

United Kingdom perspectives on the opportunities and challenges to international peace and security from the application of artificial intelligence in the military domain

Artificial Intelligence (AI) is a family of general-purpose technologies, any of which may enable machines to perform tasks that would traditionally require human or biological intelligence, especially when the machines learn from data how to do those tasks. AI technologies are maturing and being adopted at extraordinary pace. As a group of technologies with different systems, methods and applications, they have different developmental trajectories and implications. What is certain is that they have the potential to drive transformational change across all aspects of society, economy and policy, including defence and security.

The UK welcomes the opportunity presented by resolution 79/239 to consider the implications of AI in the military domain beyond those related to lethal autonomous weapons systems (LAWS), which have been subject to extensive and valuable discussions, including those ongoing in the Group of Governmental Experts established under the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons. A rigorous assessment of the broader strategic implications of military AI, bringing together thinking, ideas and good practices discussed in informal and formal international fora on this agenda, will allow for a holistic discussion on how to make the most of the opportunities AI presents in the military domain, while addressing effectively associated risks.

Opportunities of AI in military domain

The integration of AI in the military domain will potentially transform defence, global security dynamics and the character of warfare. Advanced technologies enabled by AI which can categorise and refine large quantities of data from different sources, faster and more comprehensively, will support greater efficiency and improved decision making, and accelerate the tempo and rigour of operational planning. AI in intelligence, surveillance, reconnaissance (ISR) systems can provide a more accurate picture of the operational context and enable planners to reduce the impact on civilians – resulting in greater protection for civilians and civilian infrastructure. Autonomous logistics and unexploded ordinance functions will reduce the need to have military personnel on the ground. AI in the military context could therefore strengthen national and international security and lower the risk to human life and reduce casualties.

UK Ministry of Defence's research on AI and peacekeeping identified ways in which peace operations could benefit from AI-enhanced capacities and systems, including:

- analytical capability that will improve situational awareness, operational decision making, scenario planning and sentiment analysis capability.
- autonomous systems, such as unmanned aerial vehicles (UAVs) could provide enhanced coverage of large geographical areas or high-risk regions (where it may be risky for peacekeeping personnel to maintain a permanent presence).
- logistics could improve delivery of healthcare and aid provision to local populations, supporting mission objectives and building community trust.

Such capabilities can be applied to enhance monitoring and verification of arms control and peace agreements, making it easier to detect violations or confirm compliance in a timely and credible manner. AI tools could enable better detection, identification, attribution and verification of hostile sub-threshold operations of various kinds, which would reduce the effectiveness of such activities and potentially deter them in the first place. They can help also to monitor and identify online hate speech, propaganda or changes in public sentiment in real time that might escalate tensions or undermine any peace talks or ceasefire.

Challenges and risks

AI use in the military context may exacerbate existing risks and pose additional threats both above and below the threshold of armed conflict. The rush to adopt AI-capabilities to gain strategic advantage, could result in countries using AI in ways that are unacceptable on legal, ethical or safety grounds. New risks of AI-induced escalations or accidents caused by malfunctions or the fragility, brittleness, immaturity or insecurity of AI systems will require new protocols and de-escalation mechanisms. Hostile actors may seek to attack national AI systems and undermine confidence in their performance, safety and reliability (e.g. by 'poisoning' data sources, corrupting hardware components within supply chains, and interfering with communications and commands), which could disrupt systems and skew military decision making in times of crisis and other operational environments.

In times of conflict, these technologies – and the operational tempo they enable – are likely to compress decision times dramatically, tax the limits of human understanding and may require responses at machine speed. The black box nature of many AI capabilities means that humans are often unable to discern how or why a particular output has been delivered. AI-driven operations may lead to unpredictable and opaque behaviour and make accurate inferences and judgements about the intent of an adversary difficult or could be misinterpreted or provoke unintended consequences. Operators could place excessive confidence in algorithmic outputs without a full grasp of the underlying assumptions, constraints and flaws of AI systems. Without appropriate safeguards, norms and protocols in place, AI-driven systems could exacerbate the risk of misunderstanding, miscalculation and unintended escalation.

The widespread availability of advanced AI capabilities/tools and other dual-use technologies likely increases proliferation risks and development of novel weapons by state and non-state actors. AI could be used also to augment or advance disinformation attempts designed to engender hostility towards countries, which could cause conflict and escalate tensions.

UK commitment to secure and responsible AI in the military domain

The UK recognises that AI raises profound concerns about fairness, bias, reliability, and the nature of human responsibility and accountability, especially in a military context. While States have a long history of incorporating new technologies and will continue to rely on long-established legal, safety and regulatory regimes, we must recognise the particular challenges arising from the nature of AI and importance of positively demonstrating that we are responsible and trustworthy.

The UK sets out its commitment to secure and responsible AI through its Defence AI Strategy and associated AI Ethics Principles. These AI Ethical Principles, set out in the UK's 'Ambitious, Safe, Responsible' policy, establish the ethical framework considerations of Human-Centricity, Responsibility, Understanding, Bias and Harm Mitigation and Reliability. The Joint Service Policy "Dependable Artificial Intelligence (AI) in Defence" published in November 2024, provides clear direction to the teams within Defence and beyond on how to implement these AI Ethical Principles to deliver robust, reliable and effective AI-enabled services and capabilities.

Through its AI Ethical Principles, the UK seeks to cultivate trust in AI technologies and their applications, realising the full potential of human-machine teaming, while mitigating the risks associated with its use, misuse or disuse and preventing unintended consequences. This approach allows the UK to harness the innovation and creativity found across Defence and industry in a way that will enable the ambitious adoption of AI-enabled solutions.

The UK government is clear that any UK use of AI to enhance defence processes, systems or military capabilities is governed by national and international law. UK Defence always seeks to abide by its legal obligations across the full range of activities from employment law to privacy and procurement, and the law of armed conflict, also known as International Humanitarian Law (IHL). It has robust practices and processes in place to ensure its activities and its people abide by the law. These practices and processes are being – and will continue to be – applied to AI enabled capabilities. Deployment of AI-enabled capabilities in armed conflict needs to comply fully with IHL, satisfying the four core principles of distinction, necessity, humanity and proportionality. We are clear that use of any system or weapon that does not satisfy these fundamental principles would constitute a violation of international law.

Human responsibility and accountability exercised through context-appropriate human involvement is also crucial. This context-appropriate human involvement is necessary to satisfy our policies, ethical principles and obligations under IHL. The nature of human involvement will vary depending upon the nature of the capability, operational environment, and context of use. The UK will ensure that human political control of its nuclear weapons is maintained at all times.

UK contribution to international initiatives

Global stability requires the ambitious, but responsible development of military AI. The international community's understanding of the risks, safeguards and standards related to AI use in the military context continues to evolve. Given that the risks are inherently international in nature, they require a global response.

The UK has been at the forefront of international efforts in support of secure and responsible development and use of AI. It is proud to have hosted the inaugural AI Safety Summit, which agreed the Bletchley Declaration on AI safety, and to have played a role in commissioning the International AI Safety Report - the world's first comprehensive synthesis of current literature of the risks and capabilities of advanced AI systems – published in February 2025, which builds understandings critical to informing international discussion, such as harnessing AI for peace and

security. We support efforts under the Global Digital Compact to close digital divides and enhance international governance on AI for the benefit of humanity.

The UK actively supports international initiatives to drive action in relation to the military domain. We have supported work by organisations like RAND Europe, University of California, Berkeley and the Global Commission (GC) for Responsible Uses of AI in the Military Domain (REAIM) to bring together diverse and widely recognised experts to explore these issues, make sense of the latest thinking and map out way forwards for policymakers with workable recommendations.

The UK continues to be an active participant in international dialogues on AI-related defence and security issues and continues to share its experiences of developing and operationalising secure and responsible approaches to AI adoption within the military domain. The UK welcomes progress made through initiatives like the REAIM Summits, which the UK co-hosted in 2024, and US-led Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy to increase understanding of the opportunities and strategic risks, and how to address these through appropriate measures that support secure and responsible AI use. AI ethics and assurance are dynamic fields that require continuous engagement, collaboration, and iteration.

Looking ahead

The UK looks forward to building on progress made to date in existing processes, including through discussions in the United Nations based on the Secretary General's report and focussed on tangible actions. Given the nature of AI in the military context, it will be crucial to have an inclusive and multi-stakeholder approach, informed by technical, military, and legal expertise from States, industry, academia and civil society.

While we have an abundance of information, our collective understanding of military applications and implications remains low and there remain substantial knowledge gaps and misunderstandings about the nature and capabilities of AI. Further work is required to build capacity of States, enhance our collective understanding of the implications and potential risks and challenges of military AI at the strategic level and establish universally agreed terminology to allow for constructive discussions. Discussions should focus on tangible, effective and appropriate measures and practices that could help address risks, including such things as safeguards and norms of behaviour, new communication channels and transparency mechanisms to reduce the risk of misinterpretation, updated doctrines, confidence-building measures and arms control agreements that reflect the impact of military AI.