Keith Eble*

Artificial Intelligence in Military Operations – Experiences and Challenges. British Perspective

Abstract

This article touches on the issue of understanding and approach to the use of AI by the British army from the perspective of a representative of the British armed forces. The article will address the issues of tripartite division as to the essence of the problem today. This article was an excellent part of the author's speech delivered during the international conference 2023 Warsaw Cyber Summit.

Key words: Artificial Intelligence, Cyber, British, army, military operations

* Keith Eble, Brigadier Keith Eble Headquarters of the British Army Operational Law Division, keith.eble472@mod.gov.uk.

The Warsaw Cyber Summit has become an important event in the Cyber Security calendar that enables discourse, builds relationships and strengthens interoperability. This is one secret not worth keeping to ourselves.

Why? As we have learned from previous operations, one cannot surge relationships and it is optimal to be here in person with allies and partners to learn from each other. The British Army is proudly playing its part in supporting military training to 30,000 Ukrainian Armed Forces Personnel including the training package in the Law of Armed Conflict provided by the Army Legal Services. Turning to topic on „AI in Military Operations – experiences and challenges", we need to address three specific points.

First, I will provide some strategic context applicable to AI in military operations; second, some academic and practitioner discussion about AI development and use by armed forces; and third, how I believe legal advisers can help address some of the challenges in AI military development. I should say from the outset that I am optimistic about the future of our military use of AI.

Strategic Context

Increasingly states are commenting both in unilateral statements and within multinational fora about their approach to the applicable law in cyber space and in AI development and about their policy intent. The UK commenced its public statement about the applicability of international law in cyber operations in May 2018 in the Attorney General's Chatham House Speech[1].

The UK has consistently indicated in public statements since then that regardless of the technological development, including in AI enabled capability in Defence, legal compliance and ethical outcomes that are consistent with democratic values are central to such development.

Even where states have indicated variations in their approaches to policy development, fora such as the Certain Conventional Weapons Group of Government Experts have enabled many other states to confirm the requirement to ensure AI development and use reflects the applicable international law.

1 Attorney General Jeremy Wright KC MP speech at Chatham House on 23 May 18. The most recent public statement is from Attorney General Suella Braverman KC MP from 19 May 2022.

For the UK and many other states this means that lethal autonomous weapons would require a legal review under Art. 36 of the First Additional Protocol to the Geneva Conventions which is applicable to International Armed Conflicts. For those states not bound by this protocol, the publication of the United States Department of Defence Directive 3000.09 Autonomy in Weapon Systems dated 25 January 2023 may be seen as a „best in class" with a clear statement about legal compliance and AI ethical principles.

Following publication of the NATO AI Strategy of 22 October 2021, the UK Government published its Defence Artificial Intelligence Strategy on 15 June 2022 which defined AI for us as follows „a family of general-purpose technologies, any of which may enable machines to perform tasks normally requiring human or biological intelligence, especially when the machines learn from data how to do those tasks".

This definition has general application across Defence and in all domains and is not limited to weapons. It could be said to potentially apply to many complex, dull, dirty or dangerous tasks that would normally require human involvement.

One such use publicly declared by the UK was AI data processing to enhance British Army planning and command and control on land in Exercise Spring Storm in May 2021 in Estonia. This informed human decision making and leveraged effective and trusted AI for a specified task that was measurable.

In order to inform future development, the UK established 5 ethical principles for AI in Defence Human-Centricity, Responsibility, Understanding, Bias and Harm Mitigation and Reliability.[2]

The UK National Cyber Force's „Responsible Cyber Power in Practice" is a vision statement that has just been published by the UK Government (4 April 2023) which sets out the NCF operational principles which are that Cyber Operations will be accountable, precise and calibrated.

All of these statements point to a strategic context led by NATO and similarly minded states that puts the law and ethical outcomes at the centre of our AI development. How others respond to these norms in their AI development remains to be seen and will be closely monitored.

2 *The UK Ministry of Defence Ethical Principles for AI in Defence were published on 15 June 2022 in Annex A of „Ambitious, safe, responsible: our approach to the deliver of AI-enable capability in Defence"*, https://www.gov.uk/government/publications/ambitious-safe-responsible-our-approach-to-the-delivery-of-ai-enabled-capability-in-defence/ambitious-safe-responsible-our-approach-to-the-delivery-of-ai-enabled-capability-in-defence [access: 5.10.2022].

Academic and Practitioner Legal Discussion of AI Military Use

I would submit that the conduct of the Army – which is the nation's Army – is a continuous conversation internally and with a wider community. This includes messages to our own population, civil society and allies and adversaries about our approach to the military use of AI.

Whilst the strategic context is now well understood, practical considerations remain to be discussed about how AI development may actually apply in practice and specifically may be capable of applying in the development of wide AI application by armed forces.

Within civilian society, humanitarian concerns about autonomous weapons systems were expressed by the ICRC in the May 2021 position paper on autonomous weapons systems[3]. The ICRC is to be commended on its efforts to support adherence to the Law of Armed Conflict in relation to the use of autonomous weapons systems and to address the concerns raised by their use.

This is an area of lively academic legal discussion. I note that there have been challenges in some academic circles to the ICRC's position paper. For example, Professor Brian L. Cox's May 2021 article published in the Lawfire website[4].

However, the point remains that military lawyers who may be required to legally review AI systems and advise on their use in practice have to, at least conceptually, address some of the questions raised about „human agency" and in a wider sense advise on how accountability by, and of, armed forces would be achieved.

Taking this discussion further into a wider question about potential state responsibility under the Articles on Responsibility of States For Internationally Wrongful Acts in relation to military AI application, I was greatly interested in the recent article on this subject by Dr Berenice Boutin of the Asser Institute published in the Leiden Journal of International Law[5]. Dr Boutin raises some

3 *The ICRC position on autonomous weapons systems and background paper*, 12 May 2021, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems [access: 20.09.2022].

4 B.L. Cox, *In Backing Future Autonomous Weapons Ban, the ICRC Appears Intent on Repeating Past Mistakes*, 18 May 2021, https://sites.duke.edu/lawfire/2021/05/18/in-backing-future-autonomous-weapons-ban-the-icrc-appears-intent-on-repeating-past-mistakes/ [access: 20.09.2022].

5 B. Boutin, *State responsibility in relation to military applications of artificial intelligence*, „Leiden Journal of International Law" 2023, no. 26, p. 133–150.

interesting points and questions about the attribution and allocation of responsibility and makes proposals for how „human centricity" may be said to apply or legal accountability inferred.

Relevant questions about human control and human agency are particularly related to complexity, speed, understanding and predictability.

Complexity. In the development phase – data and machine leaning may be understood in broad scientific terms but, as systems adapt and even self-develop for optimisation, some question whether they are simply too complex to be measured using current scientific methods of experimentation by observation (trial and error):

1. Speed. Given the ability for systems to gather, store and analyse huge amounts of data, questions are being asked about whether a human operator can react to the information being presented and whether they will simply defer to the system.

2. Understanding. This is the so-called black box question. How is the system operating? If we accept it is operating in a non-human way, how can we really understand the options being presented to us or even undertaken by AI?

3. Predictability. This feeds into the question of predictability. Will a super complex system, operating beyond human response levels, be capable of being measured? What if they make errors? How will we know and will AI even understand it needs to inform us of issues.

In a legal sense this all plays into legal assurance and accountability, which is ultimately how AI will be judged. This type of legal analysis is important in the continuing discussion about AI military use.

The UK is ambitious in its approach to development and with good policy and practice seeks to avoid and mitigate concerns.

For my part, as a legal practitioner, I am not concerned that these issues are, or will be, an intractable problem in practice. I have already mentioned legal reviews of weapons as a first check in the study, development, acquisition or adoption of a new weapons.

Furthermore, Government policy, military doctrine, military rules of engagement and tactical directives can be used to further control lethal and non-lethal AI capabilities and may limit such use by the armed forces, where it is felt necessary.

Training

The British Army's approach to operations is that it is command led and staff enabled. Whilst legal advisers are not the decision makers in terms of combat operations, Army Legal Services play a key role in enabling our Army to comply with the rule of law through training.

We are reminded in that role, of strategic lessons from Russia's illegal war against Ukraine, about legitimacy, legal compliance and the accountability that all leaders and states could face for legal violations. This is vital ground. In addition to the recent ICC indictments, there has been media reporting of alleged violations by Russian forces against Ukrainian captured persons released into the public domain via electronic means.

In the UK, Government lawyers, both civilian and military, play an essential part in training relevant Defence personal on the fundamentals of national and international law. AI, in my opinion, will require a wider and deeper understanding of the law across all those engaged in AI capability development so that there is a „law reflex" to support AI military use.

In my opinion, what must be made clear to our training audience is that whilst there is some complexity, there is no grey zone in the application of law. To do this most effectively, legal advice about capability development for operations below and above the threshold of armed conflict must be unambiguous and explained as simply as possible.

For example, we accept in the UK that the Law of Armed Conflict applies in all five domains we identify as land, sea, air, space and cyber. In other words, from the soldiers' rifle to AI enabled artillery and to cyber information operations anywhere. For the most part, it is the simple actions done well and repeated that count most in ensuring legal compliance.

For more complex questions, legal advisers are available to address questions of true legal risk and such advice in the UK goes from the military lawyer to the Attorney General in functional terms thus supporting the rule of law.

Bibliography

Boutin B., *State responsibility in relation to military applications of artificial intelligence*, „Leiden Journal of International Law" 2023, no. 26.

Cox L., *In Backing Future Autonomous Weapons Ban, the ICRC Appears Intent on Repeating Past Mistakes*, 18 May 2021, https://sites.duke.edu/lawfire/2021/05/18/in-backing-future-autonomous-weapons-ban-the-icrc-appears-intent-on-repeating-past-mistakes/ [access: 20.09.2022].

Sztuczna inteligencja w operacjach wojskowych – doświadczenia i wyzwania. Perspektywa brytyjska

Streszczenie

Artykuł dotyczy zrozumienia i podejścia do wykorzystania sztucznej inteligencji przez armię brytyjską z punktu widzenia przedstawiciela brytyjskich sił zbrojnych. Jest w nim poruszona kwestia trójpodziału podejścia i zrozumienia tego zjawiska w Siłach Zbrojnych Wielkiej Brytanii. Niniejszy artykuł powstał na podstawie wystąpienia jego Autora podczas 2023 Warsaw Cyber Summit.

Słowa kluczowe: sztuczna inteligencja, cyberbezpieczeństwo, wojska lądowe, operacje wojskowe