# How AI is harnessed matters

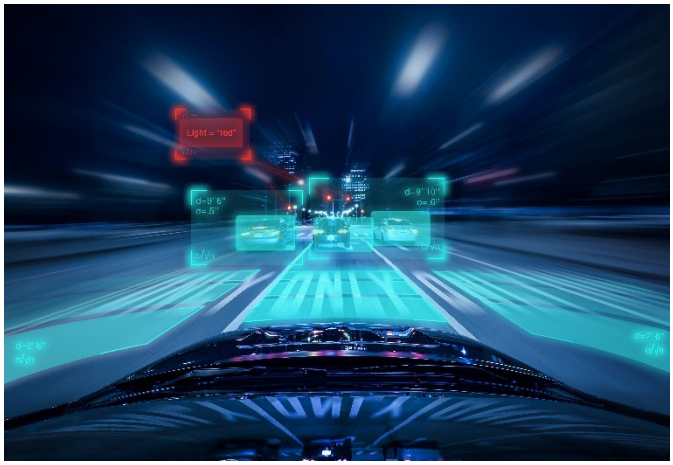
This article was first published in the
Canadian Defence Review Magazine in April 2021

## Five guiding pillars for ethical AI

Artificial intelligence (AI) is all around us.
We see AI algorithms widely used in all sectors in many ways, ranging from healthcare diagnostics, traffic management, and climate change modelling to predicting stock market trends, detecting fraud and, perhaps disturbing to some, tracking people through facial recognition.

AI is commonly used to analyze data and identify underlying patterns, improve planning and optimization, enhance knowledge capture and extraction, automate back-office processes, and analyze images or videos. On a business level, AI propels new product development, enables new customer experiences, and changes the nature of work itself. Using AI in government means balancing innovation with the ethical and responsible use of emerging technologies.

The pandemic is hastening AI adoption worldwide, the speed of which requires that we not lose sight of its ethical applications.



In no industry is ethical AI more vital than in the defence sector, where the focus is on the exceptional volume of data from multiple sources and domains and the need make fast yet effective decisions.

Here, AI – paired with military personnel or hardware such as autonomous weapons systems (AWS)– speeds command decision-making, helps to deter threats and protects national security. But, there can be no doubt that AI is reshaping the battlefield, the very character of war itself, and may well impact the balance of power in international conflict. The stakes are high, the risks huge. AI must be built on and reflect our democratic values, in line with United Nations and OECD principles[1], and deployed responsibly in both non-combat and combat functions. How AI is harnessed matters. Trust matters. AI must be responsible, equitable, traceable, reliable, and governable.[2] These are overarching principles outlined by the U.S. Defense Innovation Board and match the guiding principles set out by the Government of Canada, albeit expressed differently.[3]

There are other potential challenges and considerations. What's the right balance of commercial and government funding and data sharing for AI development? How will datasets required for enemy analysis be shared and kept secured among NATO countries? How, in the West, do we compete with authoritarian regimes who do not adhere to the ethical development and use of AI?

Ethical AI is about taking action. In the private sector, we point an organization toward a "true north" of corporate and civil ethics around AI. Our five guiding pillars are also be applicable to the Defence industry[4]:

1. Prepare employees: The rise of powerful analytics and automated decision-making fundamentally changes roles and tasks. Leaders need to prepare for wide-

[1] https://www.oecd.org/going-digital/ai/principles/
[2] DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF (defense.gov)
[3] Responsible use of artificial intelligence (AI) - Canada.ca
[4] Ethical AI: Five guiding pillars (kpmg.us)

scale change management now. New skills are needed, and people need help adjusting to the role of machines in their jobs. A new KPMG study, *Thriving in an AI World*, finds that nearly four in five U.S. government leaders would like their organizations to adopt AI more aggressively and 71 per cent said their employees are prepared for AI adoption in terms of their skill set.[5]

2. Develop strong oversight and governance: Establish clear policies about the deployment of AI, including the use of data, standards of privacy, and governance.
3. Align cybersecurity and ethical AI: Build strong security into the creation of algorithms and data governance. Security and governance of data are crucial to the overall integrity of the model. As well, clear lines of ownership need to be established for accountability.
4. Mitigate bias: Ensure the goal and purpose of critical algorithms are clearly defined and documented. Attributes used to train algorithms must be relevant, appropriate for the goal, and allowed for use. Every leader should embrace the moral imperative to mitigate bias by governing AI along its entire lifecycle – that means understanding and being able to explain what's in the black box and why.
5. Create "contracts of trust". Let the public know how you are being transparent and what decisions about their personal data will mean to them.

The AI industry is constantly evolving and is largely unregulated.

Much work is well underway around the responsible use of AI and data governance in Canada and worldwide. Canada and France co-led the creation of the Global Partnership on Artificial Intelligence (GPAI) to bring together expertise from 15 countries (including all five-eyes nations).i. Canada recently hosted the inaugural GPAI summit with participants from science, industry, government and academia to foster innovation and guide the responsible development and use of AI.[6]

As outlined by the Canadian Forces Intelligence Command (CFINTCOM), AI has significant potential for transforming the business of defence in Canada but is currently limited by both cultural and technical barriers. As such, managing the ethical implications of AI within DND/CF still requires a detailed review of the people, processes, and systems.[7]

The successful adoption of AI in the military will be gradual, not revolutionary. But it is coming – and uncontrolled AI is a risk the world cannot afford.

## Contact us

**Grant McDonald**
Global Sector Leader, Aerospace & Defense
T: +12464343900
E: grantmcdonald@Kpmg.BB

*Grant McDonald is the Global Aerospace and Defense Industry Sector Leader at KPMG in Canada. For more information, visit http://www.kpmg.ca.*

[5] Impact of AI on government decision-makers (kpmg.us)
[6] https://www.canada.ca/en/innovation-science-economic-development/news/2020/12/canada-concludes-inaugural-plenary-of-the-global-partnership-on-artificial-intelligence-with-international-counterparts-in-montreal.html

[7] https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/adm-dia.html