No. 054/2024 dated 24 June 2024

Military AI Governance:
Moving Beyond Autonomous Weapon Systems

Mei Ching Liu

SYNOPSIS

Governance of artificial intelligence in the military domain has a dominant focus on autonomous weapon systems, while AI-based decision support systems have received less attention. Given that the latter will likely be used more widely in AI-driven warfare, it is necessary to extend the focus beyond autonomous weapons systems in discussions of military AI governance.

COMMENTARY

Across several major global artificial intelligence summits in recent months, discussions regarding military AI governance have tended to focus on autonomous weapon systems (AWS). AWS, commonly known as "killer robots", have received the most attention due to an effective campaign by Human Rights Watch (HRW) to "Stop Killer Robots". The evocative image of "killer robots", which was once a mobiliser for discussions on lethal autonomous weapon systems (LAWS) at the United Nations, is now distorting and narrowing the debate on military AI applications.

Contrary to media portrayals, the use of AI in the military domain extends far beyond AWS. For example, Israel allegedly used an AI-based decision support system (ADSS) – the Lavender system – in the Gaza Strip. Observers of such military AI applications have typically failed to recognise the distinction between ADSS and AWS, thereby treating the Lavender system as an AWS. However, the Lavender system does not autonomously select and apply force to targets; it simply aids in identifying them.

Unlike AWS, which are weapon systems that, once activated, can identify, select, and engage targets without further intervention from a human operator, ADSS do not replace human decision-makers; the decisions to select and engage targets are still made by humans. Nevertheless, military applications of ADSS in Gaza and Ukraine raise doubts regarding compliance with international humanitarian law (IHL) and the ability to minimise risks for civilians. Given such doubts, policymakers should take steps to broaden current debates on military AI to encompass ADSS, building awareness, understanding, and norms of behaviour regarding their military application, particularly in decisions on the use of force.

Unlike autonomous weapon systems (AWS), AI-based decision support systems (ADSS) do not replace human decision-makers. ADSS have been allegedly used in the battlefields in Gaza and Ukraine, from identifying targets for military operations to recommending the most effective targeting options. *Image from Pixabay.*

Campaign to Stop Killer Robots

AWS were popularised by HRW in their 2012 report titled "Losing Humanity: The Case Against Killer Robots". The term "killer robots" was used to bring media attention to serious ethical and legal concerns around AWS. In 2013, HRW launched the Stop Killer Robots campaign, which successfully mobilised the international community, and the first informal meeting of experts on LAWS was held in 2014 at the United Nations. Since then, AWS have been associated or even equated with military AI, notwithstanding that AWS may or may not incorporate AI. The persistent reference to AWS on matters such as the military application of ADSS, however, is distorting the debate on the risks and challenges posed by the military use of ADSS in decisions on the use of force.

ADSS and Military Decision-making on the Use of Force

In the military context, ADSS can aid decision-makers by collecting, combining, and analysing relevant data sources, such as surveillance footage from drones and telephone metadata, to identify people or objects, assess patterns of behaviour, and make recommendations for military operations. Regarding military use of force, ADSS can be used to inform decision-makers about who or what a target is and when, where, and how to strike it.

For instance, the Lavender system allegedly used AI to support the IDF in its target selection process. Information on known Hamas and Palestinian Islamic Jihad (PIJ) operatives was used to train the system to identify characteristics associated with such

operatives. The system then combined intelligence inputs, such as intercepted chat messages and social media data, to assess the probability of an individual being a member of Hamas or PIJ. The IDF also allegedly used another ADSS – the Gospel – to identify buildings and structures used by militants.

Apart from target selection, ADSS can also assist the military in the process of target engagement. In the Ukraine/Russia conflict, ADSS were used to analyse large volumes of intelligence information, as well as radar and thermal images. The system then identified potential enemy positions, recommending the most effective options for targeting.

ADSS vs AWS – Conceptual and Legal Differences

ADSS represent a more varied category of military AI application than AWS, although some of the technologies used in both systems may be similar. For example, ADSS with facial recognition and tracking software could form part of AWS; but if a weapon system can select and engage a target without human intervention, it would be categorised as an AWS.

The main concern regarding AWS is that the system itself triggers the entire target selection and engagement process. To put it simply, humans do not choose (or know) the specific target, the precise time, or place of attack, or even the means and methods of attack. If an illegal killing is conducted by AWS, there is the question of who is responsible for such conduct. As reflected in both the Rome Statute and the 2019 Guiding Principles reached by the UN LAWS discussion, individual criminal responsibility applies only to humans and not machines. However, the challenge lies in identifying the responsible individual(s), who could include the manufacturer, the programmer, the military commander, or even the AWS operator. Therefore, the use of AWS creates what is termed an "accountability gap", where conduct potentially amounting to an IHL violation cannot be satisfactorily attributed to an individual; thus, no one is held accountable.

On the other hand, ADSS are intended to support human decision-making; they do not replace human decision-makers. Humans are theoretically "in the loop" in making the decision to select and apply force to targets. Consequently, as far as ADSS are concerned, the accountability gap problem, a thorny issue in UN LAWS discussions, may not arise to the same extent as with AWS, as ADSS are designed to retain human decision-making.

However, ADSS raise the question of what quality and level of human–machine interaction is required to ensure that their use complies with IHL obligations, notably those demanded by the principles of distinction, proportionality, and precaution. The Lavender system has been criticised for causing a high number of civilian casualties as the system's human operators allegedly served only as a "rubber stamp". This instance highlights how decision-makers could potentially end up deferring to conclusions reached by a machine, effectively making the human in the loop redundant.

Others argue that military applications of ADSS for the use of force can facilitate compliance with IHL. For instance, ADSS can aid human decision-makers in

[determining the most appropriate means of attack](#) by considering target and environment data as well as weighing the potential collateral damage.

The Way Forward for Singapore

Singapore is at the forefront of efforts related to military AI governance. It has actively participated in various military AI governance discussions, including the UN LAWS discussions and the 2023 summit on Responsible Artificial Intelligence in the Military Domain (REAIM). In February 2024, Singapore hosted the [inaugural REAIM Regional Consultations (Asia)](#) in partnership with the Netherlands and the Republic of Korea. In 2023, Singapore not only endorsed the [REAIM Call to Action](#) and the US-led "[Political Declaration on Responsible Military Use of AI and Autonomy](#)" but also [acceded](#) to the Convention on Certain Conventional Weapons, under which the UN LAWS discussions are convened.

Singapore can use its unique role as a "[trusted and substantive interlocutor](#)" at various AI governance platforms, such as REAIM, to broaden the discussions to include ADSS. Unlike AWS, which have various multilateral platforms to facilitate discussions and build consensus, ADSS have not received the level of attention needed. With Singapore's influence in these AI governance platforms, more attention and awareness could be raised among relevant stakeholders.

Second, policymakers should develop the necessary understanding of ADSS and its associated risks and challenges under IHL. They could do so through IHL training programmes and multi-stakeholder discussions involving technology companies and academics to help them better understand the measures that may be required in the design and use of ADSS to ensure compliance with IHL. In undertaking such capacity-building, Singapore could amplify its voice and leverage its influence in international fora to lead efforts in building awareness, understanding, and norms of behaviour regarding the military application of ADSS, particularly in decisions on the use of force.

__Mei Ching LIU__ is Associate Research Fellow with the Military Transformations Programme at the S. Rajaratnam School of International Studies.

_____