11 April 2025

Submission by Finland concerning UN GA resolution 79/239 "Artificial intelligence in the military domain and its implications for international security" to the United Nations Secretary-General

Reference: ODA/2025-00029/AIMD

Finland is pleased to submit its views on General Assembly Resolution 79/239 on "Artificial intelligence in the military domain and its implications for international security", adopted on 24 December 2024, that requests the Secretary-General to seek the 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 areas other than lethal autonomous weapons systems".

The adoption of international principles or regulations on the application of artificial intelligence in the military domain is fundamental to ensure compliance with international law, to increase security and to reduce potential risks of conflicts. At the same time, it is necessary to enable the development of national defense capabilities that do comply with international law. Finland has committed to develop, deploy, and use AI capabilities in the military domain in a responsible manner, in accordance with international law, in particular international humanitarian law, and in a way that does not undermine international peace, security and stability, while pursuing efforts on research, development, experimentation and innovation with AI technology.

It has become increasingly important to identify foreign, security and defence policy implications of disruptive technologies and to develop means for addressing them. Finland actively participates in global debates on technology regulation, advocating for fundamental and human rights, as well as addressing related risks, in the development and application of AI and relevant policies.

In addition to identifying the risks of disruptive technologies, it is also important to recognize the opportunities they offer for security, defence capability development, economic growth, productivity, sustainable development, technological competence, and sectoral investments.

1. **Opportunities**

Disruptive technologies present significant opportunities for advancing various sectors, driving the clean transition, fostering sustainable economic growth, and enhancing efficiency and productivity. They also have potential to enhance security, education, well-being and health on a global level.

AI and other emerging technologies bring opportunities for advancing defence capabilities while fundamentally shaping the future of battlefields and means and methods of warfare. Technological advancements enable more efficient information collection and data processing, heightened situational awareness, faster decision-making and more precise and longer reach of engagement. The importance of remotely-operated and autonomous unmanned systems is growing in modern warfare, and they will change the future of war, operations and the battlefield. Anticipating advancements in technology, integrating emerging technologies into defence systems and making use of the unexpected become

increasingly important as the pace of technological development picks up speed in the future. Technological edge can also compensate for numerical inferiority.

2. Challenges

At the same time, it is important to establish a wide understanding of the security threats, potential for misuse, human rights issues and interdependencies related to development of disruptive technologies such as artificial intelligence. As they develop, they will pose new challenges for the defence and security sectors, in particular. The development of AI makes cyberattacks, information influence activities and, as one of its instruments, disinformation, more targeted and effective. Furthermore, AI is already being used to influence elections. In such an environment, an increased focus must also be put on keeping confidential information secure.

International law, in particular the UN Charter, international human rights law, and international humanitarian law, fully applies to cyberspace. Respect for and adherence to the United Nations framework of responsible State behaviour in cyberspace remain essential to maintaining international peace, security and stability. Technological development raises new issues. These issues relate to, for example, the cyber environment, the use of artificial intelligence, new weapons technologies, and the exploitation of critical raw materials. Hybrid influence activities may resort to practises aimed at hindering the realisation of accountability under international law. Finland advocates taking fundamental and human rights and the risks related to them strongly into account when developing and applying AI and drawing up relevant regulation. Establishing national principles, standards and norms, policies and frameworks are important to ensure responsible AI applications in the military domain in compliance with international law.

Technological development has provided hostile actors with new opportunities to engage in hybrid influence activities exercised below the threshold of open conflict. Hostile cyber operations have become an established part of power politics and of the range of instruments available in influence activities conducted by state actors. Cyber, hybrid and information operations are also conducted under normal conditions, which may, for its part, obscure the boundaries between war and peace. Despite the increasingly technological nature of warfare, conventional warfare capabilities remain important, particularly in large-scale and long-term conflicts.

Many countries are facing intense information influence activities that also deploy artificial intelligence. The harmful use of information has become an everyday part of broad-spectrum influencing, and the competition in the information environment has increased.

Developments in infrastructure and technology and the growing number of users offer greater opportunities for hostile actions in the cyber domain. Many countries are constantly facing intelligence gathering on information networks, cyber espionage and cyberattacks by hostile actors who also strive to have physical impact on critical infrastructure. Alongside state actors, the role of politically motivated or state-led non-state actors as orchestrators of hostile activities is growing.