea and the South Pacific. The report's scope is regional, partly because Australian defence interests are primarily in the Indo-Pacific region. *Future Operating Environment 2035* is an initiative that meets the "Defence White Paper's" request for strategic defence interests to address future military challenges. This report provides context for the Future Joint Operating Concept tasked with providing force design solutions to national security. The ADF report addresses the adaptation needs for command and control, situational understanding, force projection, application, protection and generation, and sustainment to address warfighting in the future operating environment. The ADF identifies people and culture, climate and resources, economics and governance, geopolitical trends and technology as the seven broad drivers shaping the security horizon. The report outlines contexts of future conflict and opportunities and challenges for Australian regional security. The report identifies advanced technological change as the dominant change driver for conflict conduct and the ADF's ability to achieve strategic warfare objectives.

Like the United Kingdom's MOD report, the ADF report guides its future scenario exploration in a double-variable approach with Westphalian primacy, diffusion of power, cooperation and competition on its axes. The double-variable matrix approach produces four different future scenarios of Australian regional security as led

by multilateralism, multipolarity, a network of actors and fragmentation. The Multilateral World explores a future where states remain the most influential players in the global system and cooperate to achieve strategic interests. The Multipolar World depicts a future context where states are the key actors, and high levels of competition dictate international relations. The Networked World portrays a future scenario where states and non-state actors cooperate in a non-polar and unpredictable global order. The last scenario, Fragmented World, depicts a future shaped by competition between state and non-state actors in a race to shape the global order toward individualized strategic interests.

New Zealand

Under the Public Sector Act 2020, New Zealand's Department of the Prime Minister and Cabinet (DPMC) publishes "Long-term Insights Briefings" every three years. The 2019 terrorist attacks on the Christchurch mosques served as a turning point for the government to reconceptualize strategies for anticipating complex, surprising future national security risks. The briefings are an institutional mechanism that ensures the New Zealand government develops the anticipatory capacity to steward the next generations into a more secure and prepared future. They also provide Parliament with an assessment of future trends, risks and opportunities to explore. In 2023, The DPMC and the Ministry of Foreign Affairs and Trade published the "National Security Long-term Insights Briefing" on behalf of the Security and Intelligence Board. The briefing analyzes how the shifting trends of disinformation, cyberattacks, transnational organized crime, foreign interference, terrorism and violent extremism, and regional resilience could impact national security and defence over the next 15 years. Surveying public respondents and consulting with civil society and academia serve as the methodological backbone for the report. The research methodology provides DPMC and the Ministry with a greater understanding of how national security risks, challenges and opportunities are received by New Zealand constituents. The briefing employs a horizon-scanning technique to identify global trends, including increasing competition, technology change and climate change (which, interestingly, includes global pandemics). To better prepare and respond to possible looming national security concerns, the briefing provides a list of recommendations for national security agencies to adopt to strengthen collective stewardship, engage in proactive intelligence sharing with strategic allies, and work toward diversifying the skills and backgrounds of defence personnel.

Three hypothetical future scenarios are packaged into the report. The scenarios explore New Zealand's security environment, considering continued global decline, dramatic decline, and an optimistic and improving outlook. A future of continued decline portrays a world shadowed by competing interests, deterioration in the global order, increased likelihood of direct interstate conflict and a rise in social inequity and dis- and misinformation. A future dramatic decline explores open and lasting conflict in Ukraine and the Indo-Pacific region, the looming threat of nuclear weapon proliferation and repeated use, catastrophic cyberattacks on critical infrastructure, climate disasters and shocks, all emerging at once against a backdrop of diminished state and institutional capacity. The optimistic and improving outlook for the future captures a world fuelled by global cooperation meant to address collective action problems, technological innovation and resource sharing among disparate players, and greater transparency and public trust.

The Netherlands

The Dutch Ministry of Defence partners with foresight experts from the Hague Centre for Strategic Studies and the Netherlands Institute of International Relations Clingendael. With these partnerships, the Ministry of Defence published a long-term strategic defence report in 2020 titled *Defence Vision 2035*. The *Vision* report uses foresight methods to assess the Dutch armed forces' preparedness and response capacity, and to establish critical areas for improvement. A horizon scan informs the report's threat analysis profile of geopolitical power shifts, economic trends, climate developments and emerging security threats. The insights gathered from the threat analysis profile address cybersecurity attacks, geopolitical volatility, vital infrastructure vulnerability, chemical, biological, radiological and nuclear weapons proliferation and military expansion of adversarial forces, and transnational terrorism. After assessing the threat analysis profile, the report lays out its examination of problems and puzzles within the context of the armed forces, namely revolving around a lack of strategic information, personnel and resource shortage, and a restrictive culture of adaptability. To address the gaps between the threat

analysis profile and problem analysis, *Defence Vision 2035* outlines steps to achieving its 10 organizational design principles and financial goals to be adopted by 2035, some of which include increasing personnel, developing multidomain and integrated operations, and further defence specialization within NATO and the European Union.

The report explores the five most probable future national defence deployment scenarios to better understand the possible future security challenges the Dutch Ministry of Defence and armed forces should prepare for. The first highlights cases in which a civil war in a North African country sparks irregular European migration, transnational terrorist attacks and a joint military intervention. The second scenario explores a deteriorated security environment that leads to a hybrid attack targeting the Netherlands with a strategic goal of placing increased pressure and splintering the NATO alliance. The third depicts an attack on a NATO ally wherein the territory of a NATO ally is invaded and suffers a strategic defeat. The fourth scenario captures a crisis in the Caribbean that results in riots, large numbers of fleeing refugees and trafficking of drugs by international gangs. The last scenario portrays Arctic developments against a backdrop of runaway climate change, in which the Netherlands faces increased geopolitical risk. At the same time, Arctic melting opens the arena to greater competition and conflict across the Baltics, the Atlantic and the North Sea as states compete for access to natural resources and reserves.

This review has explored these reports' organizational purpose, themes, trends, weak signals and snapshots of select future scenarios to better illustrate how each case study uses foresight to improve contemporary national defence. Insights gleaned from the case studies cultivate an understanding of the usefulness of foresight in the national defence sector, long-term policy planning and emerging change drivers. The following sections will outline how strategic foresight has been used to approach questions related to AI and defence and will provide specific lessons for discussion from individual state applications of foresight methodology to applied AI research.

AI Weak Signals and Insights: Deepfakes, Cyberthreats and Warfare

Advancements in AI challenge policy makers to address risks over the next 15 years, let alone the next five. Strategic foresight provides tools to address the opportunities and risks of novel AI applications. The following section will detail numerous weak signals or trends that allude to future developments as indicators of future change and provide insights on current AI security challenges, opportunities, and threats. Weak signals and insights create change drivers that depict underlying dynamics influencing future discussions. The section is organized into three categories focused on applications of AI deepfakes, cyberthreats and warfare. The insights provide an actionable understanding of trends, data and patterns for new perspectives on the underlying dynamics of emerging trends. These insights provide the basis for policy development focused on emerging AI challenges. Each insight includes at least three weak signals as early indicators of potential change. The three categories provide numerous examples of AI applications that have emerged in recent months and years. These categories benefit focused research into the critical focus areas seeking to anticipate further change factors, including cases involving state and non-state actors. These cases are chosen based on weak signals and insights observed, categorized to depict central themes: deepfakes in elections, cybercrime of language models and AI in warfare.

Deepfakes and Elections

The proliferation of deep learning for fake images and audio observed in recent elections demonstrates unprecedented developments targeting public opinion. Deepfakes can influence voters, defame politicians, target support or criticism toward political candidates and create other political campaign materials. The following section will detail a timeline of selected observations of AI applied to political election campaigns since the public release of ChatGPT in November 2022 to the end of the summer of 2024. A global surge in deepfakes has targeted politicians internationally using US-

based technology, highlighting the urgent need for regulations on the emergence of AI-generated deepfakes threatening democratic institutions. In August 2024, then-US presidential candidate Donald Trump posted AI-generated content on social media that falsely claimed that Taylor Swift had endorsed him for president (Shafer 2024). Additionally, Trump posted AI-generated images that depicted Vice President Kamala Harris at the Democratic National Convention with communist flags (Liddell 2024). These incidents mark specific cases sparked by widespread criticism and highlight the worrisome ability of deepfakes to propagate false information during political campaigns. These examples are the first of numerous cases involving generative AI during political elections.

In June 2024, deepfake-generated political campaign materials were used during India's presidential election. These materials involved creating video and audio of the late Indian politician and cinematic icon, Muthuvel Karunanidhi, who endorsed politicians T. R. Baalu and M. K. Stalin in various public appearances (Christopher 2024). This case of a resurrected former politician was used to support ongoing campaigns of current politicians, representing a specialized domestic industry that has used the technology of foreign firms. For instance, Polymath Synthetic Media Solutions reportedly developed five deepfakes during the political election, charging US$720 for an "audio clone" and US$1,500 to make a "digital avatar" (Christopher and Bansal 2024). A second firm, IndiaSpeaks Research Lab, used AI deepfakes to create robocalls with the voice of politician J. Jayalalithaa, creating 250,000 personalized calls. The commercialization of AI deepfake technology represents the rise of specialized companies providing services in demand for political campaigns. In February 2024, a third case in Indonesia involved "resurrecting" the late President Suharto in video and audio, featuring the late military ruler's cloned voice and face (Chen 2024). The media was first published by Erwin Aksa, deputy chair of Golkar, the country's largest and oldest political party, receiving 4.7 million views on X (formerly Twitter) before spreading to Facebook, YouTube and TikTok. AI-generated deepfakes are increasingly frequent and underscore the risks of misinformation in influencing contemporary media environments. The extensive distribution of AI-generated videos highlights the lowered bar for malicious actors to stoke division of public opinion to target democratic processes.

In February 2024, deepfake audio disrupted Slovakia's presidential election campaign. In the lead-up to the election, audio clips spread online and suggested that the leader of Slovakia's Progressive Party manipulated voters at polling stations and was about to raise beer prices (Devine, O'Sullivan and Lyngaas 2024). The audio clip originated on Telegram and soon spread on Facebook, YouTube, TikTok and other social media platforms. During this same month, imprisoned former prime minister of Pakistan, Imran Khan, wrote AI speeches to campaign online from his cell. Written speeches were provided to his lawyers and converted into AI-generated speeches for online rallies on media platforms (Reuters 2024). The Khan campaign used the American firm ElevenLabs to create three clips of him delivering campaign speeches. AI technology provided the means to circumvent physical barriers such as imprisonment to generate speeches for campaigns that can be turned into audio of the candidate and used for campaigning. In December 2023, deepfake videos targeted Moldovan President Maia Sandu following local elections in November, and just prior to the traditional presidential New Year's address (Necsutu 2023). The video originated on the Telegram channel "Sandu Official," which spread on social media, falsely depicting Sandu mocking citizens' living standards. Some consider Moldova's presidential election in October 2024 to have been a referendum on membership in the European Union, while Moldovan opposition leaders called for closer ties with Russia and China (Tanas 2024).

The malicious use of deepfakes can discredit politicians and sway public opinion, emphasizing the importance of maintaining electoral integrity and public confidence. In January 2024, deepfakes targeted Taiwan's presidential election, spreading disinformation against Vice President Lai Ching-te and outgoing President Tsai Ing-wen, including rumours that Taiwan was about to establish an American biological weapons lab (Dotson 2023). AI video and audio suggested Lai was endorsing Beijing-friendly opponents (France 24 2024). Central to the disinformation campaign was a 300-page ebook, which portrayed Tsai as a corrupt dictator (Wenhao 2024). During the same month, AI disinformation was used to shape political discourse in Bangladesh's election, where pro-government media shared AI-generated news clips in the months leading to the country's general election. Deepfakes made it seem like the opposition leader was hesitant to commit aid to Gaza despite widespread public

support for Palestine in a majority Muslim nation. The American firm HeyGen was used to make the clips and upload them online. It was reportedly involved in creating AI avatars for US$24 a month (Parkin 2024). The troubling trend of deepfake disinformation highlights using generated news snippets to advance political agendas. AI tools are widely accessible and reasonably priced, suggesting a lower barrier to entry for creating misinformation campaigns and influence operations.

AI can, in fact, support politicians in reaching a broad audience as political campaigns facilitate enhanced approaches to tailored voter engagement. For instance, in November 2023, generative AI was used in numerous campaign materials during Argentina's presidential race. The two front-runners in the election produced political campaign materials using generative AI tools. Sergio Massa allegedly used the following prompt to create campaign posters using generative AI: "Sovietic political propaganda illustration by Gustav Klutsis featuring a leader, Massa, standing firmly…symbols of unity and power fill the environment…the image exudes authority and determination" (Nicas and Herrera 2023). Javier Milei, now president of Argentina, posted pictures of Massa as a communist dictator and of himself as a cartoon lion, which reached over 30 million views. The growing use of AI in political campaigns makes it easier to create visually striking and politically charged campaign materials.

Beyond campaign materials, further examples have involved developing an AI political candidate chatbot that interacted with voters during the campaign. In November 2022, the same month ChatGPT was released to the public, an AI chatbot in South Korea was used for political campaigning. Employees of Yoon Suk-yeol, then-candidate for the People Power Party and now President of South Korea, created a digital persona for the campaign, recording "more than 3,000 sentences — 20 hours of audio and video — to provide enough data for a local deepfake technology company to create the avatar" (*The Straits Times* 2022). These innovative developments of AI chatbots for campaigns and deepfakes have become prevalent in recent electoral campaigns globally, threatening electoral integrity with disinformation, eroding public trust in democratic institutions and spreading convincing false information. Increasingly sophisticated models are lowering the bar for malicious actors to spread misinformation. Deepfakes are a growing industry to meet increasing demand focused on political campaigns, suggesting the need for regulation to address the misuse of AI deepfakes. These cases demonstrate the need for policy makers to develop proactive strategies to counteract AI-generated misinformation. Public awareness, training and education will support the critical investment needed to advance technology and neutralize false information before it spreads widely.

Cybercrime and Language Models

This section focuses on the nexus between cyberthreats and AI. A worrying trend in the cyberthreat landscape involves the increasingly widely available tools that cybercriminals can use, which means that cybersecurity professionals face new hurdles as AI applications are adapted to organizations with untested consequences. AI-powered phishing and social engineering techniques proliferate to demonstrate the growing sophistication and accessibility of tools used by cybercriminals. These include examples of AI deepfake fraud, which manipulates social trust to trick victims into making fraudulent transactions. In May 2024, the British design firm Arup was targeted by AI deepfake fraud against the chief financial officer (CFO) and other employees at the firm's Hong Kong office, transferring US$25.6 million to the fraudsters through 15 bank transfers (Magramo 2024). The employee "initially suspected he had received a phishing email from the company's UK office, as it specified the need for a secret transaction to be carried out. However, after the video call, the worker put aside his doubts because other people in attendance had looked and sounded just like colleagues he recognized," including those he believed to be the firm's CFO and other staff (ibid.). This case of AI deepfake fraud highlights the increasing complexity of cyberthreats. Attackers can get away with fraudulent transfers by using convincing audio and video to mimic chats. For instance, an AI face-swapping scam in China cost a man US$622,000 when AI deepfake technology was used to trick him into transferring the funds to what he thought was a friend. The assailant used "AI-powered face-swapping technology to impersonate a friend of the victim during a video call," and the victim believed that the friend "needed to make a deposit during a bidding process" (Reuters 2023). Trust in a familiar voice or face is no longer enough for authentication because it is possible to counterfeit someone's face and voice.

This pattern indicates the increased challenge of guarding against AI face-swapping fraud.

AI was reported in May 2024 to have created polymorphic malware, which can change itself each time it replicates to infect a system, hiding its payload while maintaining the same malicious capabilities (De Angelo 2024). Researchers at CyberArk used ChatGPT to create polymorphic malware that could mutate code to create multiple versions with little effort and investment (Shimony and Tsarfati 2023). AI-powered polymorphic malware can mutate itself, making it increasingly difficult for cybersecurity professionals to identify and remove. In May 2024, a 25-year-old civilian was arrested in Kawasaki, Japan, using generative AI tools to create malware-like ransomware that encrypts computers held for ransom. He was arrested before the malware could be implemented and was not a malware expert, reportedly learning to create malicious code using AI tools (*The Japan Times* 2024). Non-technical individuals acting alone can use generative AI to support malware development, suggesting medium-term challenges as democratized tools empower amateur threat actors to make potentially significant strategic effects. The implications of this observation for the medium and long term remain unknown.

By July 2023, the malicious LLM FraudGPT was advertised on Telegram and the dark web as an "unrestricted alternative to ChatGPT" (Erzberger 2023). The price of the subscription model ranged from US$90–$200 monthly, US$230–$450 for three months, US$500–$1,000 for six months and US$800–$1,700 for 12 months. The product is described as a tool for creating "undetectable malware, writing malicious code, finding leaks and vulnerabilities, creating phishing pages, and learning hacking," with a demo video advertising its use for phishing (ibid.). FraudGPT represents a concerning progression in the availability of advanced cybercriminal instruments despite popular AI systems imposing usage limits and ethical requirements. WormGPT emerged at this time, transforming access to cybercriminal tools. Researchers at cybersecurity firm SlashNext revealed WormGPT was for sale on a hacker forum as "a blackhat alternative to GPT models, designed specifically for malicious activities" (Kelley 2023). Researchers tested the tool by instructing WormGPT to "generate an email intended to pressure an unsuspecting account manager into paying a fraudulent invoice" (ibid.). WormGPT can "create any malware and anything else without restriction… making easy money creating anything with it" (Chan 2023). A variety of subscription models "assist cybercriminals to create code for malware and phishing attacks…with various subscription models ranging from approximately US$112 to US$5,621" (Deloitte 2024). WormGPT represents a substitute for reputable GPT models, demonstrating increased tool sophistication and lowering the entry barrier to cybercrime.

DarkBard is another example of an affordable AI tool for cybercrime, advertised on underground forums to allow "threat actors to create fake news and deep fakes to spread false information, launching distributed denial of service (DDoS) attacks, ransomware operations, and other cyberattacks, writing malicious codes and scripts to create malware, detecting and exploiting vulnerabilities and database leaks, accessing communities, forums, and websites that are hidden from the clear web" (ibid.). DarkBard is also structured as a subscription model, advertised at US$100 for one month, US$250 for three months, US$600 for six months, US$800 for 12 months and US$1,000 for a lifetime (ibid.). DarkBard marks the beginning of a concerning trend to commoditize AI tools designed illegally without guardrails. In January 2023, researchers at WithSecure Labs demonstrated the use of generative AI to craft prompts designed to write tailored social engineering emails and email threads for credibility between the victim and assailant (Patel and Sattler 2023). Every time a prompt is generated, it creates new, unique and grammatically correct messages. Generative AI can overcome language barriers in phishing campaigns. Linguistic competence will also be less of a barrier as phishing attempts grow increasingly sophisticated and challenging to identify. Generative language models write grammatically sound and contextually relevant content, adding heightened hyperrealism to fake content.

AI Applications in Warfare

AI has been applied to warfare in several ways under discussion, including a focus on uncrewed aerial vehicles and drone swarms. Notably, having an AI system does not automatically mean that the system is autonomous. AI can have numerous applications requiring human oversight, decision making or control. These examples focus on AI applications in warfare and do not suggest these systems are thereby autonomous. In October 2023, Palantir's AI technology boosted Ukraine's

demining efforts. Palantir signed an agreement with the Government of Ukraine to use its AI-powered technology for demining efforts (Ministry of Economy of Ukraine 2023). Palantir and the Ministry of Economy of Ukraine built the software to help the government prioritize resources for demining capabilities across Ukraine. One example involves mapping "new demining methods — such as drones and unmanned vehicles — against traditional methods to determine which would be more appropriate for an identified area" (Business Wire 2024). The partnership between Palantir and the Ukrainian government involves the firm's AI platform leveraging data from cutting-edge and conventional techniques, to optimize demining operations customized to specific regions.

AI-powered uncrewed aerial systems (UASs) represent dramatic changes in warfare, with examples of how AI can handle complicated combat situations, including drone swarms and autonomous military aircraft. AI-powered UASs are used for military and recreational purposes, demonstrated by converting recreational drones into weapons, suggesting dual-use risks. In February 2024, AI-controlled drone swarms have been observed in recent wars, with militaries advancing autonomous weapons systems to operate as swarms with increased coordination, intelligence and speed (Klare 2024). For instance, US Air Force Project Venom is part of the 2024 budget allotted US$50 million to "perform a variety of missions, including striking enemy targets, conducting surveillance, jamming enemy signals, or even acting as decoys" (Losey 2023). Self-governing systems exhibit improved synchronization, intelligence and speed, suggesting a future of military operations where minimum human intervention is required. This indicates a strategic shift toward using AI and robots to collaborate with industry and push the limits of what autonomous AI can accomplish.

AI-powered drone warfare in Ukraine granted the ability to manoeuvre over rugged terrain, and partnerships between American industry and the Ukrainian government demonstrate how AI can improve resource management and demining operations. For example, in March 2024, AI-enhanced Ukrainian drones were used for precision strikes and "machine vision" targeted Russian energy plants (Cotovio, Sebastian and Goodwin 2024). A Ukrainian drone strike targeted Russia's energy infrastructure using long-range drones at targets 500 km from Ukraine. Drone capabilities have integrated "a basic form of [AI] to help them navigate and avoid being jammed," a source close to Ukraine's drone program reported to CNN (ibid.). The source added that "accuracy under jamming is enabled using [AI]. Each aircraft has a terminal computer with satellite and terrain data… the flights are determined in advance with our allies, and the aircraft follow the flight plan to enable us to strike targets with meters of precision" (ibid.).

AI has improved the operational capabilities of unmanned systems, suggesting a future where military operations increasingly depend on autonomous technologies. In March 2024, Ukraine leveraged AI to eavesdrop on and analyze Russian communications. Ukraine used AI to listen to Russian radio communications, which "automatically captured, transcribed, translated and analysed using several [AI] algorithms developed by Primer, a US company that provides AI services for intelligence analysts" (Knight 2022). Primer's tool carries out novel tasks involving "using natural language processing technology to analyse Russian military communications that are especially novel" (ibid.). Ukraine's use of AI emphasizes essential information pertinent to the battlefield to provide real-time, actionable insights to capture audio from web streams and learn to identify the military language.

In March 2024, a do-it-yourself (DIY) AI drone was created as an innocent game-turned-lethal weapon in hours. In a post to X, entrepreneur and scientist Luis Wenus (2024) explained how he built a drone as a game "that chases you around… the drone is programmed to fly…at full speed as soon as it detects someone. This took a few hours to build…you could easily strap a small number of explosives on these and let 100's of them fly around…I was also able to add face recognition to it." A seemingly harmless AI-powered drone designed as a game can quickly be turned into a fatal weapon. It may be the case that ammunition and other armaments to weaponize this drone may be hard to come by, yet the ability for terrorists to use everyday items to create explosives covertly demonstrates the danger when combined with this DIY UAS. Multi-purpose drones intended for recreational purposes can easily and quickly be modified into lethal weapons that could target specific individuals using facial recognition.

Some central observations from this section provide general lessons on the capabilities of autonomous systems to perform high-precision tasks with minimal human intervention. Dual-use technologies

pose significant risks for civilian technologies to be converted and used as weapons. Combined efforts for collaboration between the military and industry will drive innovation to ensure the development of cutting-edge technology tailored to specific military needs. Robust regulatory frameworks must address ethical concerns, prevent misuse and ensure compliance with international laws and norms. AI is reshaping modern warfare, and autonomous technologies will likely play a central role as military strategies evolve to incorporate emerging applications of AI-driven systems.

AI Scenarios: Futures in Defence and Security

In foresight, scenarios help readers and users accomplish a great many things. They provide a way to imagine and explore a future environment on multiple levels of analysis from their personal, institutional, national and international perspectives. They help identify future challenges and opportunities, focusing our collective attention on core considerations that help circumvent the worst that the future may bring. Scenarios spur further research, debate and action by encouraging readers to explore different contexts in which we might subsequently find ourselves. Future-proofing contemporary policies, strategies, processes and expectations is prioritized so that we survive and thrive among divergent and complex futures. Structurally, scenarios provide a way to package a great deal of scanning material and analysis into a practical, relatively small and accessible deliverable.

Scenarios usually represent a foresight report's flagship findings. They provide foresight practitioners with a way to communicate complex (and, at times, unappealing) results about the future to audiences that may know little about foresight or, worse, are inherently skeptical about its utility in policy thinking and making. This report adopts an archetypal scenario construction approach to create distinct future scenarios capturing the range of outcomes. The scenarios are archetypal, representing fundamental patterns or themes to explore the dynamics of uncertainty and change. These scenarios will depict the future of AI and defence to highlight several further examples worldwide.

While many different archetypes exist, the gist of the process is to anchor alternative scenarios to a core narrative structure or framework, and to flesh out the storyline using fictionalized accounts of the scanning material and foresight analysis.

Strategic foresight uses weak signals and insights to systematically construct scenarios to identify, analyze and extrapolate early change indicators. Weak signals are subtle, often ambiguous cues that suggest potential future developments that are not widely recognized or understood. They can be early warning signs of possible future changes, materializing as unique behaviours, innovations or emerging trends. The weak signals and insights from the previous section were clustered, based on commonalities that reveal broader trends and change drivers, which are condensed into broader themes to determine their possible influence. This approach scrutinizes various signals to uncover potential synergies or conflicts among emerging trends and create possible scenarios using these weak signals' insights. Scenarios explain what might happen and cover a range of potential futures, thereby helping to determine future strategic implications.

Each scenario follows a similar structure: A brief introduction sets up the background of the fundamental forces and uncertainties that are driving significant trends. The scenario narrative timeline involves a beginning, middle and end. The strategic implications are addressed to derive lessons from the scenarios based on the weak signals and insights detailed in the previous section. This approach allows for comparative scenario analysis, which includes elements and strategies across various potential futures. Three scenarios are presented below, circa 2040, hewing to the muddling through, worst case and transformative archetype scenario constructs.

Scenario 1: Muddling Through — The Humbling of the Machine

Narrative

It is spring 2040 and peak AI has set in.

After three decades of explosive growth, AI has proven its utility across various fields, disciplines and domains. However, its runaway progress has definitively stalled, mired by over a decade in which seemingly sophisticated AIs continue to hallucinate, fabricate impossible findings and otherwise fail to provide much utility to their users. Disinformation has given way to non-information: some academic studies posit that nearly 75 percent of the information collated by the world's leading internet search engines includes false, misleading or fabricated content. Not without reason, *The Economist*'s phrase of the year for 2038 was "AI farts," a noxious blend of algorithmically fabricated nonsense and technical glitches too silly to cause harm but too hilarious to pass up. Where AI failures were once deemed a potentially calamitous affair, today, they mostly elicit a few knowing chuckles. That is not to say AI technologies have not proven some worth. Indeed, they certainly have. All functioning governments and sophisticated militaries have come to rely on AI for peripheral and less-sensitive tasks, including training, recruitment, retirement and veteran affairs; automated cybersecurity; equipment maintenance and repair; translation, graphic design and writing; logistics; and other back-office activities. AI shines at these well-defined, incredibly tedious tasks. However, AI is given a back seat for truly complex and potentially life-altering tasks.

Most significant militaries, for instance, do not trust AI to act as promised or provide what is intended. Beyond AI, militaries worldwide are struggling with the issues of trust and culture, which constitute a significant challenge in adopting new technologies within the armed forces. For example, nuclear command-and-control systems and structures are ancient and still rely on legacy systems from the Cold War era. But AI technology is not trusted enough; many believe it may introduce more vulnerabilities to nuclear deterrence. Long sensitive to machines, weapons platforms and other systems that will not function as needed when required, the world's leading militaries largely shun AI in intelligence analysis, targeting, strategic planning and other complex tasks. As Canada's new Chief of Defence Staff General Lucy Jacinthe Nassif, noted colourfully at the 2039 NATO Summit in Yellowknife, NWT: "We don't trust guns that won't shoot, drones that won't fly and satellites that won't communicate. We sure as hell aren't going to trust AI that falters and fails, time and time again." So, while militaries around the world have leveraged AI to recruit, equip and train more soldiers and better care for their wounded and have otherwise automated some logistics and maintenance activities, a premium has been placed on human innovation and wit in all things related to intelligence analysis, military planning and strategic planning. When used carefully and judiciously, AI has made some militaries, including Canada's, much more efficient. When used carelessly, as Azerbaijan found out the hard way during the opening phase of the Third Nagorno-Karabakh War, it can needlessly complicate relatively simple tasks, slow down a military campaign and otherwise put troops in harm's way.

It is not that the high-tech industry is not trying to improve its wares. They are, but they have also realized that AI hubris has hurt their bottom line. Most major data-centric companies have moved on to perfecting quantum engineering and blockchain technologies, which they (now) promise will combine to "revolutionize computing for generations to come," as one leading tech maven pledged during Davos 2037. In the meantime, and until then, the slowing pace of AI development has left states and regulators with the time they need to make significant headway in finally building geopolitical and public-private sector consensus on the development of international norms and institutions for the ethical and fair use of AI. Green shoots of success were apparent to all at the 2036 AI Safety Summit in Bengaluru, India, during which the United States and China agreed to several key initiatives. Some redistribution of wealth has since followed. In Estonia, for example, commercial entities who have long benefitted from the automation of some jobs and sectors — notably, notaries, accountants, traders, artists and computer coders — have agreed to pay citizens of the country a small but fixed yearly income. The program has proven exceptionally successful, stabilizing society in ways that have bolstered support for democracy, good governance and political fairness. Thus, while geopolitical turmoil has and will continue to lead to

periodic episodes of crisis, conflict and — at times — open hostilities between warring parties, recent conflagration between Israelis and Palestinians, and Armenians and Azerbaijanians, for instance, have had a distinctive twentieth-century feel to them.

Discussion

The first scenario, Muddling Through, provides lessons based on incremental adjustments to emerging AI threats and opportunities without significant strategic overhaul. This scenario includes the sporadic use of deepfakes involving hostile entities, leading to isolated incidents of misinformation and ad-hoc countermeasures identified to mitigate threats. Resource constraints and bureaucratic inertia challenge the ability to keep pace with emerging threats. The slow integration of AI into military operations, in large part because of AI's real and believed weaknesses, leads to the use of small-scale isolated implementation of AI in specific defence projects. Without a comprehensive strategy, tactical advantages may be gained to suggest tactical developments in specific scenarios. This scenario has envisioned a future where national institutions have only made incremental adjustments to AI's growing impact, leading to ad-hoc, reactive, piecemeal responses, rather than a comprehensive forward-looking strategy.

The use of AI deepfakes by hostile entities is sporadic, and adversaries release deepfakes targeting government officials or election campaigns, which has been observed in recent years. This scenario involves temporary confusion and destabilization, as isolated incidents are widespread and largely dependent on the regulations that individual states do or do not put into place. The case-by-case development of the measures without integrating a broader strategy leads to a cat-and-mouse game where defence remains steps behind the evolving threats of AI capabilities to various applications. The steady increase of AI in cybercrime are gradually acknowledged by defence organizations, given hampered responses due to resource constraints and limits to funding, personnel or technological capabilities. A situation has emerged where the defence sector continues trying to catch up with the latest developments. Bureaucratic processes slow down the adoption of new technologies and necessary reforms. Lacking coordination, different branches of the defence establishment develop their own uses and applications of AI, leading to gaps and inefficiencies. Applications of AI in warfare include enabling autonomous systems, enhancing decision making and improving other operational efficiencies. Slow and uneven integration of AI into military operations leads to small-scale and isolated projects. For example, applications to enhance specific tactical operations for drone surveillance and logistics management, but lacking in the development of a large comprehensive vision, mean that the effect of these developments has limited impact on military effectiveness.

This scenario explored how organizations and democratic institutions adapt with specific examples highlighting weak signals and insights to include deepfake technology where advancements make it easier to create compelling manipulated media. Fake endorsements, altered speeches and misleading images aim to sway public opinion at targeted times to influence political outcomes — manipulated endorsements of celebrities supposedly supporting politicians and doctored videos used for smear campaigns. The flood of fakeries erodes public confidence in the transparency and fairness of electoral processes as citizens become increasingly skeptical of the authenticity of political communication. Most video, audio and text are viewed with some skepticism. Fact checking has become a booming industry as the proliferation of untruths makes verifiable truth a top commodity. Improved verification processes and robust fact-checking frameworks have become increasingly important parts of the AI industry.

Scenario 2: Worst Case — The Unbearable Weight of Massive AI

Narrative

It is spring 2040 and the AI wars have set in.

AI dominates all fields and all domains. Machine learning has progressed far faster and more broadly than anticipated, jumping from one task or domain to another almost seamlessly. Most experts believe that some AI applications are

growing, learning and expanding independently beyond their original tasks and with little human input. Something very close to AGI exists, although naval-gazing debates among philosophers and humanists alike continue as to whether machines are truly sentient and conscious. But who cares? Either way, governments, militaries and a handful of violent non-state actors have entirely relied on a combination of in-house and corporate AI for strategic advice, guidance and action. Not without reason, *The Economist*'s phrase of the year for 2038 was "dA.I.bolic loop" (pronounced day·i·baa·lukh), a vicious cycle in which algorithmic advice trained on winning rather than avoiding conflict, provides feedback that inevitably triggers a similar response in an adversary's machine. Putting a break on this iteration of the security dilemma leads to inevitable defeat. Even the mere appearance of attempting to slow down the spiral unilaterally invites defeat. And so it goes.

AI analysts have replaced human analysts across all intelligence services and military planning staff. Special operators continue to thrive, but their numbers are far outnumbered by intelligent robotic systems designed to thrive under specific conditions. Most worrisome, one characteristic of the dA.I.bolic loop is a realization that unknown unknowns have proliferated too. Adversaries and allies alike cannot be sure about the potency of another's AI systems, given that machines themselves are self-evolving and self-replicating. As Canada's new Chief of Defence Staff General Lucy Jacinthe Nassif warned colourfully at the 2039 NATO Summit at Mar-a-Lago, Florida: "We can't know what we don't know, but we sure as hell do know that if their AIs outcompete ours, it's game over for us." Canada's allies are increasingly on hair-trigger alert, actively guarding against AI-generated surprise attacks, which are too fanciful to imagine except by the most sophisticated machines. Nobody wants to live through Russia's 2036 orbital attack against Estonia again. That was a human tragedy entirely dreamt up by a Kremlin machine. Then again, like all AI-generated attack plans, that one was a one-and-done, zero-day event, an unknown that, at the very moment of launch, became immediately known and countered by all other competing military AIs. Once the siphoned coronal mass ejections dissipated, it was clear Estonia was not going to be the same again, but at least fear of a similar orbital attack taking place anywhere else immediately subsided. However, the next unknown AI bolt-from-the-blue is perpetually around the corner. That fear has crept into NATO's new AI deterrence framework: let allied machines determine who to threaten when, and how. The more diabolic the threat, the better.

Under most of these conditions, corporate AI dominates military affairs, but it operates in different settings: American, and some European, corporations function within the marketplace independent of the government, purchasing exclusive rights and access to specific machines, as they have with other technologies. Elsewhere, notably in China, France, Russia and Singapore, the state has forcefully captured corporate developments in AI, making it nearly impossible to distinguish between commercial and state interests. Now, it appears both models function at par. However, authoritarian regimes, and even some ostensibly democratic states, find the former model more conducive to domestic control and repression. With only a nudge and a prompt, China's leading military AI was used domestically to quell everything from environmental dissent to jaywalking. Dual use now has an entirely different meaning. Thus, geopolitical turmoil continues apace, with intense but brief periods of conflict subsiding as quickly as they emerge. While some twentieth-century alliances and diplomatic arrangements still hold, military AIs call and carry out all the shots, providing modern warfare with a distinctly twenty-first-century feel.

Discussion

In the Worst-Case scenario, massive disruption of AI threats overwhelms defence, leading to widespread disruption. Sophisticated deepfakes lead to mass confusion, eroding public trust in governments and the military, and AI-generated misinformation campaigns become the norm, targeting political processes with the intent to sow chaos, leading to domestic unrest. AI-powered cyberattacks cripple critical infrastructure, defence systems, communication networks and financial systems. AI is used in aggressive, targeted reconnaissance campaigns designed to find vulnerabilities and develop tools specifically designed to target them. State and non-state actors deploy advanced AI and autonomous weapons, outpacing defence response and rendering traditional military strategies obsolete with the full extent of AI warfare, leading to unprecedented casualties and strategic loss. AI capabilities are weaponized, leading to a breakdown in national security and defence, and an erosion of sovereignty by the instability to counter

AI threats, resulting in significant geopolitical losses on the international stage and loss of territory.

The Worst-Case scenario involves hostile actors, foreign states and extremist groups deploying large-scale, sophisticated deepfake campaigns. Examples include using AI-generated video and audio to mimic government officials, military leaders and other authoritative figures. Public trust has been significantly eroded, and citizens can no longer know who or what to believe, with even legitimate government messages questioned for validity due to the widespread information circulation challenging the legitimacy of elected officials. Cybercrime is becoming increasingly sophisticated in employing AI, which is used to automate enhanced effectiveness unleased on a national scale. AI-driven cyberattacks are launched to target critical infrastructure, defence systems, communication networks, power grids and financial systems. Defence system breaches target warning systems, command-and-control networks, and military databases.

AI in warfare, in the Worst-Case scenario, involves technologies weaponized against the state by hostile actors, where AI-enabled autonomous weapons systems are deployed, but unable to keep pace with the rapid advancement of AI warfare technologies, leading to unprecedented casualties among military personnel and civilians, capable of executing large-scale attacks with minimal human intervention. The emergence of self-replicating and autonomous evolving AI systems has unanticipated consequences, with the capacity for self-replication developing in unpredictable ways. A fierce arms race creates cutting-edge AI systems for warfare and other applications, and the dual-use applications of AI developments prove challenging to regulate.

Scenario 3: Transformative — AI Diplomatique

Narrative

It is spring 2040 and AI's true purpose has finally emerged.

The catastrophic and accidental launch of a single Russian nuclear intercontinental ballistic missile against a US missile installation in North Dakota on the very eve of President Jason Walker's January 2033 (1/33) inauguration was as close to mutual nuclear annihilation as human civilization has ever come. Thankfully, cooler heads among both states' militaries prevailed during the immediate crisis, setting the world up for a new and collaborative path forward for co-managing AI risks and rewards.

While states still compete against one another, and conflict and war still periodically emerge, on its fifth anniversary, the United Nations's North Dakota AI Control Framework (N-DAIC) functions even better than its founders had anticipated. Out of the ashes of 1/33, foes and friends alike have several new mechanisms to share and verify information about AI innovation and development, building mutual trust about its use and implementation. Not without reason, *The Economist*'s phrase of the year for 2038 was "machine diplomacy," an automated process by which geopolitical divisions, big and small, are addressed efficiently and sensitively by AI Diplomatique, a multilateral, open-sourced, public-private non-profit and mutually beneficial AI system able to weave together solutions to the globe's many wicked problems. Generations of animosity between rival communities, countries and blocs have given way to a skeptical but healthy cooperation. AI-driven solutions to the world's most significant conflicts have created new relations built around hope, respect and goodwill.

Military might still matters, but great power now resonates most as a lever for safeguarding peace and progress. The combined effects of 1/33, N-DAIC and AI diplomacy have meant the near total cessation of the offensive use of AI in strategic and military affairs. New, powerful algorithms are now trained to find positive-sum solutions rather than exploit zero-sum weaknesses. Reflecting a socio-cultural ethos emerging around them, most military leaders agree that their time is better served focusing on mutually beneficial solutions than on fighting over a dwindling heap of scraps. As Canada's new Chief of Defence Staff General Lucy Jacinthe Nassif encouraged the cheering crowds at the 2039 NATO Summit in Hong Kong: "You all know it because you all feel it. A better way is not only possible but necessary. We can continue to build a stronger, more united, more equitable future for our children together, or we can languish, suffer and perish together." Government-

civil society consortia are finding exciting ways to deploy AI to solve many other problems and issues, from alleviating food insecurity and malnutrition around the globe to addressing the menace of regional wildfires, plastic-borne diseases and biodiversity collapse. Military personnel and assets have been retooled and expanded to help assist in these positive endeavours. A collective sense of hope has taken hold.

Corporations have found technical ways to better explain and communicate how their AI systems function in practice. Trust in the positive characteristics of AI has risen year over year, followed by commercial expansion. Research collaboration, in which transnational AIs are used to decipher the mysteries of physics, chemistry, medicine, consciousness and space travel, regularly results in "game-changing" discoveries. In 2037, the Nobel Prize created a new award category — the aptly named Nobel AI Prize — to recognize accomplishments achieved by machine-human collaborative teams; the inaugural award recognized the Canadian-based collaborative behind the Abraham Alliance, an AI-enhanced diplomatic solution to the Israeli-Palestinian conflict that single-handedly rewrote the constructs of the contemporary Middle East. Canada's military reputation as a peacekeeping conciliator has never felt more assured. Thus, following its near-death experience, humanity has found ways to short-circuit and circumvent geopolitical turmoil. Conflict has not disappeared, but even the staunchest of antagonists have steadily accepted that a better, brighter future is possible and feasible with machines facilitating the way.

Discussion

AI's proactive and comprehensive integration into national defence will lead to transformative and robust security postures. AI deepfakes are impacted by the defence sector to develop advanced AI-driven tools to detect and neutralize deepfakes. AI-powered cybersecurity creates adaptive and predictive systems where national infrastructure resists AI-powered cyberattacks. AI in warfare integrates across all levels of military operations and autonomous systems, and AI-enhanced decision making and predictive analysis will support military development. The proactive embrace of AI across all levels has led to robust and resilient security by integrating AI strategically and comprehensively to neutralize threats. The defence sector's application of AI-driven detection tools is heavily investigated to develop advanced AI and use AI trained on vast data sets to recognize subtle indicators and digital manipulation. The use of AI to develop countermeasures and publicly demonstrate the effectiveness of the tools for the government to build public trust, allows citizens to be more confident that the information they receive is trustworthy.

With AI-powered cybersecurity, the increasing sophistication of attacks targeting critical infrastructure needs advanced measures to detect threats before they materialize. AI will be used for systems of adaptive prediction capable of anticipating cyberthreats before they materialize to improve detection to neutralize even the most advanced AI-driven cyberattacks. Investment is made in AI-powered cybersecurity measures for national infrastructure to ensure resilience to cyberattacks, protect systems and collaborate with private-sector partners to secure broader national infrastructure. AI in military operations offers new capabilities that can be integrated across all levels of military operations. Powered by AI, predictive analytics tools provide military leaders with insights into potential future scenarios for timely, informed, real-time decisions. AI-driven capabilities such as predictive analytics, autonomous systems and enhanced decision making provide a competitive edge for strategic geopolitical competition. Collaborative AI evolves to enhance military capabilities in a world transformed by AI breakthroughs. International cooperation attains compounding political will to promote moral AI developments to tackle complex global issues and transform contemporary conflict with AI-enhanced military weapons. Collaboration aims to establish international norms, principles of responsible use and standards. Global collaboration in AI development provides the opportunity for positive-sum solutions using AI as a tool to solve global problems, allowing nations to work together to address ongoing challenges. Collaborative projects and research emphasizing convergence require careful management, ethical considerations and practices of responsible use.

Conclusion: Next Steps and Future Research

Several central lessons can be drawn from the above discussion and scenarios. Proactive measures must be taken to combat the application of AI for deepfakes, cyberthreats, and warfare. This paper has outlined insights from the threat landscape that suggest crucial lessons based on the discussion of malicious applications of AI developments. Future research supports the necessary depth of analysis to compare policy approaches and recommendations to address vulnerabilities based on the use of these technologies and the pressing need to regulate and contain these approaches. Thematic areas of interest are based on the observations presented by this study to analyze the weak signals for early indicators of change. AI deepfakes and misinformation are changing the information landscape and erode public confidence in politicians, the media and other democratic institutions. Emerging applications of these tools disseminate propaganda and false information, undermining democratic processes. These observations necessitate robust moral and legal frameworks to safeguard public trust and voter participation.

Each of the scenarios provides central lessons. In the first scenario, Muddling Through, AI's lack of reliability for complex tasks does not meet the high expectations for AI in critical military strategy and intelligence applications, leading to cautious approaches where human oversight remains paramount. The first scenario provides several key points related to reliability, where applied AI is used to perform routine tasks effectively, yet it is unreliable for complex areas requiring human involvement. Further research within this scenario can assess the impact of AI's limited capabilities on effective integration.

In the second scenario, Worst Case, an overwhelming dominant AI system is depicted, which is self-evolving and self-replicating, such that reliance on AI for strategic and military decisions involves algorithmic decisions driving continuous cycles of escalation. The resulting destabilizing effects include an arms race driven by autonomous systems that, along with AI's self-evolving nature, introduces unknowns that complicate defence planning. Dual-use opportunities involve the same technology for military and civilian purposes, requiring careful management to avoid misuse. Policies must be created to govern dual-use AI to ensure responsible development and deployment. Strategic AI management will develop frameworks for international cooperation to manage AI-driven conflicts and arms races.

In the final scenario, Transformative, the world has embraced a collaborative approach to AI management, leading to global cooperation and problem-solving advancements. AI facilitates international cooperation to resolve complex international issues, managed collaboratively and ethically while shifting the focus from zero-sum competition. Positive-sum solutions provide the means to build the capacity to collaborate, and future research will investigate how AI can address studying the mechanisms and frameworks to enable successful international collaboration. AI development presents numerous diverse trajectories, each with implications for defence and security. The presented scenarios point to different impacts on lessons and the security framework for managing dual-use technologies, fostering international cooperation and addressing ethical AI development.

Strategic foresight is a crucial methodology to navigate the complexities of future advancements of AI in national defence. Foresight supports exploring multiple scenarios, and weak signals support anticipating medium- and long-term changes to prepare for emerging risks and opportunities. Policy makers can leverage the tools of foresight to better understand and address AI's unprecedented impacts, providing a flexible framework to adapt to evolving threats. This paper has specifically focused on AI-powered deepfakes, cybercrime and warfare. Strategic foresight has shaped defence policies in the Five Eyes countries and the Netherlands, proactively managing future security challenges to enhance situational awareness and readiness by incorporating comprehensive scenario planning and trend analysis. These scenarios underscore the need for robust, adaptive defence strategies aligned with international collaboration to ensure the responsible use of AI.

Works Cited

Altman, Sam. 2023. "Planning for AGI and beyond." OpenAI, February 24. https://openai.com/index/planning-for-agi-and-beyond/.

Bishop, Peter. 2001. "A yardstick too far?" *Foresight* 3 (3): 163–67. https://doi.org/10.1108/14636680110803085.

Bishop, Peter Andy Hines and Terry Collins. 2007. "The current state of scenario development: an overview of techniques." *Foresight* 9 (1): 5–25. https://doi.org/10.1108/14636680710727516.

Bostrom, Nick. 2014. *Superintelligence*. Oxford, UK: Oxford University Press.

Business Wire. 2024. "Palantir and Ministry of Economy of Ukraine Sign Demining Partnership." Yahoo Finance, March 4. https://finance.yahoo.com/news/palantir-ministry-economy-ukraine-sign-115900879.html.

Cairns, George and George Wright. 2020. "A reflection on the mass production of ßscenarios in response to COVID-19." *Futures and Foresight Science* 2 (3–4). https://doi.org/10.1002/ffo2.34.

Calof, Jon and Brian Colton. 2024. "Developing foresight that impacts senior management decisions." *Technological Forecasting and Social Change* 198: 123036. https://doi.org/10.1016/j.techfore.2023.123036.

Chan, Wilfred. 2023. "Is ChatGPT's 'evil twin' FraudGPT itself a scam?" Fast Company, July 28. www.fastcompany.com/90929870/is-chatgpts-evil-twin-fraudgpt-itself-a-scam.

Chen, Heather. 2024. "AI 'resurrects' long dead dictator in murky new era of deepfake electioneering." CNN, February 11. https://edition.cnn.com/2024/02/12/asia/suharto-deepfake-ai-scam-indonesia-election-hnk-intl/index.html.

Christopher, Nilesh. 2024. "How AI is resurrecting dead Indian politicians as election looms." Al Jazeera, February 12. www.aljazeera.com/economy/2024/2/12/how-ai-is-used-to-resurrect-dead-indian-politicians-as-elections-loom.

Christopher, Nilesh and Varsha Bansal. 2024. "Indian Voters Are Being Bombarded with Millions of Deepfakes. Political Candidates Approve." *Wired*, May 20. www.wired.com/story/indian-elections-ai-deepfakes/.

Cotovio, Vasco, Clare Sebastian and Allegra Goodwin. 2024. "Ukraine's AI-enabled drones are trying to disrupt Russia's energy industry. So far, it's working." CNN, April 2. www.cnn.com/2024/04/01/energy/ukrainian-drones-disrupting-russian-energy-industry-intl-cmd/index.html.

Cuhls, Kerstin E. 2020. "Horizon Scanning in Foresight — Why Horizons Scanning is only a part of the game." *Futures & Foresight Science* 1 (2): e23. https://doi.org/10.1002/ffo2.23.

DCDC. 2018. *Global Strategic Trends: The Future Starts Today*. London, UK: MOD.

De Angelo, Dena. 2024. "The Dark Side of AI in Cybersecurity — AI-Generated Malware." *Palo Alto Networks Blog*, May 15. www.paloaltonetworks.com/blog/2024/05/ai-generated-malware/.

Deloitte. 2024. *Threat Report: How threat actors are leveraging Artificial Intelligence (AI) technology to conduct sophisticated attacks*. Global Threat Intelligence. March. www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-design-ai-threat-report-v2.pdf.

Devine, Curt, Donie O'Sullivan and Sean Lyngaas. 2024. "A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning." CNN, February 1. https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html.

Dotson, John. 2023. "Beijing Dusts Off an Old Playbook with Disinformation about Taiwan Biological Warfare Labs." Global Taiwan Institute, November 1. https://globaltaiwan.org/2023/11/beijing-dusts-off-an-old-playbook-with-disinformation-about-taiwan-biological-warfare-labs/.

Erzberger, Arthur. 2023. "WormGPT and FraudGPT — The Rise of Malicious LLMs." *SpiderLabs Blog*, August 8. www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/wormgpt-and-fraudgpt-the-rise-of-malicious-llms/.

Fergnani, Alessandro and Thomas J. Chermack. 2021. "The resistance to scientific theory in futures and foresight, and what to do about it." *Futures and Foresight Science* 3 (3–4): : e61. https://doi.org/10.1002/ffo2.61.

France 24. 2024. "Taiwan voters face flood of pro-China disinformation." France 24, January 10. www.france24.com/en/live-news/20240110-taiwan-voters-face-flood-of-pro-china-disinformation.

Global Affairs Canada. 2018. "A (De)Globalizing World? Environmental Scan." Foreign Policy Research and Foresight.

Honda, Hidehito, Yuichi Washida, Akihito Sudo, Yuichiro Wajima, Keigo Awata and Kazuhiro Ueda. 2017. "The difference in foresight using the scanning method between experts and non-experts." *Technological Forecasting and Social Change* 119: 18–26. https://doi.org/10.1016/j.techfore.2017.03.005.

IBM. 2023. "Understanding the different types of artificial intelligence." IBM, October. www.ibm.com/think/topics/artificial-intelligence-types.

Kahn, Herman. 1962. *Thinking About the Unthinkable.* New York, NY: Horizon.

Kelley, Daniel. 2023. "WormGPT — The Generative AI Tool Cybercriminals Are Using to Launch BEC Attacks." *SlashNext Blog*, July 13. https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/.

Klare, Michael. 2024. "Swarms of AI 'killer robots' are the future of war: If that sounds scary, it should." *Salon*, February 24. www.salon.com/2024/02/24/swarms-of-ai-killer-robots-are-the-future-of-war-if-that-sounds-scary-it-should_partner/.

Knight, Will. 2022. "As Russia Plots Its Next Move, an AI Listens to the Chatter." *Wired*, April 4. www.wired.com/story/russia-ukraine-war-ai-surveillance/.

Kuusi, Osmo and Sirkka Heinonen. 2022. "Scenarios From Artificial Narrow Intelligence to Artificial General Intelligence — Reviewing the Results of the International Work/Technology 2050 Study." *World Futures Review* 14 (1): 65–79. https://doi.org/10.1177/19467567221101637.

Larkin, Zoe 2022. "General AI vs Narrow AI." *Levity* (blog), September 30 https://levity.ai/blog/general-ai-vs-narrow-ai.

Liddell, James. 2024. "Trump posts AI-generated image of Harris speaking at DNC with communist flags." *The Independent*, August 19. www.independent.co.uk/news/world/americas/us-politics/trump-ai-communism-harris-dnc-b2598303.html.

Losey, Stephen. 2023. "New in 2024: Air Force plans autonomous flight tests for drone wingmen." *Military Times*, December 30. www.militarytimes.com/air/2023/12/30/new-in-2024-air-force-plans-autonomous-flight-tests-for-drone-wingmen/.

Magramo, Kathleen. 2024. "British engineering giant Arup revealed as $25 million deepfake scam victim." CNN, May 17. www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html.

Marantz, Andrew. 2024. "O.K., Doomer." *The New Yorker*, March 18. www.magzter.com/stories/culture/The-New-Yorker/OK-DOOMER.

Marcovitch, Inbal and Alex Wilner. 2024. "Tackling the Geopolitics of Standardization: Lessons from Canada's Foresight-to-Standards Pilot Project." *International Journal* 79 (4): 577–99. https://doi.org/10.1177/00207020241298264.

Metz, Cade. 2024a. "OpenAI Unveils A.I. That Instantly Generates Eye-Popping Videos." *The New York Times*, February 15. www.nytimes.com/2024/02/15/technology/openai-sora-videos.html.

———. 2024b. "How the A.I. That Drives ChatGPT Will Move Into the Physical World." *The New York Times*, March 11. www.nytimes.com/2024/03/11/technology/ai-robots-technology.html.

Ministry of Economy of Ukraine. 2023. "Artificial Intelligence to Help Demining Ukraine." October 23. www.me.gov.ua/News/Detail?lang=en-GB&id=db1e15c6-b9f4-43ec-88b9-7a1bcf336e5a&title=ArtificialIntelligenceToHelpDeminingUkraine.

Mizsei, Berta. 2023. "Foresight is a messy methodology but a marvellous mindset." Centre for European Policy Studies, March 6. www.ceps.eu/foresight-is-a-messy-methodology-but-a-marvellous-mindset/.

Necsutu, Madalin. 2023. "Moldova Dismisses Deepfake Video Targeting President Sandu." Balkan Insight, December 29. https://balkaninsight.com/2023/12/29/moldova-dismisses-deepfake-video-targeting-president-sandu/.

NIC. 2021. *Global Trends Report 2040: A More Contested World.* March. www.dni.gov/index.php/gt2040-home.

Nicas, Jack and Lucia Cholakian Herrera. 2023. "Is Argentina the First A.I. Election?" *The New York Times*, November 15. www.nytimes.com/2023/11/15/world/americas/argentina-election-ai-milei-massa.html.

Office of the Chief Scientist. 2019. *The Future of Space 2060 and Implications for U.S. Strategy: Report on the Space Futures Workshop.* Air Force Space Command, September 5. https://aerospace.csis.org/wp-content/uploads/2019/09/Future-of-Space-2060-v2-5-Sep.pdf.

Parkin, Benjamin. 2024."Deepfakes for $24 a month: how AI is disrupting Bangladesh's election." *Financial Times*, January 14. www.ft.com/content/bd1bc5b4-f540-48f8-9cda-75c19e5ac69c.

Patel, Andrew and Jason Sattler. 2023. "Creatively malicious prompt engineering." WithSecure Labs, January 11. https://labs.withsecure.com/publications/creatively-malicious-prompt-engineering.

Policy Horizons Canada. 2018. Foresight Training Module 1.

———. 2021. "Foresight on Covid-19." March.

Prítyi, Marek, Dexter Docherty and Trish Lavery. 2022. *Foresight and Anticipatory Governance in Practice: Lessons in effective foresight institutionalisation.* Organisation for Economic Co-operation and Development. www.oecd.org/content/dam/oecd/en/about/programmes/strategic-foresight/foresight-and-anticipatory-governance-2021.pdf.

Reilly-King, Fraser, Collee Duggan and Alex Wilner. 2024. "Foresight and futures thinking for international development co-operation: Promises and pitfalls." *Development Policy Review* 42 (1). https://doi.org/10.1111/dpr.12790.

Reuters. 2023. "'Deepfake' scam in China fans worries over AI-driven fraud." Reuters, May 22. www.reuters.com/technology/deepfake-scam-china-fans-worries-over-ai-driven-fraud-2023-05-22/.

———. 2024. "AI and covert canvassing: How Imran Khan is campaigning from jail in Pakistan." NBC News, February 6. www.nbcnews.com/news/world/pakistan-election-imran-khan-rcna137413.

School of International Futures. 2021. *Features of effective systemic foresight in governments around the world.* Government Office for Science. April. www.gov.uk/government/publications/features-of-effective-systemic-foresight-in-governments-globally.

Shafer, Ellise. 2024. "Donald Trump Falsely Claims Taylor Swift Has Endorsed Him by Posting AI Images: 'I Accept.'" *Variety*, August 19. https://variety.com/2024/music/news/donald-trump-falsely-claims-taylor-swift-endorsed-ai-images-1236110583/.

Shimony, Eran and Omer Tsarfati. 2023. "Chatting Our Way Into Creating a Polymorphic Malware." *CyberArk Threat Research Blog*, January 17. www.cyberark.com/resources/threat-research-blog/chatting-our-way-into-creating-a-polymorphic-malware.

Spaniol, Matthew J. and Nicholas J. Rowland. 2018. "Defining scenario." *Futures and Foresight Sciences* 1 (1): e3. https://doi.org/10.1002/ffo2.3.

Tanas, Alexander. 2024. "Moldovan Opposition Leader Calls for Better Ties with Russia, China." Reuters, June 1. www.reuters.com/world/europe/moldovan-opposition-leader-calls-better-ties-with-russia-china-2024-06-01/.

The Japan Times. 2024. "Kawasaki man arrested over malware made using generative AI." The Japan Times, May 28. www.japantimes.co.jp/news/2024/05/28/japan/crime-legal/man-arrested-malware-generative-ai/.

The Straits Times. 2022. "Deepfake democracy: South Korean presidential candidate's avatar a huge hit." February 14. www.straitstimes.com/asia/east-asia/deepfake-democracy-south-korean-candidate-goes-virtual-for-votes.

Tobin, Meaghan and Cade Metz. 2024. "China Is Closing the A.I. Gap With the United States." *The New York Times*, July 25. www.nytimes.com/2024/07/25/technology/china-open-source-ai.html.

Urban, R. B. and Herman Kahn. 1971. "Herman Kahn thinks about the thinkable." An interview of Herman Kahn by R. B. Urban in *The New York Times*, June 20. www.nytimes.com/1971/06/20/archives/most-of-the-traditional-causes-of-war-have-disappeared-a-talk-with.html.

Van Der Meer, Robert. 2023. "COVID: how incorrect assumptions and poor foresight hampered the UK's pandemic preparedness." *The Conversation*, June 30. https://theconversation.com/covid-how-incorrect-assumptions-and-poor-foresight-hampered-the-uks-pandemic-preparedness-208720.

Webb, Amy. 2024. "How true strategic foresight can help companies survive and thrive." World Economic Forum, January 31. www.weforum.org/stories/2024/01/strategic-foresight-help-companies-survive-thrive/.

Wenhao. 2024. "An E-book titled 'The Secret History of Tsai Ing-Wen' is being spread by bots in the Chinese language social media circle" (X thread). X, January 10, 12:21 p.m. https://x.com/ThisIsWenhao/status/1745133673358274621.

Wenus, Luis. 2024. "We built an AI-steered homing/killer drone in just a few hours." X, March 2, 12:23 p.m. https://x.com/luiswenus/status/1763978511092478221.

Wilner, Alex and Talya Stein. Forthcoming 2025. "Revisiting the Use and Utility of Domain Mapping: A Comparative Study of the Future(s) of Diplomacy and International Affairs."

Wilner, Alex and Martin Roy. 2020. "Canada's emerging foresight landscape: observations and lessons." *Foresight* 22 (5/6): 551–62. https://doi.org/10.1108/FS-03-2020-0027.

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