11 April 2025

Norway. Submission to the United Nations Secretary-General pursuant to UNGA resolution 79/239.

Norway welcomes the opportunity to submit its views on "the opportunities and challenges posed to international peace and security by the application of artificial intelligence in the military domain, with specific focus on areas other than lethal autonomous weapons systems", pursuant to resolution 79/239 "Artificial intelligence in the military domain and its implications for international peace and security".

As recognised in the Secretary-General's July 2023 policy brief A New Agenda for Peace, AI is both an enabling and a disruptive technology that is being increasingly employed in a wide array of civilian, military, and dual-use applications. AI's increasing ubiquity, coupled with rapid scalability, lack of transparency, and pace of innovation, presents potential risks to international peace and security and poses governance challenges.

As a consistent advocate of international law, multilateralism, and responsible innovation in the defence sector, Norway supports efforts to promote common understandings, strengthen governance and develop adequate regulation of artificial intelligence (AI) in the military domain. As a minimum starting point, AI applications in the military domain must be developed, deployed and applied in a responsible manner throughout their entire life cycle and in compliance with applicable international law, in particular, international humanitarian law.

Importantly, resolution 79/239 affirmed the applicability of international law, including the UN Charter, international humanitarian law, and human rights law in the use of AI in the military domain and stressed the importance of responsible, human-centric AI use.

AI as an enabling technology holds extraordinary potential to transform every aspect of military affairs, including procurement, hardware, software, operations, command and control, strategic communications, surveillance, intelligence, training, information management and logistical support. The application of AI in the military domain presents foreseeable and unforeseeable opportunities and risks on both the tactical and strategic level. As a general-purpose technology, AI represents a force multiplier with a capacity to reshape the conduct of warfare. Technological convergence between artificial intelligence, neurotechnology, synthetic biology and quantum computing adds further complexity.

It is foundational that AI is developed, deployed, used and governed responsibly, in line with fundamental ethical principles, in strict compliance with states' obligations under international law, including international humanitarian law and human rights law, and with risk identification and mitigation at the very core.

The Norwegian Strategy for Artificial Intelligence in the Defence Sector (2023) outlines key areas where AI may contribute constructively to areas other than lethal autonomous weapons systems:

- Enhanced situational awareness and decision support: The utilisation of AI is both a possibility and a necessity in intelligence, surveillance and reconnaissance, as large and increasing volumes of data cannot be analysed manually. AI can be used for filtering out relevant data, for example by pre-processing data, automatic translation or detection of special objects in images, detecting anomalies and repetitions, as well as cross-checking information to detect attempts at disinformation. Improvements in this area can lead to more effective, precise operations and reduced loss of life.

- Cyber defence: Digitalisation and increased dependence on ICT introduce vulnerabilities along with the benefits. The digital space provides threat actors with the opportunity to commit data breaches, engage in espionage and sabotage and conduct influence campaigns. AI can support the defence sector's ability to detect, monitor, report, manage and counter digital threats. Among other things, the use of AI can more quickly provide a more complete picture of goals and complex relationships, collect information from relevant sources and streamline the use of analysis. Knowledge and expertise development relating to how AI can constitute a digital threat are essential to being able to detect and avert digital attacks in the future. AI therefore has to be a central element in the further development of the sector's defence against digital threats, both through existing and future instruments.

- Logistics: Successful, effective military operations depend on effective logistics support. By streamlining logistics using systems that adopt AI, better operational capability and greater preparedness can be ensured. Applications of AI in the civilian logistics sector has already progressed far. Many of these could likely be easily adapted for use in the military sector.

- Support activities: Many military support activities could likely be improved and streamlined using AI. This includes tasks that support and strengthen operational capability, such as operating and maintaining materiel, procuring, managing and disposing of materiel and buildings, recruiting, training and managing personnel and delivering common services such as accounting and archiving. AI has the potential to strengthen support activities through improved utilisation of data for analyses and decision-making support, automation of tasks and improved ability to handle information and knowledge. This could make it possible to switch to a model of predictive maintenance, improved information flow, introduce new and better support systems for HR management and improved modelling of cost trends for materiel and buildings. A successful introduction of AI technology in support activities could therefore lead to reduced time consumption and increased efficiency.

Additionally, AI applications in the military domain have the potential to enhance the implementation of international humanitarian law and assist in efforts to protect civilians and civilian objects in armed conflicts. It can be beneficial to peacebuilding and peacekeeping activities, and enhance verification and monitoring capabilities for arms control, disarmament and other compliance regimes.

AI in the military domain also introduces unprecedented challenges. AI has inherent vulnerabilities that can have unintended consequences and lead to the degradation of meaningful human control, responsibility and accountability. The use of deep learning has the potential to make AI models hard to understand, explain and predict. Lack of understanding can for instance render conflict escalation dynamics more opaque and unpredictable.

Effective safeguards must be in place to ensure that humans retain meaningful control and oversight over the development, deployment and use of AI. This is particularly important the closer the application is to combat operations and the use of force, e.g. decision support systems. Accountability and responsibility for the use and effects of military AI must always remain with humans.

AI systems may be highly sensitive to the quality and representativeness of training data. Possible biases, des- and misinformation, or incomplete training data can lead to models that generate inaccurate or discriminatory results. Automation bias can cause over-reliance by the human user on the outputs of the system.

Highly automated or autonomous response capabilities in the cyber domain—particularly those without adequate human-in-the-loop mechanisms—may lead to unintended responses and rapid escalation.

Increased reliance on cyber technology for tasks that previously were performed manually or with basic automation also comes with the risk of malicious exploitation of vulnerabilities in that technology. Increasing reliance on commercial systems raises concerns about dependency on external providers, loss of control over updates, and other vulnerabilities related to proprietary systems.

The aforementioned are mere examples of potential risks associated with the application of AI in the military domain. There are also many unknown unknowns. In a military context, these factors can, combined or by themselves, undermine mission outcomes and pose fundamental legal, ethical, humanitarian and military risks.

The Norwegian Strategy for Artificial Intelligence in the Defence Sector (2023) also outlines key principles for the responsible development and use of AI:

- Lawfulness: AI applications must be developed and used in accordance with international law, including international humanitarian law and human rights law. In the study, development, acquisition or adoption of a new AI reliant weapon, means

or method of warfare, each state is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by international human rights law or any other rule of international law applicable to the state.

- Responsibility and accountability: Human responsibility and accountability for the use of AI must be ensured. Decision-making authority over the use of an AI system and responsibility for its actual use must be unambiguously determined.

- Explainability, understandability, traceability: AI applications must be sufficiently explainable, understandable, transparent and traceable.

- Training: AI operators must have the necessary training to understand the behaviour of the AI application, including how to identify abnormal behaviour.

- Reliability, safety and security: AI applications should have explicit and well-defined scopes of use. The resilience, reliability and security of AI applications must be subject to testing and verification throughout the entire life cycle within their respective scopes of use. AI applications must have adequate levels of security and be protected against digital threats.

- Control: Meaningful human control must be ensured. AI-systems must include an interface for human-machine interaction that is adequate for its intended use, which provides the capacity to identify and mitigate unintended consequences, as well as the means to take necessary corrective action if the system operates in an unintended way.

There is need for the international community to deepen the dialogue on the military applications of AI and their implications for peace and security, including on measures to ensure responsible AI in the military domain. Particular attention should be given to systems supporting combat operations including the use of AI for situational awareness and decision-support, where undesired outputs and behaviours in the AI application, and loss of meaningful human control, can have particularly harmful consequences. There is also a need to address AI in hybrid warfare, including but not limited to AI in cyber operations, AI in electronic warfare and AI in information operations.

Norway is committed to strengthening international cooperation on information sharing and capacity building. By developing a shared knowledge base, states would promote common understanding, close gaps, enhance transparency and build trust. To this end Norway would encourage the development and publication of national strategies and policy documents related to military applications of AI. Attention should be given to risk reduction and confidence-building measures.

11 April 2025

The timely development of adequate international AI governance, with flexibility to respond to the rapid technological advancements, can help prevent technology-driven arms races whilst ensuring that innovation supports global security.