

Artificial Intelligence

Briefing paper

1/9

Artificial Intelligence (AI) refers to the ability of machines to perform tasks that traditionally require human intelligence, such as pattern recognition, learning from experience, drawing conclusions, and making predictions. AI enhances digital computer software and physical autonomous systems. It will likely play a prominent role in combat models and simulation, target detection and recognition, decision support, cyber defence and autonomous vehicles.



Implications

Economic Implications – AI is expected to contribute over \$15.7 trillion to the global economy by 2030, and has already enhanced business analytics efficiencies and driven scientific, mathematical, and engineering discoveries. Recent breakthroughs include large language models (LLMs) and advanced text-to-image models generating highly realistic images. Insufficient numbers of AI professionals in many countries, however, could hinder some nations in competitive global markets.

Military Implications – AI is already being used to power advanced cyber-attacks, electronic warfare, and digital disinformation, and provide commanders with improved intelligence analysis. Eventually, AI may allow a single operator to control swarms of uncrewed vehicles for intelligence, surveillance and reconnaissance (ISR), and combat missions. Sophisticated real-time automated data analysis from sensor inputs will provide critical decision support and enhanced actionable intelligence, target detection and recognition.

Additionally, AI will improve training capabilities through virtual and augmented reality (VR/AR), and highly realistic modelling and scenario planning.

Societal Implications – Unregulated generative AI could majorly propagate disinformation. Believable 'deep fake' videos of public figures and AI-supported disinformation campaigns are already disrupting the political landscape. AI is also likely to impact labour markets and make certain roles that entail routine, repetitive tasks (including manual manufacturing, data entry, customer service and basic administrative support) redundant. Current AI models have raised ethical concerns around biased data inputs, lack of transparency on how outputs are created, and the use of LLMs by malign actors intending to cause harm. Trust in AI is crucial for widespread adoption and, as such, the technology needs to be reliable, safe and transparent. 'Explainability', or the ability of AI to provide understandable reasons for decisions, as well as training and education, will be key for building trust.



Key Technology Areas

Deep Learning and Neural Networks – A subset of machine learning, these networks emulate brains' computational processes. They are highly adaptable, have broad applicability, and are capable of continuous learning. Research is currently focused on enhancing AI systems' agility and resilience. One approach is to increase data volume through federated learning (or collaborative learning) to train future computer models on de-centralised datasets, while another is to streamline cumbersome data labelling for training purposes. Additionally, there are efforts to integrate a baseline level of "machine common sense" for more effective, robust, and agile systems with human-like reasoning.

Applications – AI will have an extremely broad range of applications, integrating and advancing many systems, processes and defence capabilities. This will enable new

scientific methods, driving scientific discovery. Human-machine teaming, an effective psycho-social-technical collaborative system, is crucial for future AI applications, for which reproducibility and trust will require research.

Counter-AI – Detecting, deflecting, and limiting attacks on the Alliance's AI systems and defending against adversarial AI are becoming increasingly necessary. For example, AI-on-AI engagements are gradually emerging, driving disinformation. Furthermore, potential for criminal uses of AI is underappreciated. While AI currently excels under specific conditions, it can fail with slight deviations from expected parameters. Assessing reliability is difficult, yet vital for enhancing resilient and validated AI to counter adversarial AI. Deception of AI will hence become a significant aspect of future warfare.



Technology Convergence

Robotics and Autonomous Systems – Data, Autonomy, and AI are expected to significantly disrupt military capabilities over the next decade. The proliferation of ubiquitous, intelligent and interconnected sensors will facilitate AI-assisted decision-making in cyberspace and physical domains. Physically, these will include autonomous aerial, naval and ground vehicles, and swarms. VR, autonomy and AI will facilitate surveillance, cyber defence, electronic warfare and signals intelligence, collecting data autonomously and implementing countermeasures.

Biotechnology, Materials and Energy – AI will contribute to the design, development and manufacturing of novel materials with unique properties, and also the direct manipulation of both biological and chemical reactions. This will lead to numerous dual-use applications that are of interest to NATO, ranging from biotechnologies and 3D/4D (bio)printing, energy storage, power generation and propulsion systems.