INTELLIGENCE ASSESSMENT SECRETARIAT | SECRÉTARIAT DE L'ÉVALUATION DU RENSEIGNEMENT

ARTIFICIAL INTELLIGENCE (AI) RISK INVENTORY

UNCLASSIFIED / NON CLASSIFIÉ
FOR OFFICIAL USE ONLY / UTILISATION OFFICIELLE SEULEMENT
MAY 2023

Analyst: Economic Security and Technology Program, Graphics: H. Cardichon, K. Barban

WHO?

Allies and adversaries seek to secure AI advantage and manage AI's growing risks. The AI community increasingly warns of these risks, amid rapid AI development and use.

WHAT?

Risks are inherent; human harm has already occurred and some future hazards are likely unavoidable. Baseline risks are compounded by threat actors who will deliberately use AI to inflict harm.

WHY?

Failures to anticipate and mitigate AI risks will likely impose significant costs. The consequences will be measured across our sovereignty, democracy, human rights, safety, security, and prosperity.

	GOVERNANCE LAG	SOCIETAL DISRUPTION	ECONOMIC IMPACTS	SYSTEMIC VULNERABILITY	STRATEGIC SURPRISE
WHAT?	Governments and regulators are falling behind AI development and adoption. The pace of change means this lag will continue.	AI tools reflect wider biases and stereotypes in society, and have no understanding of the meaning of their output, nor whether it is false, offensive, or harmful.	New business models, markets and job categories are emerging for AI. Adoption of AI tools will change the nature of work across many industries.	AI is being integrated into a wide range of everyday digital services and platforms, but its supply chains and vulnerabilities are poorly understood.	AI capabilities are increasingly sophisticated and applicable to a broader range of tasks.
SO WHAT?	Competition is instilling an AI race mentality. The development and use of AI puts human rights and established democratic and legal principles at risk, including protection of privacy and personal data, transparency of decision-making, and accountability for harms.	Use of AI tools risks creating biased outcomes and harmful outputs, particularly affecting communities and individuals already facing discrimination. AI can amplify the scale, speed and scope of misinformation. It will be increasingly difficult to distinguish between AI and human-created content.	Adoption of AI will result in broad and unevenly distributed labour and market disruption. This will likely include significant displacement of human workers in several sectors and activities, even rendering some jobs obsolete. The scope and timeline for AI's impact across industries and jobs will vary.	The inputs to AI systems (including energy and data) are opaque, and ownership and control of underlying models are concentrated in a handful of firms. AI systems cannot yet be reliably tested or validated. This creates a risk of becoming reliant on a brittle and fragile yet widely-deployed technology.	The "intelligence" of the current generation of AI is distinctly inhuman. The complexity of the underlying models means developers do not fully know how their AI systems operate or can be used.
NOW WHAT?	Anxiety over AI development and use is triggering legislative and regulatory responses. China and the European Union lead the way in setting legislative frameworks for managing some AI risks, and may limit options for late-movers.	Opaque algorithmic decision-making, and erosion of verifiable and shared truth would damage societal trust in information, institutions and each other.	Widespread use of AI will change the skills needed by the future workforce, including the technical AI-specific skills now in high demand. AI may further embed international labour patterns, or create opportunities for their disruption.	AI is likely to become part of the infrastructure underpinning many societal and economic functions. This will create new challenges for securing the resilience of those critical functions.	The future of AI technology is highly uncertain. There is a likelihood of unexpected and unintended leaps in capability – leading to moments of strategic surprise.

Government of Canada Privy Council Office | Gouvernement du Canada Bureau du Conseil privé

This AI Risk Inventory benefits from consultation with academia, private sector, Government of Canada, and Five Eyes partners

Canada

INTELLIGENCE ASSESSMENT SECRETARIAT | SECRÉTARIAT DE L'ÉVALUATION DU RENSEIGNEMENT

UNCLASSIFIED / NON CLASSIFIÉ
FOR OFFICIAL USE ONLY / UTILISATION OFFICIELLE SEULEMENT

AI WILL ALMOST CERTAINLY BE USED BY THREAT ACTORS, SUCH AS STATES, EXTREMISTS, OR CRIMINALS, TO...

CONSIDERATIONS

- Intent and capability varies enormously across actors.
- Many AI systems are open and publicly accessible.
- Limits set by AI providers can be manipulated and overcome.

	CREATE AND SPREAD DISINFORMATION AND DEEPFAKES	BOOST CYBER ATTACK CAPABILITIES	CREATE AND PROLIFERATE WEAPONS	TARGET AND SURVEIL PEOPLE	ENHANCE MILITARY CAPABILITY
WHAT?	AI tools will be used to create inauthentic but persuasive online profiles, and misleading or deceitful content, at scale.	AI will augment many methods used to compromise and access networks and devices, including vulnerability discovery, malware design, and spear-phishing.	AI tools can be used to identify and assemble high-risk information about making dangerous substances or weapons, and even obtain components.	AI tools can be used to conduct targeting analysis and modelling, and make predictions, with population-scale data.	AI will likely enable new lethal autonomous weapons, accelerate battlefield decision-making, and support logistical functions for military operations.
SO WHAT?	Disinformation campaigns and information operations may reach more people and be more influential. This risks exacerbating existing disinformation effects, through manipulating public and market sentiment, interfering with policy and democratic processes, or damaging diplomatic relations.	AI is likely to add to already unmanageable volumes of cyber threat activity, and could overwhelm current approaches to cyber security. AI may degrade the efficacy of authentication, and adversarial techniques may help create tools capable of evading advanced detection.	Discovery of novel weapons and means of attack by non-state actors could increase the risk of proliferation of destructive capabilities, such as chemical or biological weapons. However, AI tools may not help a threat actor overcome all barriers to achieving these capabilities.	AI could bolster surveillance and targeting capabilities for espionage, radicalisation and commercial purposes. This could enhance discovery of individual patterns of life, vulnerabilities and susceptibility; improve behavioural prediction; and deepen personalization and persuasiveness in foreign intelligence operations.	A lack of international norms creates uncertainty over how AI will be used in conflict - minimal human control could provide an advantage but erode accountability. Open access to sophisticated AI systems may lead to a proliferation of advanced military capabilities.
NOW WHAT?	Determining the authenticity of information, and detecting disinformation and its impacts, are already difficult. A pervasive environment of amplified deception will likely degrade institutional and societal trust, challenging the basis of democracy and sovereignty.	The benefits of progress in AI technologies will accrue to both cyber attackers and defenders, but which side it will benefit more is uncertain. Defending against AI-enabled attacks will likely require new practices and tools, possibly including AI tools for cyber security.	The accessibility of more specialized AI tools and platforms may grant previously state-level capabilities to non-state threat actors. Unconventional biological and chemical synthesis techniques are more likely to evade existing control regimes.	AI-enabled capabilities will likely create challenges (and opportunities) for Canadian and allied intelligence operations, while enhancing adversaries' ability to leverage non-traditional collection avenues. These capabilities may also inform other threat activities, such as influencing public opinion or widening divisions.	Unpredictable autonomous systems would pose a risk of accidents, or unintended escalatory action. Asymmetry in capability could disrupt conventional doctrine or cause battlefield surprise.

Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

This AI Risk Inventory benefits from consultation with academia, private sector, Government of Canada, and Five Eyes partners

Canada