National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Artificial Intelligence and Global Security Challenges With Governance

Lieutenant-Colonel Steven W. Flavel

JCSP 49 DL

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 49 AD

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 DL - PCEMI n° 49 AD
2022 - 2024

Exercise Solo Flight – Exercice Solo Flight

Artificial Intelligence and Global Security Challenges With Governance

Lieutenant-Colonel Steven W. Flavel

ARTIFICIAL INTELLIGENCE AND GLOBAL SECURITY CHALLENGES WITH GOVERNANCE

INTRODUCTION

Canada is uniquely fortunate due to its geographical location and abundant natural resources, which insulate it from many global issues. Bordered by three oceans and sharing its southern boundary with the United States, Canada benefits from a degree of physical separation from regions prone to conflict and instability. This strategic positioning allows for greater physical control over its borders and reduces the immediate impact of geopolitical tensions[1]As Canada becomes more digital, with businesses and services moved online and data stored in distributed external systems (the cloud), the Information Age's latest emerging technology, artificial intelligence (AI), will significantly change Canada's national security and alter global security by enhancing both defensive and offensive capabilities, requiring new and updated global governance strategies and regulatory agreements[2].

The rapid emergence of AI is reshaping global dynamics and presenting urgent new challenges and opportunities for global governance. As AI technologies become progressively integrated into all national organizations, from healthcare and finance to national security and defense, they intersect traditional systems and create novel forms of interdependence and vulnerability. AI development is rapidly surpassing established regulatory processes at a scale that demands an immediate and comprehensive response. It is AI's ability to process vast amounts of data, automate complex tasks, and make autonomous decisions that are challenging economic systems, labor markets, and military strategies and also necessitate a reassessment of existing governance frameworks[3].Global governance must also address ethical AI use, cross-border data flows, cybersecurity, and the equitable distribution of AI benefits. Effective management of these challenges will require unprecedented levels of international cooperation, innovative regulatory mechanisms, and a commitment to ensuring that AI advances contribute to global stability and security[4].

AI advancements will revolutionize and make obsolete numerous sectors and present unprecedented challenges to global security governance. The ongoing integration of AI into critical infrastructure, military applications, and economic systems introduces new vulnerabilities that traditional governance frameworks are currently unprepared to manage. Regulatory approaches must be reassessed to keep pace with AI technology's rapid evolution to establish robust international cooperation and develop innovative governance strategies[5]. The security risks associated with AI must be managed through strategies designed to ensure that its development and deployment align with global security and ethical standards. Traditional security governance mechanisms must evolve to address AI's dynamic and complex nature,

---

[1] Nossal. "Geography and Canada's National Interests."
[2] Haswel. "Development, Adoption, and Integration of Artificial Intelligence: National Security Implications."
[3] The White House. *The Impact of Artificial Intelligence on the Future of Workforces in the European Union and the United States of America*. 6.
[4] Bremmer, et al. "The AI Power Paradox: Can States Learn to Govern Artificial Intelligence-Before It's Too Late?"
[5] Nelson. "The Right Way to Regulate AI Focus on Its Possibilities, Not Its Perils"

considering these challenges and emphasizing the need for innovative approaches to keep pace with the AI revolution.

TERMINOLOGY

Artificial intelligence (AI) is the capability of machines to perform tasks that typically require human intelligence such as learning, reasoning, problem-solving, perception, and language understanding. AI systems can process vast amounts of data, identify patterns, and make decisions or predictions with minimal human intervention utilizing techniques like deep learning and neural networks, these advancements enable AI to transform industries, drive economic growth, and present both opportunities and challenges in various sectors, including security and governance[6].

International or global security refers to the measures and strategies implemented by states and international organizations to protect against threats that transcend national borders, ensuring the safety and stability of the global community. This encompasses efforts to prevent and respond to conflicts, terrorism, cyberattacks, and other challenges that can impact multiple countries and regions, maintaining peace and security worldwide[7].

National governance involves the exercise of authority to manage a country's economic, political, and administrative affairs. It includes the processes, mechanisms, and institutions through which citizens and groups articulate their interests, exercise their rights, fulfill their obligations, and resolve their differences[8].

ARTIFICIAL INTELLIGENCE IN GLOBAL SECURITY

Opportunities Offered by Artificial Intelligence

Artificial intelligence (AI) is revolutionizing global security by augmenting human intelligence with unprecedented gathering and analysis capabilities, improving defensive measures through autonomous systems, and demonstrating successful integrations in various security contexts. For instance, AI-powered facial recognition systems identify potential threats in crowded public spaces and analyze social media data to scrape individual information and help identify initial signs of instability[9]. These examples of AI's enhanced intelligence capabilities can use diverse sources to process enormous quantities of data, identifying patterns and variances that may be undetectable to human analysts. This collaborative potential of AI and human intelligence in security contexts enables quicker and more accurate threat assessments, reassuring users and decision-makers of the reliability and transparency AI[10].

---

[6] Willett. “Cyber instruments and international security”. 12.
[7] Payne. “Artificial Intelligence: A Revolution in Strategic Affairs?”
[8] United Nations. *Chapter VI - Governance and Institutions.* 142.
[9] Fontes, et al. “AI-powered public surveillance systems: why we (might) need them and how we want them.” 5.
[10] Gesk, et al. “Artificial intelligence in public services: When and why citizens accept its usage.” 2-3.

The advantages of AI in global security extend to improved defensive capabilities. Autonomous systems, such as uncrewed aerial vehicles (UAVs) and automated defense platforms, significantly enhance operational efficiency and response times. These systems, capable of operating in hazardous or inaccessible environments to human operators, provide critical support during reconnaissance missions and in active combat zones. The integration of AI into missile defense systems, for example, allows for rapid identification and neutralization of incoming threats, reducing the likelihood of successful enemy strikes. The competitive edge provided by AI includes the ability to predict maintenance needs, optimize resource allocation, and analyze vast amounts of data to forecast international events and potential adversaries' actions. For example, AI was instrumental in predicting Russia's invasion of Ukraine, providing critical early warnings.[11].

Real-world applications of AI in security systems prove these technologies' benefits. The United States has employed AI to create real-time software visualizations of operational battlefields, improving situational awareness and decision-making to reduce battlefield casualties and damage[12]. Similarly, China has developed advanced AI-driven drones and cyber capabilities, which are increasingly integrated into its military strategies[13] and the United Kingdom is also investing heavily in AI through its UK National AI Strategy for security purposes, ensuring that they remain at the forefront of AI innovation[14]. These practical examples underscore the global potential of AI to transform conventional defense mechanisms and enhance national security frameworks, inspiring the audience with the possibilities of AI in global security.

Threats and Challenges Posed by Artificial Intelligence

Despite the opportunities, AI introduces threats and challenges that must be balanced between accelerating AI adoption and implementing necessary safeguards to ensure AI technologies are used responsibly and ethically. There are significant challenges in fully integrating AI into defense systems, which can make independent decisions about the use of lethal force, raising ethical and operational issues, particularly the potential loss of human oversight[15]. The risk of malfunction or unintended escalation due to autonomous systems acting unpredictably is a serious concern, as demonstrated by incidents where automated defense systems have misidentified targets, leading to friendly fire incidents[16].

AI threatens democratic processes by potentially spreading biased or flawed information. The technology's ability to influence public opinion subtly and powerfully, without transparency, can undermine democratic discourse. Instances of AI-generated propaganda and deepfakes illustrate the risks of misinformation and manipulation. There is concern over the oligopoly of a few AI companies controlling the flow of information, raising questions about who defines the social and political norms embedded in AI outputs[17].

---

[11] Flournoy. “AI Is Already at War.” 60-61.
[12] Bollmann, et al. The Strategic Corporal, the Tactical General, and the Digital Coup d’oeil – Military Decision-Making and Organizational Competences in Future Military Operations.” 156.
[13] Zhang, Jiayu. “China’s Military Employment of Artificial Intelligence and Its Security Implications.”
[14] Government of the United Kingdom. *National AI Strategy*. 8-9.
[15] Flournoy. “AI Is Already at War.” 61-62.
[16] Kendall-Taylor, et al. “The Digital Dictators: How Technology Strengthens Autocracy.”
[17] Feldstein. “The Consequences of Generative AI for Democracy, Governance and War.” 121-122.

The potential for cyber operations to escalate beyond the conflict zone remains a significant concern. The Russia-Ukraine War saw extensive cyber vigilantism, with groups like Anonymous, Network Battalion 65, and the Cyber Partisans targeting Russian networks. These volunteer efforts resulted in significant data breaches and disruptions, further complicating the cyber landscape. While these activities added a diversion that could obscure state operations, they also demonstrated the impact of non-state actors in cyber conflicts[18].

GOVERNANCE CHALLENGES

Regulatory Challenges

Researchers argue that AI large language models (LLMs) can enforce ethical uses of force, however, there are others who caution they could remove human decision-making in critical situations. Nations are actively exploring AI's military applications and are establishing units, departments, and government organizations that are developing AI adoption strategies. LLMs are now used for various military functions, including target selection and war games. Despite their potential, there are concerns about LLMs' unpredictable actions and security vulnerabilities, leading to cautious implementation in high-stakes decisions. Training and fine-tuning LLMs involve complex processes to balance human-like behavior with ethical considerations. However, LLMs cannot replicate human reasoning, posing risks in military use. Proper understanding and training are essential for integrating LLMs safely in military operations without compromising decision-making[19].

National versus international governance adds another layer of complexity. AI cyberattacks often transcend national boundaries, complicating jurisdiction and response efforts. The global nature of these cyberattacks necessitates robust international collaboration, including the sharing of threat intelligence and the harmonization of regulatory frameworks Attribution of these cross-border attacks is particularly challenging, complicating accountability and potential retaliation. Moreover, varying international laws and ethical standards create disparities in how AI cyberattacks are managed, potentially leading to conflicts and inconsistent responses underscoring the need for a coordinated global approach[20].

Ten nations, including Canada, have signed a Digital Nations Charter that outlines a commitment among member countries to foster innovation, enhance digital government services, and promote open government through the ethical use of data and technology. It emphasizes collaboration, knowledge sharing, and the development of digital infrastructure to improve public services and citizen engagement. The Charter was reviewed and updated in 2021 but remains non-binding with no legal obligations or enforceability among the signatories. On July 18, 2023, the United Nations Security Council met for the first time to discuss AI risks, emphasizing the urgent need for international cooperation to develop governance frameworks ensuring AI technologies are

[18] Willett. “The Cyber Dimension of the Russia–Ukraine War.” 16-17.
[19] Lamparth, et al. “Why the Military Can’t Trust AI: Large Language Models Can Make Bad Decisions- and Could Trigger Nuclear War.”
[20] United Kingdom House of Lords. “Proceed with Caution: Artificial Intelligence in Weapon Systems.” 12-13.

safe, transparent, and aligned with human rights and democratic values[21]. This late start and political gridlock in United Nations discussions indicate that crucial discussions on international regulatory frameworks, ethical guidelines, and international cooperation to mitigate AI risks will increasingly lag the pace of technological development[22].

Ethical and Moral Considerations

The moral and ethical implications of AI in military and security settings are both significant and intricate. They underscore the risk of unintended conflict escalation due to AI technologies and emphasize the pressing need for international standards to regulate AI use in military contexts. The introduction and use of autonomous weapons systems spark serious worries about the "dehumanization of lethal force," where crucial decisions about life and death might be made without human involvement. Furthermore, the propensity of AI models to "hallucinate" or produce incorrect information threatens both operational integrity and the precision of decision-making[23]. The race to fully integrate AI into military operations amplifies the potential for misuse and unintended consequences and underscores the necessity for thorough regulatory frameworks and ethical guidelines to ensure responsible AI deployment in security domains[24].

The issue of accountability in military operations becomes significantly more complex with the use of AI, especially when systems fail or behave unexpectedly. Autonomous systems cause issues with the traditional military chain of command decision-making process, complicating the process of attributing responsibility for decisions and holding individuals responsible for AI actions. The problem is further complicated by the 'black box' nature of many AI algorithms, where even developers cannot fully understand the decision-making processes. This opacity erodes trust and creates substantial challenges for accountability and oversight, underscoring the issue's complexity.[25]

CASE STUDY APPROACHES TO AI IN GOVERNANCE AND SECURITY

There is a consensus on the need for comprehensive international artificial intelligence (AI) regulatory frameworks regarding governance and security, but global efforts remain fragmented. As countries develop their own governance, we will examine several nations and the European Union (EU) to view current AI governance in security-specific challenges and individual approaches to AI regulation.

Canada

Canada is actively working to integrate AI's transformative technologies and its future potential into its national security framework. It's approach is distinguished by a strong emphasis on

[21] Nichols. "UN Security Council meets for the first time on AI risks."
[22] Heath. "UN deadlocked over regulating AI."
[23] Feldstein. "The Consequences of Generative AI for Democracy, Governance and War." 130-132.
[24] Grome. "Spectres of the Sea: The United States Navy's Autonomous Ghost Fleet, its Capabilities and Impacts, and the Legal Ethical Issues that Surround." 36.
[25] United States Department of Homeland Security. "Mitigating Artificial Intelligence (AI) Risk." 19-20, 23.

ethical considerations and public trust[26]. The country has established the Advisory Council on Artificial Intelligence, which provides strategic advice on AI policy and governance[27] and launched the Pan-Canadian Artificial Intelligence Strategy to support research and development in AI technologies[28].

In early 2024, the Government of Canada released a report that identified 35 potential disruptions that could significantly impact Canadian society. The report emphasized the importance of foresight in policy development and suggested that considering these disruptions can help seize opportunities, navigate impacts, and minimize risks. Key disruptions included frequent cyberattacks on critical infrastructure, the rapid development of AI, and erosion of trust in information due to AI-generated content which was identified as the most likely to occur and have the most significant impact within three to five years[29].

Canada faces a labyrinth of challenges in AI governance for national security. At the forefront, ensuring that AI development and usage align with ethical standards and uphold human rights is a formidable task. Consistently, Canada champions creating and deploying AI that is transparent, accountable, and in tune with democratic values[30]. Yet, turning these lofty ideals into practical regulatory frameworks is an intricate endeavor. Adding another layer of complexity, coordinating AI regulation between federal and provincial governments proves intricate. Harmonizing AI policies across diverse jurisdictions is an immense challenge, intensified by Canada's decentralized political system. To confront this issue, the federal government has launched collaborative initiatives with provinces and territories to craft a unified and cohesive national strategy for AI governance[31].

United States

The United States has led the world in AI development and integration of AI technologies into military and security frameworks, yet significant challenges persist in effectively governing AI. Despite numerous initiatives to embed AI into defense strategies, AI governance implementation has been slow and fragmented. For example, the Joint Artificial Intelligence Center (JAIC) was established by the U.S. Department of Defense in June 2018 to accelerate AI adoption across the military, but bureaucratic hurdles and a risk-averse culture have hindered rapid progress[32].National regulatory frameworks have been established with the National Defense Authorization Act (NDAA), which includes provisions for AI research and development[33], and the National Artificial Intelligence Initiative (NAII) aims to coordinate AI policy across federal agencies[34].

---

[26] Government of Canada. “Responsible Use of Artificial Intelligence (AI): Exploring the Future of Responsible AI in Government.”
[27] Government of Canada. “Advisory Council on Artificial Intelligence”
[28] Government of Canada. “Pan-Canadian Artificial Intelligence Strategy”
[29] Government of Canada. *Disruptions on the Horizon – 2024 Report*. 9.
[30] Government of Canada. “The Future of Generative AI.”
[31] Government of Canada. “Pan-Canadian Artificial Intelligence Strategy”
[32] Clark. “DOD Releases AI Adoption Strategy.”
[33] McCarthy, et al. “Highlights From the 2024 National Defense Authorization Act (NDAA) and What It Means for the Security Industry.”
[34] The White House. *National Artificial Intelligence Research and Development Strategic Plan – 2023 Update*. 1.

The United States focuses more on promoting innovation than on regulatory oversight. Although the White House has initiated voluntary commitments from AI companies to set safety standards, private sector responses vary[35]. Some companies support more regulation but simultaneously resist stringent controls that could hinder innovation. However, gaps remain in ensuring ethical standards and accountability, particularly in deploying autonomous systems in combat scenarios[36].

China

China is the only major power with explicit generative AI regulations, and its approach to AI in security and governance is characterized by aggressive investment and rapid integration into military and surveillance systems[37]. Their AI strategy emphasizes developing AI-driven autonomous weapons, cybersecurity tools, and surveillance technologies. China's extensive use of AI for authoritative domestic surveillance and social control highlights its commitment to leveraging AI for national security and internal stability[38].

China's regulatory approach to AI governance starkly contrasts with that of the U.S., leaning heavily towards a top-down strategy that prioritizes state control over individual rights. This method lacks transparency and independent oversight, integrating AI into the social credit system in ways that bolster authoritarian governance. Such an approach raises profound ethical concerns, especially regarding privacy and human rights[39].

European Union and Russia

The EU's approach to AI governance has been expectedly stringent and regulation advancing towards legislation reminiscent of China by identifying AI models as "high risk" and subjecting them to strict oversight[40]. The EU's General Data Protection Regulation (GDPR) achieves this by setting stringent data privacy and security standards for influencing AI development and deployment. The regulation emphasizes ethical considerations, transparency, and accountability, balancing innovation with protecting fundamental rights.[41].

The EU recently implemented the Artificial Intelligence Act. The first comprehensive regulation of AI by a major regulator and includes stringent requirements for high-risk AI applications in security and defense, ensuring robust oversight and accountability mechanisms. The EU's emphasis on ethical AI provides a model for balancing technological advancement with human rights protection, although the challenge remains in ensuring effective implementation across member states[42].

---

[35] Feldstein. "The Consequences of Generative AI for Democracy, Governance and War." 131-132.
[36] Scharre. "The Perilous Coming Age of AI Warfare - How to Limit the Threat of Autonomous Weapons."
[37] Feldstein. "The Consequences of Generative AI for Democracy, Governance and War." 131-132.
[38] Habib. "In Xinjiang, China, surveillance technology is used to help the state control its citizens."
[39] Donnelly. "China Social Credit System Explained – What is it & How Does it Work?"
[40] Feldstein. "The Consequences of Generative AI for Democracy, Governance and War." 131-132.
[41] European Parliament and Council of the European Union. "General Data Protection Regulation – GDPR".
[42] Chee, et al. "Europe sets benchmark for rest of the world with landmark AI laws."

CONCLUSION AND RECOMMENDATIONS

The development of effective governance mechanisms becomes more urgent as artificial intelligence (AI) technologies advance and surpass existing governance frameworks' capacity to manage their implications effectively. Policymakers and international bodies must take decisive action to address these challenges ensuring that AI advancements contribute to global stability and security rather than exacerbating existing vulnerabilities.

Developing Effective Governance Mechanisms

The potential risks associated with AI including autonomous weapons, cybersecurity threats, and information warfare, underscore the critical need for comprehensive governance mechanisms to keep pace with technological advancements. Integrating AI into military strategies is inevitable, and failure to regulate these technologies adequately could lead to catastrophic consequences, such as algorithmic malfunctions or manipulations that result in civilian casualties[43].

Recommendations for Policymakers and International Bodies

1. International Cooperation and Coordination: Effective AI governance requires unprecedented international cooperation. Policymakers should work towards establishing international treaties and agreements that set clear standards for the ethical use of AI in security contexts[44]. Collaborative frameworks, such as the Digital Nations Charter, provide a foundation for such efforts but must be expanded and binding to ensure compliance and accountability[45].

2. Comprehensive Regulatory Frameworks Development: Regulatory frameworks must be developed to address the complexity of AI-related risks and must include guidelines for developing and deploying AI technologies, emphasizing transparency, accountability, and ethical considerations. For instance, autonomous weapons systems require stringent oversight to prevent misuse and ensure that human oversight is maintained in decision-making processes involving lethal force[46].

3. Research and Development Investment: Governments should invest in AI research and development, emphasizing security and ethical considerations through funding AI safety research to identify risks and opportunities associated with AI technologies towards global security and national governance. By fostering innovation in a controlled and responsible manner, policymakers can ensure that AI advancements contribute to societal well-being and global security[47].

4. Public-Private Partnerships: Policymakers should encourage public-private partnerships (P3) that leverage the resources and expertise of technology companies while adhering to strict

---

[43] Horowitz, et al. "A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation." 158-160.
[44] Bremmer. "The AI Power Paradox: Can States Learn to Govern Artificial Intelligence-Before It's Too Late?" 5-6.
[45] Digital Nations. *Digital Nations Charter*.
[46] Feldstein. "The Consequences of Generative AI for Democracy, Governance and War." 132.
[47] Puscas. "AI and International Security - Understanding the Risks and Paving the Path for Confidence Building Measures."

ethical standards[48]. Initiatives like the National Artificial Intelligence Research Resource (NAIRR) Task Force in the United States exemplify how such collaborations can be structured to promote responsible AI innovation[49].

5. Strengthening Cybersecurity: Policymakers must prioritize the development of robust cybersecurity frameworks that can defend against AI-powered cyberattacks as these AI-driven cybersecurity threats pose a significant challenge to global security. These frameworks include enhancing the resilience of critical infrastructure and developing international protocols for responding to cyber incidents[50].

6. Ethical and Moral Considerations: Policymakers must create ethical guidelines for AI use, ensuring the development and deployment of these technologies respect human rights and democratic values. This requires establishing mechanisms for accountability and oversight to prevent abuses and ensure AI technologies benefit everyone.[51].

The effective governance of AI in global security contexts demands a proactive and coordinated approach. By prioritizing international cooperation, developing comprehensive regulatory frameworks, investing in research and development, fostering public-private partnerships, strengthening cybersecurity measures, and addressing ethical considerations, policymakers and international bodies can navigate AI technologies' complex challenges and ensure their responsible integration into global security strategies.

[48] Maggioncalda. "4 ways public-private partnerships can bridge the AI opportunity gap."
[49] The White House. *Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem An Implementation Plan for a National Artificial Intelligence Research Resource*. iv-vii.
[50] Feldstein, "The Consequences of Generative AI for Democracy, Governance and War." 133.
[51] Flourney. "AI Is Already at War."

BIBLIOGRAPHY

Bremmer, Ian and Mustafa Suleyman. "The AI Power Paradox: Can States Learn to Govern Artificial Intelligence - Before It's Too Late?" Foreign Affairs. September/October 2023, Vol. 102 Issue 5, p26-43.

Bollmann, Anders, and Therese Heltberg. "The Strategic Corporal, the Tactical General, and the Digital Coup d'oeil – Military Decision-Making and Organizational Competences in Future Military Operations." Scandinavian Journal of Military Studies, Volume: 6 Issue: 1, 151–168. 21 August 2023. https://sjms.nu/articles/10.31374/sjms.190

Chee, Foo Yun and Tassilo Hummel. "Europe sets benchmark for rest of the world with landmark AI laws." Reuters. 22 May 2024, Accessed: 24 May 2024. https://www.reuters.com/world/europe/eu-countries-back-landmark-artificial-intelligence-rules-2024-05-21/

Clark, Joseph. "DOD Releases AI Adoption Strategy." United States Department of Defense, DOD News. 2 November 2023, Accessed: 24 May 2024. https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

Digital Nations. *Digital Nations Charter*. Signed: 18 November 2023. https://www.leadingdigitalgovs.org/_files/ugd/189d02_ff9d33d670124239a3f6475e7c833ca8.pdf

Donnelly, Drew. "China Social Credit System Explained – What is it & How Does it Work?" Horizons. 11 February 2024, Accessed: 24 May 2024. https://joinhorizons.com/china-social-credit-system-explained/

European Parliament and Council of the European Union. "General Data Protection Regulation – GDPR." Intersoft Consulting. Accessed: 14 May 2024. https://gdpr-info.eu/

Feldstein, Steven. "The Consequences of Generative AI for Democracy, Governance and War." Survival, 65:5, 117-142. https://doi.org/10.1080/00396338.2023.2261260.

Fontes, Catarina, Ellen Hohma, Caitlin C. Corrigan, and Christoph Lütge. "AI-powered public surveillance systems: why we (might) need them and how we want them." Technology in Society, Volume 71, November 2022. https://www.sciencedirect.com/science/article/pii/S0160791X22002780

Flournoy, Michele. "AI Is Already at War." Foreign Affairs. Nov/Dec 2023, Vol. 102 Issue 6, p56-69.

Gesk, Tanya and Michael Leyer. "Artificial intelligence in public services: When and why citizens accept its usage." Government Information Quarterly, Volume 39, Issue 3, July 2022. https://www.sciencedirect.com/science/article/pii/S0740624X22000375#bbib406

Government of Canada. “Advisory Council on Artificial Intelligence.” Innovation, Science and Economic Development Canada. 26 April 2022. https://ised-isde.canada.ca/site/advisory-council-artificial-intelligence/en

Government of Canada. *Disruptions on the Horizon – 2024 Report*. Government of Canada, Policy Horizons Canada. 22 May 2024, Accessed 23 May 2024. https://horizons.service.canada.ca/en/2024/disruptions/Disruptions_on_the_Horizon_2024_report.pdf

Government of Canada. “The Future of Generative AI.” Policy Horizons. 1 August 2023, Accessed: 23 May 2024. https://horizons.service.canada.ca/en/2023/08/01/the-future-of-generative-ai/index.shtml

Government of Canada. “Pan-Canadian Artificial Intelligence Strategy.” Government of Canada, Innovation, Science and Economic Development Canada. Date Modified: 20 Jul 2022, Accessed 23 May 2024. https://ised-isde.canada.ca/site/ai-strategy/en

Government of Canada. “Responsible Use of Artificial Intelligence (AI): Exploring the Future of Responsible AI in Government”. Government of Canada. Accessed 14 May 2024. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html

Government of the United Kingdom. *National AI Strategy*. 22 September 2021, Last updated: 18 December 2022. https://www.gov.uk/government/publications/national-ai-strategy

Grome, Erich. “Spectres of the Sea: The United States Navy's Autonomous Ghost Fleet, its Capabilities and Impacts, and the Legal Ethical Issues that Surround.” Journal of Maritime Law and Commerce, 49(1), January 2018. 31-69. https://www.proquest.com/docview/2036208261

Habib, Jacky. “In Xinjiang, China, surveillance technology is used to help the state control its citizens.” Canadian Broadcasting Corporation, the Passionate Eye. 12 August 2024, Accessed: 24 May 2024. https://www.cbc.ca/passionateeye/features/in-xinjiang-china-surveillance-technology-is-used-to-help-the-state-control

Haswell, Rob. “Development, Adoption, and Integration of Artificial Intelligence: National Security Implications.” Canadian Global Affairs Institute. January 2024. https://www.cgai.ca/development_adoption_and_integration_of_artificial_intelligence_national_security_implications

Heath, Ryan. “UN deadlocked over regulating AI.” Axios. 21 September 2023, Accessed: 24 May 2024. https://www.axios.com/2023/09/21/global-ai-regulator-united-nations

Horowitz, Michael C., Lauren Kahn, and Laura Samotin. “A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation.” Foreign Affairs. May/June 2022, Vol. 101 Issue 1, p157-164.

Kendall-Taylor, Andrea, Erica Frantz, and Joseph Wright. “The Digital Dictators: How Technology Strengthens Autocracy.” Foreign Affairs. March/April 2020, Vol. 99 Issue 2, p103-115.

Lamparth, Max and Jacquelyn Schneider. “Why the Military Can’t Trust AI: Large Language Models Can Make Bad Decisions- and Could Trigger Nuclear War.” Foreign Affairs. 29 April 2024, Accessed: 23 May 2024. https://www-foreignaffairs-com.cfc.idm.oclc.org/united-states/why-military-cant-trust-ai

Nelson, Alondra.“The Right Way to Regulate AI: Focus on Its Possibilities, Not Its Perils” Foreign Affairs. 12 January 2024, Accessed: 23 May 2024. https://www-foreignaffairs-com.cfc.idm.oclc.org/united-states/right-way-regulate-artificial-intelligence-alondra-nelson

Nichols, Michelle. “UN Security Council meets for first time on AI risks.” Reuters. 18 July 2023, Accessed: 4 May 2024. https://www.reuters.com/technology/un-security-council-meets-first-time-ai-risks-2023-07-18

Maggioncalda, Jeff. “4 ways public-private partnerships can bridge the AI opportunity gap.” World Economic Forum. 8 January 2024, Accessed: 24 May 2024. https://www.weforum.org/agenda/2024/01/public-private-partnerships-ai-reskilling/

McCarthy, Dave. “Highlights From the 2024 National Defense Authorization Act (NDAA) and What It Means for the Security Industry.” Security Industry Association. 30 January 2024, Accessed: 24 May 2024. https://www.securityindustry.org/2024/01/30/highlights-from-the-2024-national-defense-authorization-act-ndaa-and-what-it-means-for-the-security-industry/

Nelson, Alondra. “The Right Way to Regulate AI - Focus on Its Possibilities, Not Its Perils.” Foreign Affairs. 12 January 2024, Accessed: 24 May 2024. https://www.foreignaffairs.com/united-states/right-way-regulate-artificial-intelligence-alondra-nelson

Nossal, Kim. “Geography and Canada’s National Interests.” The Institute for Peace & Diplomacy. 18 July 2022, Accessed: 24 May 2024. https://peacediplomacy.org/2022/07/18/geography-and-canadas-national-interests/

Payne, Kenneth. “Artificial Intelligence: A Revolution in Strategic Affairs?” Survival, 60:5, 7-32. https://doi.org/10.1080/00396338.2018.1518374

Puscas, Ioana. “AI and International Security - Understanding the Risks and Paving the Path for Confidence Building Measures.” The United Nations Institute for Disarmament Research

(UNIDIR). 12 October 2023. https://unidir.org/wp-content/uploads/2023/10/UNIDIR_AI-international-security_understanding_risks_paving_the_path_for_confidence_building_measures.pdf

Scharre, Paul. "The Perilous Coming Age of AI Warfare - How to Limit the Threat of Autonomous Weapons." Foreign Affairs. 29 February 2024, Accessed: 23 May 2024. https://www-foreignaffairs-com.cfc.idm.oclc.org/ukraine/perilous-coming-age-ai-warfare

The White House. "The Impact of Artificial Intelligence on the Future of Workforces in the European Union and the United States of America." 5 December 2022. https://www.whitehouse.gov/wp-content/uploads/2022/12/TTC-EC-CEA-AI-Report-12052022-1.pdf

The White House. *National Artificial Intelligence Research and Development Strategic Plan – 2023 Update*. Select Committee on Artificial Intelligence of the National Science and Technology Council. May 2023. https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf

The White House. *Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem An Implementation Plan for a National Artificial Intelligence Research Resource*. National Artificial Intelligence Research Resource Task Force. January 2023. https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf

United Kingdom House of Lords. "Proceed with Caution: Artificial Intelligence in Weapon Systems." AI in Weapon Systems Committee, Report of Session 2023–24. 1 December 2023. https://committees.parliament.uk/publications/42387/documents/210740/default/

United States Department of Homeland Security. "Mitigating Artificial Intelligence (AI) Risk." Department of Homeland Security. April 2024. https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf

United Nations. *Chapter VI - Governance and Institutions*. United Nations Department of Economic and Social Affairs. 1 March 2016. https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/2015wess_ch6_en.pdf

Willett, Marcus. "The Cyber Dimension of the Russia–Ukraine War." International Institute for Strategic Studies (IISS). Published: 4 October 2022. https://doi.org/10.1080/00396338.2022.2126193

Willett, Marcus. "Cyber instruments and international security." Survival, 64:5, 7-26. Published: 12 March 2019, Accessed: 15 May 2024. https://www.iiss.org/online-analysis/online-analysis/2019/03/cyber-instruments-and-international-security/

Zhang, Jiayu. “China’s Military Employment of Artificial Intelligence and Its Security Implications.” The International Affairs News. Published: 16 August 2023. Accessed: 20 May 2024.https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap