Defence Studies

ISSN: 1470-2436 (Print) 1743-9698 (Online) Journal homepage: www.tandfonline.com/journals/fdef20

The military use of AI and the law of armed conflict: what role for government and industry?

Aurel Sari & Geraint Evans

To cite this article: Aurel Sari & Geraint Evans (10 Jun 2026): The military use of AI and the law of armed conflict: what role for government and industry?, Defence Studies, DOI: 10.1080/14702436.2026.2686609

To link to this article: https://doi.org/10.1080/14702436.2026.2686609

Published online: 10 Jun 2026.

DEFENCE STUDIES
https://doi.org/10.1080/14702436.2026.2686609

Routledge
Taylor & Francis Group

The military use of AI and the law of armed conflict: what role for government and industry?

Aurel Sari[a,b] and Geraint Evans[c]

[a]School of Law, University of Exeter, Exeter, UK; [b]CIAS, Corvinus University of Budapest, Budapest, Hungary; [c]Strategy and Security Institute, University of Exeter, Exeter, UK

ABSTRACT

The UK has committed itself to the responsible adoption of AI technologies for military use. While the Ministry of Defence has published detailed guidance on the ethical dimension of military AI, so far it has offered remarkably little guidance on its legal aspects, including the law of armed conflict. The purpose of this article is to call attention to this imbalance and the risks it poses. A large proportion of AI capability development is now driven from the bottom up. Yet industry is not bound to ensure that its products are compliant with the law of armed conflict. Considerable time, effort and resources may therefore be invested in the design and development of AI systems that subsequently turn out to raise substantial legal concerns. This could present the Ministry of Defence with an unpalatable choice between redesigning these systems at considerable expense or deploying them at the risk of non-compliance. To avoid this outcome, we argue that the Ministry should recognize that the legal and ethical considerations of AI are distinct, determine what exactly its legal obligations demand, communicate these requirements to industry by setting detailed expectations and proactively engage with businesses early in the AI system lifecycle.

ARTICLE HISTORY
Received 24 December 2025
Accepted 5 June 2026

KEYWORDS
Artificial Intelligence; law of armed conflict; international humanitarian law; industry; defence; autonomy

1. Introduction

The adoption of artificial intelligence (AI) for military use has accelerated dramatically in recent years. Estimates indicate that worldwide spending on military AI has increased from approximately USD 4.6bn in 2022 to over USD 10bn in 2025, with some of the more optimistic forecasts predicting that it will surpass USD 30bn by 2030 (Grand View Research 2025; Research and Markets 2025). Recent conflicts underline the growing impact of AI technologies on the battlefield. Ukraine has become what some commentators describe as an "AI war lab" (Bergengruen 2024), showcasing how AI may be employed from intelligence analysis and electronic warfare to operational planning and target engagement (Bondar 2025; Fontes and Kamminga 2023). In Gaza, Israel's use of AI-assisted targeting has demonstrated the operational application of algorithmic

CONTACT Aurel Sari a.sari@exeter.ac.uk School of Law, University of Exeter, Amory Building, Rennes Drive, Exeter EX4 4RJ, UK

warfare systems at scale (Israel Defense Forces 2024). In Iran, the deployment of the Maven Smart System has enabled the US to significantly increase the volume and tempo of its operations (Klare 2026).

Against this backdrop, the UK has positioned itself as a leading adopter of AI across Defence. The Defence Artificial Intelligence Strategy, published in June 2022, commits the UK to pursuing strategic and operational advantage through AI, noting that "future conflicts may be won or lost on the speed and efficacy of the AI solutions employed" (UK Ministry of Defence 2022a, 4). The Strategic Defence Review (SDR) of 2025 calls for a "shift towards greater use of autonomy and Artificial Intelligence (AI) within the UK's conventional forces" in order to enhance lethality and provide cheaper capabilities (UK Ministry of Defence 2025h, 96). Recent investment decisions illustrate the scale of these ambitions. In June 2025, the Government announced an investment package that allocates more than GBP 4bn to autonomous systems in an effort to shape Britain's military future and boost its export potential (UK Ministry of Defence 2025g). In September 2025, the Government entered into a strategic partnership with Palantir Technologies that would see up to GBP 750 m invested in the most advanced AI-enabled technologies (UK Ministry of Defence 2025d). In parallel, more than GBP 1bn is being allocated to the Digital Targeting Web to connect different sensors, platforms and weapons systems to allow targeting decisions to be made and executed faster.

The UK has committed itself to deliver and deploy AI-enabled military capabilities in a safe and responsible manner (UK Ministry of Defence 2022b, 1). This commitment rests on two normative foundations: ethical principles and legal obligations. The ethical framework for military AI has been articulated in some detail. The Ministry of Defence has formulated five core ethical principles to guide the responsible use of AI for military purposes: human-centricity, responsibility, understanding, bias and harm mitigation, and reliability. The principle of human-centricity, for example, demands that "the impact of AI-enabled systems on humans must be assessed and considered, for a full range of effects both positive and negative across the entire system lifecycle" (UK Ministry of Defence (2022b), 9). Considerable effort has gone into developing guidance on how the five ethical principles should be implemented. Joint Service Publication 936 (JSP 936) identifies specific requirements for each principle that must be fulfilled across AI life-cycles. For instance, with regard to the principle of understanding, it specifies that any "[s]takeholder groups that interact with the AI capability or its development must be identified, and their required interactions analysed to determine the level of understanding they require to engage with the system, or its development, responsibly" (UK Ministry of Defence 2025c, 12). By comparison, the treatment of the legal aspects of military AI consists mostly of emphatic assertions about the need to comply with the law, coupled with very little detailed guidance as to what this entails. JSP 936 devotes almost 50 paragraphs to ethical questions in a section dealing with the legal and ethical considerations of AI, but only a meagre three paragraphs to legal matters. This is followed by a section on AI ethics governance, but no comparable section on AI legal governance. Inexplicably, the passages on AI assurance fail to even mention any legal aspects.

This asymmetry in the treatment of ethical and legal considerations is striking. One possible explanation for the imbalance might be the sheer volume and complexity of the legal questions raised by the military use of AI. Clearly, documents like JSP 936 are not

the appropriate place to dissect the finer points of the law or to indulge in long-winded doctrinal discussions. However, at the very least, one may legitimately expect JSP 936 and similar publications to prominently acknowledge the scale of the legal challenges arising and to highlight their importance and implications. This is all the more the case given that the Ministry of Defence recognizes that its legal obligations, including those under the law of armed conflict, serve as a foundation for the development and deployment of AI-enabled systems and that the five ethical principles "do not affect or supersede existing legal obligations" (UK Ministry of Defence (2022b), 9). Without wishing to downplay the importance of ethical considerations, the fact remains that if legal compliance is a non-negotiable baseline requirement, then AI systems that do not meet the applicable legal standards are not deployable. Sidelining the legal requirements and the challenges they present creates problems downstream.

The preoccupation with the ethical aspects of military AI at the expense of its legal dimension should be a cause for concern: it has implications not only for the rule of law, but also for operational readiness. The purpose of this paper is to address this attention deficit across Defence by focusing on the normative and practical challenges that the military use of AI raises under the law of armed conflict. As we explain in the second section, how the law of armed conflict applies to military AI is surrounded by considerable uncertainty, fuelled by the contextual nature of the law and the distinct features of AI. Commanders and others deploying AI systems will have to navigate this uncertainty in order to comply with their obligations under the law of armed conflict. In the third section, we illustrate the difficulties that this presents by exploring some of the questions that a hypothetical AI-enabled decision-support system raises. We then set out in the fourth section why compliance with the law of armed conflict remains critical, before turning to discuss what obligations are incumbent on government and industry to ensure that military AI systems are compatible with the law. In the fifth section, we offer a brief overview of the UK's AI ecosystem, noting that a significant proportion of AI adoption is driven from the bottom up. Even though industry is not subject to an obligation to ensure that the products it brings to market comply with the law of armed conflict, we suggest that there are good reasons why military AI systems should be compatible with the law by design. This is so principally because the UK, as a State bound by the law of armed conflict, may only deploy systems that are consistent with its legal obligations. Letting industry develop technologies that the UK and other law-abiding States may not put into operational use because they might contravene their legal obligations runs the risk of much wasted effort, costly redesigns and potential gaps in capability. We suggest that the Ministry of Defence should do more to avoid this outcome. We end by offering some concluding thoughts.

2. Military AI and the law of armed conflict

The applicability of the law of armed conflict to the military use of AI is not in any doubt. Both legal scholarship and State practice affirm with overwhelming consistency that the law of armed conflict governs the use of AI systems during armed conflict, regardless of whether such systems constitute weapons or serve some other military purpose (e.g. Coco and Talita 2024, 244). United Nations General Assembly Resolution 79/239, adopted on 24 December 2024, affirms that international law, including the law of

armed conflict, "applies to matters governed by it that occur throughout all stages of the life cycle of artificial intelligence, including systems enabled by artificial intelligence, in the military domain."[1] Adopted by 159 States in favour with only two against and five abstentions, Resolution 79/239 represents a significant articulation of State practice. Regional organizations and informal groupings of States have similarly affirmed the applicability of the law of armed conflict to military AI. NATO's Artificial Intelligence Strategy, first adopted in 2021, declares that AI applications must be developed and used in accordance with the law of armed conflict.[2] The Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, endorsed by more than 30 States in February 2023, likewise affirms the applicability of the law of armed conflict to the use of AI systems.[3]

This consensus should not come as a surprise. The law of armed conflict is technology-agnostic: most of its rules apply irrespective of what specific capabilities the parties to a conflict may deploy (Liivoja 2015, 1167–68). The fact that much of the law was adopted before the advent of modern AI technology, and that none of the rules expressly address the use of AI, therefore does not render the law inapplicable. Indeed, many of the relevant rules and principles are formulated in general terms. The duty of distinction, for instance, requires parties to a conflict to distinguish *at all times* between civilians and civilian objects on the one hand and military objectives on the other.[4] The general character of this obligation means that it applies irrespective of the technologies a party may employ. This is reinforced by the underlying principle that the right of the parties to the conflict to choose methods or means of warfare is not unlimited (Boothby 2025, 96).[5]

While the applicability of the law of armed conflict to the military use of AI is a matter of consensus, significant uncertainty persists about *how* specific rules and principles apply. This uncertainty is not driven solely by technological novelty. Rather, it arises from the convergence of two distinct factors: the high level of generality and contextual dependency that characterize the law of armed conflict and certain distinct features of contemporary AI systems.

2.1. The character of the law

Many rules and principles of the law of armed conflict lack detail and are not formulated in very precise terms. This is not the result of careless drafting, but an intentional response to the unpredictability, confusion and changeability that defines armed conflict. For example, the parties to a conflict are subject to a precautionary duty to provide effective advance warning of attacks which may affect the civilian population, unless circumstances do not permit.[6] The rule does not define what kind of effects on the civilian population trigger the duty to give advance warnings, what counts as an "effective" warning for these purposes or precisely what kind of circumstances absolve a party from the duty to issue warnings. The answer to these questions depends on the specific circumstances of each case and requires the application of common sense in a manner that balances the humanitarian and operational considerations that may arise in good faith (see Baruch and Neuman 2011). Put differently, the law does not impose a static obligation governed by clearly defined benchmarks, but a duty that is context-dependent and thus articulated with a degree of openness. This openness imparts flexibility,

ensuring that the duty to give advance warnings is both applicable and capable of application across a wide range of operational scenarios.

The same holds true for many other rules. Wounded or sick enemy combatants must be respected and protected.[7] Even though this condition is not expressly stated in the law, clearly only those enemy combatants are entitled to respect and protection who refrain from hostile acts: many a medal has been earned by wounded soldiers who have carried on the fight despite their injuries. As the International Committee of the Red Cross notes, it can be extremely difficult in the midst of combat to determine whether a person is wounded in the legal sense and refrains from any hostile act.[8] The test to be applied is whether under the given circumstances a reasonable fighter would consider the person in question to abstain from hostile acts.[9]

The general wording and context-dependent nature of many law of armed conflict rules allows them to apply in highly diverse situations, yet this also leaves their meaning uncertain and subject to disagreement among commentators and States. Some of these disagreements are long-standing and deep-seated. Crucially, many are also unresolved. This complicates the application of the law to the military use of AI systems, since what exactly a particular rule requires is often not evident or settled.

2.2. The features of AI

Certain distinct features of modern AI systems present a second source of uncertainty. Four features merit attention here.

At their core, most AI systems carry out computational tasks that perform cognitive functions, such as learning and reasoning. We can leave open the question whether machines merely mimic or actually perform cognitive functions and also in what sense artificial intelligence differs from human intelligence (see Korteling et al. 2021). The important point for our purposes is that one of the principal benefits that human operators derive from the use of AI systems is the delegation of cognitive tasks to machines that otherwise they would have to perform themselves. For example, an object recognition system may be deployed to identify certain classes of vehicles. In performing this function, the system makes factual determinations by assigning labels to objects. Another system may be tasked with determining whether some of these objects constitute military objectives liable to attack. This would be a legal determination. When humans delegate tasks to machines, they do not delegate their duty to respect the law of armed conflict.[10] Accordingly, human operators must ensure that any factual or legal determinations made by machines under their control, and any subsequent actions or omissions based on those outputs, are compliant with their obligations under the law of armed conflict. Conventional weapons or other systems that are not AI-enabled typically do not raise such issues.

AI is a technology that lends itself to a wide range of military applications (Rashid et al. 2023). Common use-cases include intelligence, surveillance and reconnaissance (ISR), command and control, target recognition, autonomous systems and vehicles, cyber operations and electronic warfare, simulation and training, maintenance and logistics, and medical care. The functions that AI systems may be tasked to carry out in these areas range from data collection, collation and analysis, decision support and content generation to controlling the

operation of physical assets. Given the extraordinarily wide range of domains, use-cases, functions, outputs and effects, not much can be said about how the law of armed conflict applies to AI systems in general. For anything reasonably informative, it is necessary to consider on a case-by-case basis what a specific AI system actually does, what effects it generates and what happens to its outputs, so as to determine what legal concerns, if any, it presents. For example, a system tasked with optimizing logistic chains or producing vehicle maintenance schedules is unlikely to engage any law of armed conflict rules. By contrast, a system that collects the personal data of prisoners of war, generates intelligence reports or nominates targets for attack will almost certainly do. Given the complexity of AI systems and the dynamic nature of the operating environment, it may not always be immediately obvious what rules are engaged and what legal concerns arise.

Contemporary AI systems, particularly those employing machine learning techniques, frequently function as "black boxes" whose internal processes cannot be readily understood or explained by humans (Burrell 2016). Whilst these systems can achieve high levels of performance in pattern recognition and classification tasks, the precise route through which they arrive at their outputs may be opaque even to the engineers who designed them. This opacity may pose significant challenges for human operators seeking to establish whether a system has generated its factual or legal determinations in compliance with the law of armed conflict. For example, if operators do not understand what factors a machine has considered and what weight it gave to different considerations when producing outputs that engage rules requiring contextual assessments, such as status determinations,[11] then they are unable to reassure themselves that those outputs are consistent with their legal obligations. Relying on the outputs without such reassurance poses a real risk of non-compliance, either because the factual or legal determinations made by the machine may turn out to be incorrect or because the lack of reassurance contravenes specific obligations that the law imposes on human operators.[12]

While all systems are susceptible to malfunction, the distinct configuration of AI systems creates forms of failure that pose novel compliance challenges. The quality and representativeness of training data constitute the foundation upon which machine learning systems are built. Where a system was trained on data that does not reflect its operational environment, either because of limitations in the training data set or because of subsequent changes in the operational context, its performance may be severely compromised (Heim and Frank 2025). Training data may also replicate biases which could expose persons or objects to harm as a result of misidentification or failure to identify them (Bruun and Bo 2025). Whereas conventional sensor systems can be jammed or spoofed, AI systems are vulnerable to adversarial attacks that exploit the pattern-recognition logic of machine learning algorithms in ways that would not affect non-AI-enabled systems (Hinton 2023). Even advanced AI systems are only capable of performing relatively narrow tasks under specific conditions. Where these conditions are not met or the machines are deployed outside their intended operating environment, AI systems are prone to a wide range of errors that renders them brittle in ways that conventional weapons are not (Scharre 2019). As these limitations and their potential adverse consequences are readily foreseeable, they must be addressed by those operating AI systems to comply with their obligations under the law of armed conflict.

3. Case-study: a fictional AI decision-support system

To illustrate the normative and practical challenges that arise in applying the law of armed conflict to military AI systems, we turn to a toolkit co-developed by the Defence Science and Technology Laboratory (Dstl). The toolkit contains a set of "AI Ethics Playing Cards." Each card addresses an AI case-study meant to demonstrate how the five ethics principles adopted by the Ministry of Defence and the risk assessment tools found in JSP 936 can help to identify ethical risks, so that these can be properly assessed, considered and mitigated (Dstl 2024).

One of the AI Ethics Playing Cards envisages the deployment of a hypothetical AI system to assist a military commander by recommending strategic and tactical decisions based on battlefield data. The system is said to free up multiple staff officer positions and, by processing all incoming data at speed, provide faster recommendations based on operational need. We are told to envisage a situation where the commander decides to launch a time-sensitive strike based on the system's recommendations. However, it turns out that these recommendations were informed by flawed data or analysis about civilian movements, resulting in the strike causing excessive civilian harm. Let us unpack this scenario from a law of armed conflict perspective.

For the sake of our analysis, we assume that the incident occurred in the context of an international armed conflict, which engages the UK's obligations under Additional Protocol I.[13] The incident involved a "strike," which means that it is an "attack" for the purposes of the law of armed conflict and thus subject to the rules governing the conduct of hostilities.[14] The case-study is silent on several important points. For example, it does not disclose what the intended target of the attack was, what exactly the AI system's recommendation consisted of and how this output informed the planning and decision-making process leading to the attack. We are told, however, that the recommendations were based on flawed data or analysis about civilian movements and that the attack caused "excessive" civilian harm. The reference to excessive civilian harm suggests that the case-study's authors believe that the attack engaged the proportionality rule.[15] However, proportionality is relevant only in situations where those planning or deciding upon an attack expect that it will cause incidental harm to civilians or civilian objects. Where no incidental civilian harm is expected, the proportionality rule is not applicable, even if civilians are in fact harmed by the attack.[16] We must therefore assess two possible scenarios, depending on whether incidental civilian harm was expected or not.

3.1. No incidental civilian harm was expected

If the attack was launched without an expectation that it would cause incidental harm to civilians, the key question is whether the commander and others who planned or decided upon the attack complied with their duty to do everything feasible to verify that the target was liable to attack.[17] For this scenario, we assume that the AI system recommended the intended target for attack based on a flawed assessment that no civilians would be present. The presence or absence of civilians at a particular point in time and space is a matter of fact. By declaring civilians to be absent, the AI system thus made a factual determination.

In verifying targets, commanders must base their decisions, including decisions about facts, on reasonably available information, which includes information actually available to them at the relevant time and information they could reasonably have obtained.[18] Their decisions must be made in good faith, meaning that commanders must take steps to verify the accuracy and reliability of the information they consider.[19] They are also expected to make their decisions with a requisite level of certainty,[20] not least because if a minimum threshold of certainty is not met in verifying that persons or objects are liable to attack, they must be presumed to be civilians or civilian objects.[21] What degree of certainty is required beyond this minimum threshold depends on the operational context (Schmitt and Schauss 2019).[22] Everything feasible must be done to verify a target, which means taking all steps that are "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations."[23] Targeting decisions must therefore be based on "the level of certainty that can reasonably be achieved in the circumstances."[24] For example, it is reasonable to expect a headquarters prosecuting preplanned targets at a time and place of its own choosing to verify those targets at a higher level of certainty than a patrol of soldiers returning fire after walking into an ambush.[25]

Returning to our scenario, the commander had two basic options to comply with the duty to verify the target when launching an attack based on the AI system's recommendations: they could have relied on the machine to produce its outputs consistently with the duty of target verification if it was capable of doing so. Alternatively, if the machine lacked that capability, they could have manually reviewed those outputs.

Pursuant to the first option, the AI system in our scenario might have been capable of verifying targets autonomously, in other words it might have possessed the capability to make the necessary factual and legal determinations without human input in a way that is consistent with the commander's precautionary duties. Obviously, this is not a capability that can just be bolted on as an afterthought: the system would have had to be designed to operate like this. In fact, its developers would have had to overcome significant difficulties to make this happen.

The system would have to be equipped with whatever sensors and other capabilities are necessary to receive and process relevant inputs from its operating environment. The applicable law of armed conflict rules would then have to be translated into computational language for machine processing. This raises unresolved normative questions. For example, human operators would need to decide exactly what levels of certainty must be met under what operational circumstances and then translate these into probability scores or other numerical values intelligible to computers. Not only is there no agreement whether a high level of certainty equates to a probability score of 0.72, 0.81 or 0.98, but it is also impossible to exhaustively identify all the different operational circumstances that the system may encounter in its use. If the machine is to rely on general principles instead, it would have to apply common sense and make reasonable decisions in unforeseen situations. However, this is something that AI has traditionally struggled with (Bennett and Anthony 2021; Choi 2022). Machine learning techniques may offer a solution, but training data is likely to be limited and system opacity could make it difficult or impossible to predict with confidence how well the system will perform in conditions of actual combat.

Provided these matters can be resolved, the system would need to apply the rules it has been programmed with under battlefield conditions. The scope of this challenge depends on what exactly the system has been tasked with. If the system is merely asked to identify the presence of civilians, this should be relatively straightforward. Every person is a civilian, unless they are a member of the armed forces of an adverse party.[26] Civilians do not change or lose their civilian status easily. By contrast, if the system is tasked with identifying lawful human targets and nominating them for attack, it would have to verify that these persons are not subject to special protections.[27] Lawful targets may gain protected status in a range of circumstances, for instance if a combatant clearly expresses an intention to surrender.[28] If the system cannot make contextual assessments in dynamic conditions to recognize and process such changes in a person's liability to attack, putting it into service may not be lawful.[29] Since it is entirely foreseeable that the performance of an AI system may degrade, for example as a result of concept drift, adversarial action or evolving battlefield conditions, its human operators would also have to monitor the system to ensure that it continues to perform at the level required by the duty of target verification.

Assuming all these conditions are met, the system may have been capable of producing factual determinations, recommendations and other outputs autonomously in a manner consistent with the commander's duty of target verification. However, this would not have been sufficient to fully discharge the duty to do everything feasible to verify the target: the commander was bound to consider other information reasonably available to them and their reliance on the AI system's recommendations had to be reasonable. Provided this was the case, the commander would have complied with their precautionary obligations when they decided to launch the attack based on the system's recommendations, even if the attack caused unexpected civilian harm.

Pursuant to the second option, if the AI system did not possess the technical capabilities necessary for autonomous compliance as outlined above or the commander's understanding of how the system arrived at its recommendations was not sufficient to reassure them that the machine's output took into account all reasonably available information, was based on a reasonable and good faith assessment and met the levels of certainty appropriate for the operational context, then the commander or their staff would have had to review the machine's outputs themselves to ensure that these conditions were met. Bearing in mind the opacity of many AI systems (the "black box" effect), this may have required human operators to manually collect and reassess all the reasonably available intelligence. Assuming that the commander and their staff carried out this reassessment and in doing so did everything feasible to verify the target, they would have complied with their precautionary obligations, even if the attack caused high levels of unexpected civilian harm. However, manually reviewing all machine outputs would not only slow the targeting cycle down to human speed again, but it would call into question the utility of using the AI system in the first place.

Alternatively, should the commander have decided to launch the attack based on the system's recommendations without sufficient reassurance that those outputs met the precautionary obligations imposed by the law, this would have been no better than

flipping a coin. Not only would it amount to a failure to comply with the duty of target verification, but the use of an AI system in these circumstances may well constitute a method of combat which cannot be directed at a specific military objective, thus rendering the attack indiscriminate to begin with.[30] It is worth noting that certain indiscriminate attacks "may give rise to the inference that civilians were actually the object of attack."[31] Intentionally directing attacks against civilians who are not directly participating in hostilities is a war crime.[32]

3.2. Incidental civilian harm was expected

For the second scenario, we assume that the attack was launched with the expectation that civilians would suffer incidental harm. We also assume that based on the AI system's recommendations, the commander expected this incidental civilian harm to be proportionate, but due to the flawed data or analysis, it was in fact excessive. In these circumstances, the question is whether the commander complied, first, with the precautionary duty to take all feasible precautions in the choice of means and methods of attack to avoid, and in any event to minimize, incidental civilian harm and, second, with the precautionary duty to refrain from deciding to launch any attack which may be expected to cause excessive incidental civilian harm.[33]

The duty to take all feasible precautions in the choice of means and methods of attack demands that even proportionate incidental civilian harm must, to the extent feasible, be avoided or at least be kept to a minimum. The different weaponeering options considered under the Collateral Damage Estimation Methodology offer an example of how this duty might be implemented in practice, at least as far as persons are concerned.[34] However, since the obligation applies to the choice of means and methods of attack, it is relevant to the use of an AI system only if the latter constitutes a means or method of attack.

Means of attack are sometimes understood to be synonymous with weapons.[35] A better approach is to consider means of attack to include weapons as well as all related equipment, materials and delivery mechanisms necessary for a weapon to operate as intended.[36] Either way, the AI decision-support system in our case-study is not a weapon, since it is not designed or intended to inflict physical harm directly. Nor does it qualify as a means of attack, since it is not performing functions that are directly necessary to enable a weapon to operate as intended. This leads to the question whether it is a method of attack. What constitutes a method of attack is not defined, but it is generally understood to refer to the way or manner in which means of attack are used by a party.[37] For example, aerial bombardment is a method of attack, as it constitutes a distinct way for delivering a projectile on target.[38] As this example illustrates, a method of attack describes a technique or process that defines how a kinetic effect is achieved. Using a computer to prepare a deck of slides to brief the commander during a targeting board does not constitute a method of attack, as it does not define the way in which the kinetic effect of the attack is delivered. Accordingly, if an AI system were to nominate targets for attack and these would be serviced by other assets without any intervening decision-making stages, a reasonable case could be made that such a system would constitute a method of attack, as the decision to attack would be an automated one, which is a distinct method. By contrast, if an AI system merely produces outputs that feed into the decision-making process of a commander, as in our scenario, this system would not

qualify as a method of attack, since it does not directly affect the way or manner in which the attack is executed. Given that the AI decision-support system in our case-study is neither a means nor a method of attack, the precautionary duty relating to the choice of means or methods of attack does not apply to it.

This leaves the precautionary duty to refrain from deciding to launch an attack which may be expected to cause excessive incidental civilian harm. It is important to emphasize that the rule is concerned with the decisions taken by those who plan or decide upon an attack based on what they *expected* at the relevant time, not with the actual outcome of the attack. To assess the extent of the incidental harm an attack is expected to cause, those who plan or decide upon the attack must determine its foreseeable effects in good faith.[39] At a minimum, this requires them to make "reasonable use of the information available."[40] Some States take the position that proportionality assessments require sufficient levels of situational awareness and must be based on sufficient degrees of certainty.[41] This is echoed by commentators who suggest that those who plan or decide upon attacks have an obligation to gather as much information as feasible (Cohen and Zlotogorski 2021, 194) and "to regularly check that the sources and methods they are using are reliable and approximate the actual consequences" (Henderson 2009, 227). In our case, the question therefore is whether the commander made reasonable use of the information available in relying on the AI system's recommendations.

As in the earlier scenario, the commander's first option for complying with this obligation was to rely on the AI system to generate its outputs consistently with the law, provided the machine possessed the technical capability to do so. As outlined above, equipping an AI system with the capability to apply the law of armed conflict autonomously presents significant difficulties. In the present case, these difficulties are severe, as proportionality assessments cannot be reduced to a mathematical formula, due to their context dependence and the need to exercise professional judgment in an attempt to weigh incommensurable values (van den Boogaard 2023, 187). In fact, proportionality is widely recognized as one of the most challenging law of armed conflict rules to apply (see Statman et al. 2020). Unless the commander had reason to place absolute confidence in the ability of the AI system to carry out a proportionality assessment autonomously, at a minimum, they would have had to clearly understand, review and accept the exact factual and legal reasoning on which the system based its recommendations. In addition, they would have had to consider all other information reasonably available to them to attain the highest level of certainty feasible in the circumstances prevailing at the time. Anything less would almost certainly not have met the standard of the reasonable military commander (Henderson and Reece 2021, 839–46).[42] Alternatively, the commander could have delegated to the machine the more modest task of determining how many civilians were likely to be affected by the attack, but then carry out the rest of the proportionality assessment themselves. However, even if the commander had relied on the AI system only in this more limited manner, they would have had to ensure that the machine's factual determinations met the certainty standards imposed by the law and consider these outputs together with any other reasonably available information.

If the AI system lacked the capability to perform these tasks, or the commander was not reassured that the system was capable of performing them at the level required by the law, the commander's second option would have been to review all AI outputs manually. As before, this calls into question the value of using an AI decision-support system in the

first place. However, provided that the commander and their staff made reasonable use of the information available to assess the level of incidental civilian harm to be expected from the attack and concluded that it would not be excessive, they would have discharged the obligation to refrain from launching a disproportionate attack. This remains true even if the attack ended up causing excessive incidental harm because their assessment was compromised by honest and reasonable mistakes (van den Boogaard 2023, 269–70).

However, we are informed by the case-study's authors that the system did not "highlight uncertainties, flag ethical concerns and provide a clear rationale for its recommendations." According to the authors, had the system "emphasized the limitations of its civilian movement data or required additional validation steps before recommending an airstrike, the commanding officer might have reconsidered or sought additional intelligence" (Dstl 2024). We strongly agree that any AI system must be designed to provide human operators with whatever information is necessary so that they can reassure themselves that the machine operates consistently with their legal obligations. In the present case, it appears that the system was not designed in this way. However, this does not in any way diminish the commander's obligations. If the commander relied on the system's outputs without reassurance that it operated in conformity with the law of armed conflict, had no clear understanding of the rationale for the system's recommendations and failed to take into account other reasonably available information, there is no doubt whatsoever that they failed in their precautionary duties. If this was the case, the excessive levels of incidental civilian harm were not the result of honest and reasonable mistakes, or a "tragic outcome" as the case-study puts it (Dstl 2024), but constituted a violation of the law of armed conflict.

3.3. Lessons to take away

Several lessons may be drawn from this analysis. What legal questions, if any, the use of an AI system raises under the law of armed conflict depends on what exactly the system does, what effects it generates and what happens to its outputs. Even AI decision-support systems that merely produce recommendations can raise substantial concerns. How these concerns should be addressed may not be obvious, as the meaning of the law often remains unsettled and how it applies to AI may be unclear. Faced with this uncertainty, the UK must formulate its own national position on how the law applies in this area. Without determining what exactly, in its view, the relevant rules and principles demand, the Ministry of Defence will not be able to decide what performance standards particular AI systems must meet and what technical capabilities they must possess to comply with the law. To proclaim that Defence always seeks to comply with its legal obligations under the law of armed conflict is an excellent starting point (UK Ministry of Defence (2025c), 8), but it is only that. Precisely what compliance involves is the real question and work remains to be done to answer this.

Humans must respect the law of armed conflict whenever they operate AI systems or rely on AI outputs just as in any other circumstances. This means that they must use AI technology in a manner that complies with their legal obligations. As our analysis illustrates, human operators cannot simply delegate certain tasks to a machine without reassuring themselves that the system operates consistently with

the law. If human operators fail to do so, they run the risk of violating their obligations and, in certain circumstances, may also incur individual criminal responsibility. The need for reassurance does not mean that commanders and operators must test and validate these systems personally. As the concept of "context-appropriate human involvement" championed by the UK in the context of lethal autonomous weapons systems recognizes, human involvement is not limited to the real-time operator, but extends across the lifecycle of the system to include those involved in its development, assurance, training and review.[43] Accordingly, commanders and operators may rely on the expertise and work of others, as necessary and appropriate, to reassure themselves that the systems they deploy are compliant.

Enabling machines to comply with the law of armed conflict autonomously is not an easy undertaking. Indeed, one school of thought suggests that determining the lawfulness of an attack must always be done by humans, not machines.[44] However, where no rule expressly or implicitly precludes this, human operators may task machines with making factual and legal determinations. The wider the tasks delegated to the system and the more difficult the operating environment is, the greater the normative and practical challenges become, as the proportionality rule demonstrates. Depending on the task delegated and the rules engaged, AI technology at its current stage of development may either be capable of autonomous compliance or it may not be.

Should the technology not enable the system to meet the performance standards and capability requirements demanded by the applicable rules, deploying the system or relying on its outputs without further human involvement will most likely break the law. This means that AI may not be a lawful option for certain use-cases or in certain operational environments. Even where a system is capable of performing its tasks at the requisite level demanded by the law, human operators must still monitor the system to ensure that it does in fact operate in a compliant manner and they must use any outputs consistently with their obligations. For example, as our analysis has highlighted, the use of an AI decision-support system's outputs must be reasonable and operators must consider other information reasonably available to them alongside the AI outputs.

Ethical considerations have an important role to play in armed conflict. The fact that a particular course of action is lawful does not mean that it is also the right thing to do. However, a preoccupation with ethical considerations breeds both compliance risks and misplaced caution if it remains uninformed by the law. Adopting an ethical perspective, the commentary accompanying our chosen case-study queries whether responsibility for the excessive civilian casualties lies with the commander or with the system's developers (Dstl 2024). Whatever the answer to that question is, approaching the matter from a legal perspective suggests that the commander almost certainly did not comply with their precautionary duties to do everything feasible to verify the target or to refrain from launching a disproportionate attack.

We hasten to underline that we do not question the importance of ethical considerations: our point is that they must not divert attention away from the legal considerations, as the two are distinct. The commentary to the case-study proclaims that it is the responsibility of developers to ensure that a system actively supports human judgment, rather than replaces it. The implicit assumption is that supporting human judgment is beneficial, whereas replacing it with a machine

outputs is bad or even impermissible. From a legal perspective, this misses the point. First, the dividing line between supporting or replacing human judgment is at best fluid. If the commander in our case-study had to decide whether incidental civilian harm was to be expected or not, and relied on the outputs of the AI system to this end, did the machine merely support their judgment or replace it? Second, and more importantly, whether machine outputs merely support or fully replace human judgment and decision-making, the humans concerned must comply with their obligations in both cases. It is not the extent of the cognitive tasks that are delegated to machines that determines the legality of the delegation, but whether the delegated tasks are performed and any outputs employed in compliance with the law of armed conflict.

4. The need to comply with the law

The UK is committed to developing and deploying AI in a manner that complies with the law of armed conflict (UK Ministry of Defence (2025c), 8). However, the law is not a monolith and compliance is not a simple binary matter. States have considerable room for manoeuvre in the interpretation and application of the rules. Where humanitarian considerations and military effectiveness are at odds, governments may prioritize one over the other. Despite the professed commitment to uphold the law, it is therefore perfectly conceivable that significant legal challenges encountered in the adoption of AI across Defence may prompt calls for the law to be fitted around the technology, especially where difficulties in resolving these challenges may prevent the development of much needed capabilities or delay their entry into service. In this section, we therefore briefly recall why adherence to the law of armed conflict matters, before we turn to discuss the respective duties of government and industry to comply with the rules.

4.1. Why compliance matters

The law of armed conflict is binding on the UK, its agencies and personnel as a matter of international law. The UK is a party to the major law of armed conflict treaties, such as the four Geneva Conventions of 1949,[45] and is bound by the customary law of armed conflict. Many of these rules have been incorporated into domestic law, for instance by the Cultural Property (Armed Conflicts) Act 2017.[46] Compliance is therefore not a matter of grace, but mandatory. A failure to respect the law of armed conflict could expose the UK to legal accountability in the form of State responsibility and may also engage the criminal liability of British service personnel.[47]

Government treats the law of armed conflict as an essential component of the international rule of law. The Ministry of Defence cites adherence to the rules as a key example of how Defence supports broader efforts to uphold an open international order.[48] Senior officials regularly profess their support for the law of armed conflict and pride themselves on Britain's record of compliance.[49] They also regularly demand that other parties comply with their own obligations.[50] Respect for the law of armed conflict is therefore not just a question of narrow legality, but involves wider considerations of international order and reputation.

In fact, Defence doctrine recognizes that respect for the law of armed conflict is closely linked to legitimacy in warfare, which is the perception by domestic and international audiences that a conflict and the conduct of forces during that conflict is justified and consistent with normative expectations.[51] A perception of compliance helps to maintain legitimacy, whereas non-compliance will almost certainly erode campaign authority.[52] This is so partly because many law of armed conflict rules serve humanitarian objectives by preserving human dignity in war, mitigating suffering and imposing limits on the destructive effects of conflict. Serious breaches of these rules, such as torture, medical experiments or wanton destruction, are not just technical violations of abstract norms, but defy basic human decency and values. As such, they often invite moral outrage and condemnation in international and domestic fora.

Complying with the law of armed conflict in the development and deployment of military AI systems is therefore prudent for both principled and instrumental reasons: it is mandatory, essential to the UK's reputation, the right thing to do and operationally expedient.

4.2. Government

Common Article 1 to the four Geneva Conventions of 1949 requires that the High Contracting Parties respect and ensure respect for the Conventions in all circumstances. The obligation reflects customary international law.[53] It is composed of two distinct, but related duties: the duty to "respect" and the duty to "ensure respect."

The duty to respect is the more straightforward component. It imposes a negative obligation on each State party to ensure that the conduct of its organs and agents complies with the provisions of the Geneva Conventions. In essence, this is a restatement of the principle of *pacta sunt servanda*, whereby a State must abide in good faith by the treaty obligations it has assumed (Focarelli 2010, 137–38).[54] For the UK, this means that its armed forces and other government agencies must refrain from acts that would violate the law of armed conflict. Accordingly, they must refrain from developing, deploying or otherwise operating AI systems in a manner that contravenes applicable law of armed conflict obligations. The duty could be breached, for example, if British forces were to deploy an AI system that collects data about enemy civilians or data belonging to them where this collection serves no reasonable military or security purpose related to the conflict.[55]

The duty to ensure respect is more complex and subject to considerable debate. The duty imposes a positive obligation on States, extending beyond mere abstention from violations to require proactive measures to promote, supervise and, where appropriate, enforce compliance with the law. The central controversy revolves around the question as to whether this duty is purely internal or whether it also has an external dimension requiring a State to ensure compliance by other States (Robson 2020; Schmitt and Watts 2020). A minimalist reading suggests the duty is purely inward-looking. On this view, a State is required to ensure respect for the law by its own organs, including its armed forces, and any *de facto* agents or other persons and groups acting on its instructions or under its direction or control. A somewhat broader variation of this approach posits that the duty to ensure respect extends to all persons and entities within a State's jurisdiction, including its nationals and any private corporate entities on its territory, even where such

persons or entities are not subject to its control or authority (Geiß 2015, 118). The maximalist interpretation argues that every State party to the Geneva Conventions must take appropriate measures to prevent or bring to an end violations committed by any other State party.[56] While the International Court of Justice has endorsed this approach,[57] it does not enjoy universal support.

The UK takes the view that Common Article 1 imposes "a duty to ensure that all those within a party's jurisdiction respect the Convention[s] and not an obligation to ensure respect for the Convention[s] by other States."[58] Accordingly, the UK charts a middle course between the minimalist and the maximalist position: it rejects the idea that it has a duty to ensure respect by other States, but accepts that it must ensure respect by persons and entities subject to its jurisdiction, rather than only persons or entities under its control. This implies that the UK considers itself bound to ensure that any AI developers and system manufacturers subject to its jurisdiction respect the law of armed conflict.

4.3. Industry

Private business entities are not High Contracting Parties to the Geneva Conventions and as such are not bound by the obligations under Common Article 1 or by its counterpart in customary international law (Gillard 2006, 130).[59] However, there are other ways in which the law of armed conflict may become applicable to their activities (Hughes 2020).

As interpreted by the UK, the duty to ensure respect requires the UK to take measures to secure compliance by persons or entities within its jurisdiction. The Geneva Conventions Act 1957 thus makes it a criminal offence for any person to commit a grave breach of the Geneva Conventions, Additional Protocol I or Additional Protocol III,[60] or to aid, abet or procure the commission of a grave breach by any other person, whether in or outside the UK.[61] Grave breaches, as defined by the Geneva Conventions and their Additional Protocols, include wanton destruction of property, launching an indiscriminate attack in the knowledge that it will cause excessive incidental civilian harm and making a person the object of attack in the knowledge that they are *hors de combat*.[62] Accordingly, amongst other things, individuals acting for private businesses that supply AI systems or services to British forces must be mindful of the prohibition of launching disproportionate attacks, as aiding or abetting the launching of such attacks – for instance in the circumstances of the hypothetical AI decision-support system we explored earlier – may render them criminally liable.[63]

Should a company or its agents act pursuant to the instructions of the UK or under its direction or control, their conduct would become attributable to the UK under the law of State responsibility.[64] In such circumstances, the UK would have to ensure that the company and its staff acted consistently with its obligations under the law of armed conflict. For example, a private business may provide an AI platform and cloud-based services to the Ministry of Defence based on a commercial contract. To the extent that the company thereby acts under the instructions, direction or control of the Ministry (Mačák 2016, 414–26), the latter must ensure that these acts are consistent with the law of armed conflict.

The UK has implemented export control measures for military and dual-use goods, software and technology pursuant to the Export Control Act 2002.[65] Military AI systems, software and technologies fall squarely within the scope of these controls and may require

a licence to be exported from the UK. An export licence will not be granted if doing so would be inconsistent with the Strategic Export Licensing Criteria issued by the Secretary of State.[66] Specifically, the Government will not grant a licence if to do so would be inconsistent with the UK's international obligations and relevant commitments (Criterion 1) or if it determines that there is a clear risk that the items might be used to commit or facilitate a serious violation of the law of armed conflict (Criterion 2(c)). To meet these criteria, businesses seeking to export AI systems, software or technologies that require a licence may need to ensure that the items destined for export or their likely use are compliant with the law of armed conflict.

Finally, various non-binding documents suggest that private business has a corporate responsibility to comply with the law of armed conflict. The United Nations Guiding Principles on Business and Human Rights (UNGPs) of 2011 declares that in situations of armed conflict, business enterprises should respect the standards of the law of armed conflict.[67] The UK was the first country to produce a National Action Plan to implement the UNGPs, although the Plan does not specifically mention the law of armed conflict.[68] The OECD Guidelines for Multinational Enterprises on Responsible Business Conduct of 2023 likewise declare that enterprises should respect the standards of the law of armed conflict in situations of armed conflict, adding that in the context of armed conflict or heightened risk of gross abuses, enterprises should conduct enhanced due diligence in relation to adverse impacts, including violations of the law of armed conflict.[69] As one of the Adherents to the OECD Declaration on International Investment and Multinational Enterprise, the UK has committed itself to recommend to multinational enterprises operating in or from its territories the observance of these Guidelines.[70] Private business supplying AI technologies and services that constitute military or security services, such as the maintenance and operation of weapons systems, may qualify as private military and security companies within the meaning of the Montreux Document and similar codes (see Lubin 2025).[71] At least on a wide reading, businesses that provide services which serve as a foundation layer for a military application layer, such as large language models powering the Maven Smart System, may also fall within the scope of these codes. The Montreux Document, supported by the UK and almost 60 other States, recognizes that States contracting with such companies have an obligation to ensure that they respect the law of armed conflict, that the companies themselves must comply with law of armed conflict rules imposed upon them under domestic law and that their personnel are obliged to comply with the law of armed conflict.[72]

5. Overcoming the AI innovation-obligation gap

As the previous section demonstrates, States retain primary responsibility to respect and to ensure respect for the law of armed conflict: the obligations incumbent on industry are more limited and mostly indirect in nature. As a result, these obligations are not distributed evenly across the lifecycle of AI systems (De Silva and Alahakoon 2022).

For example, the Geneva Conventions Act 1957 attaches criminal liability to certain war crimes under domestic law. The offences in question, such as wilful killing, wanton destruction or launching disproportionate attacks, pertain to the deployment phase of an AI system, not to its design or development phase. Criterion 2(c) of the Strategic Export Licensing Criteria, which requires licences to be denied should there be clear risk that the

items might be used to commit or facilitate a serious violation of the law of armed conflict, too is concerned with the deployment phase of AI systems. The OECD Guidelines call on industry to respect the standards of the law of armed conflict in situations of armed conflict. This excludes the design and development of AI systems in times of peace.

Even in situations that trigger the UK's duty to ensure that industry respects the law of armed conflict, for instance where private business acts under the direction or control of government, the impact on the design and development phase of AI is limited. This is so because few law of armed conflict rules are directly concerned with the design and development of means and methods of warfare. One notable exception is the duty imposed by Article 36 of Additional Protocol I to determine whether the employment of new weapons, means or methods of warfare would, in some or all circumstances, be prohibited by the Protocol or by any other rule of international law applicable to the UK.[73] This duty to review is engaged should UK government agencies study, develop, acquire or adopt new weapons, means or methods of warfare. It may also be engaged where the UK funds, sponsors or otherwise supports industry or other private entities to carry out these activities, for example in the framework of the Defence and Security Accelerator (DASA)[74] or NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) (Copeland 2024, 96).[75] However, it does not apply in circumstances where private business studies, designs or develops new AI-enabled weapons, means or methods of warfare independently of government (Nasu 2020, 136). Moreover, the rule is concerned exclusively with determining the legality of *using* new weapons, means or methods of warfare (Jevglevskaja 2021, 22).[76] Article 36 does not prohibit the development or possession of weapons, means or methods of warfare that cannot be deployed in compliance with the law of armed conflict (Dienelt 2018, 131).[77] Unless their development or possession is prohibited by other rules, such as arms control treaties to which the UK is a party,[78] nothing precludes the UK from designing, developing and possessing AI systems or technologies that cannot be deployed consistently with the law of armed conflict in some or all circumstances. Accordingly, the UK is not bound to ensure that industry only studies, designs or develops AI systems and technologies that are compliant with the law of armed conflict, since it is not subject to such an obligation itself.

Consequently, there is a distinct lack of international rules that directly or indirectly compel private businesses to only design and develop AI systems that can be deployed consistently with the law of armed conflict. This opens up a gap between technological innovation and expertise, which sits primarily with industry, and legal obligations and expertise, which resides mostly at the level of the State and its agencies. The present section explores why this is a problem and offers some suggestions as to how government and industry might address this gap.

5.1. AI capability development: dual pathway

The development of military AI capabilities in the UK now follows two tracks that proceed from fundamentally different starting points: a requirements-led approach where government defines specific capability gaps and solicits industry solutions and an innovation-led approach where industry or academia develop capabilities that may be matched to emerging or unrecognized Defence needs.

Requirements-led capability development follows the traditional Defence acquisition model, which is a top-down process characterized by the centralized articulation of requirements and typically involves complex programmes and long timelines (National Audit Office 2015; Taylor 2019). The Ministry of Defence, through its various commands and capability development organizations, identifies specific operational requirements arising from strategic assessments, capability gap analysis, lessons learned or evolving threats. These requirements are then translated into procurement programmes managed primarily through organizations that sit within the National Armaments Directorate Group. For major AI-enabled programmes such as the Future Combat Air System, this process normally involves detailed requirement specifications, competitive tendering, contract negotiation and staged development with formal reviews at various points in the project lifecycle (e.g. Defence Equipment and Support 2025).

The requirements-led approach was designed primarily for the procurement of hardware and as such does not sit well with the AI sector, as recognized by government (House of Commons Defence Committee 2025a, para. 37). The timelines are fundamentally different. Writing algorithms does not involve lengthy manufacturing processes and therefore significantly outpaces the traditional procurement cycle, as does the evolution of the underlying technology. Many transformative AI capabilities emerge from commercial research and development, meaning that innovation is driven by factors other than capability needs identified centrally by government. It also means that AI suppliers are more likely to be companies operating across civilian and military markets (House of Commons Defence Committee 2025b; Onderco 2025, 612) and their business model may not be aligned with the traditional acquisition process. Start-ups typically follow a venture capital-funded development model where they build capabilities using private investment, before seeking government contracts for deployment, further development or scaling up (González 2024). Helsing offers one example. Founded in 2021, the company secured major venture capital funding through multiple rounds to develop products and services such as its Altra decision-support platform and HX-2 strike drone (Contrary Research 2025). In the first seven months of 2025, UK defence technology start-ups were reported to have attracted EUR 243 m of private investment (Nicol-Schwarz and Sraders 2025). Whether this figure is entirely accurate or not, it illustrates the flow of private investment into the sector and thus the trend towards privately funded development of military and dual-use AI capabilities.

The mismatch between the requirements-led approach and the prevailing dynamics of the AI sector drive demand for an alternative, innovation-led pathway that supports the development of AI capabilities from the bottom up. One model that emerged during the Global War on Terror involves close collaboration between front line commands and technology companies, leading to the rise of what Tony King has termed a new "military-tech complex" (King 2025, 60–98). Another model involves industry developing AI systems and services through private investment, before government purchases these products off the shelf. For instance, Helsing's edge-AI software, drones and fire control software are now being tested by British forces as part of Project ASGARD, itself part of the wider digital targeting web (Cranny-Evans 2025). Palantir and Anduril offer another example: these US-based companies have developed a range of commercially available AI platforms with the help of private investment before entering the UK market. As Anduril puts it: "[u]nlike most defense companies, we don't wait for our customers to tell us what

they need" (Anduril 2025). The Ministry of Defence is also contracting with major technology companies, such as Google, to access their cloud-based services and AI platforms (Google Cloud 2025).

Yet another model of innovation-led capability development involves government stepping into the role of private funders, in essence, to enable business to develop exploitable ideas at varying levels of technological readiness. Since 2016, DASA has provided funding to 461 small and medium enterprises, including in the AI sector (Beauhurst 2025), though the scale and impact of this support has been relatively limited (House of Commons Defence Committee 2025b, para. 64). In July 2025, the Ministry of Defence launched UK Defence Innovation (UKDI). Supported by an annual budget of GBP 400 m, UKDI is meant to provide UK businesses with a simplified entry point into Defence acquisition. In November 2025, the Defence Artificial Intelligence Centre (DAIC) announced the creation of "AI Model Arena," an online platform enabling suppliers to test and demonstrate their models against Defence use cases (UK Ministry of Defence 2025a). All these efforts further reinforce the trend towards innovation-led capability development.

Neither the requirements-led nor the innovation-led capability pathway guarantees that all AI systems acquired within these frameworks are compliant with the law of armed conflict. The Ministry of Defence carries out formal legal reviews pursuant to Article 36 of Additional Protocol I at several points in the traditional, requirements-led procurement cycle. The first of these takes place when the Ministry decides to commit funds to developing a specific capability, known as "initial gate" (UK Ministry of Defence 2016). This will only cover AI systems that fall within the scope of Article 36 because they constitute weapons, means or methods of warfare. As our earlier analysis of the hypothetical AI decision-support system has shown, not all AI systems are weapons, means or methods of warfare, meaning that not all systems or services that raise law of armed conflict concerns are subject to a mandatory review under Article 36, as traditionally understood. The same issue arises with innovation-led capabilities: an AI-enabled strike drone developed by a private business will trigger an Article 36 review should the UK decide to purchase or otherwise adopt the system, but privately developed AI platforms, applications, decision-support systems or cloud services may fall outside the scope of Article 36. Moreover, even where the Ministry of Defence does review an AI system's compatibility with the law of armed conflict, either under Article 36 or under a more inclusive process, this may come at a relatively late stage in its design or development. This is almost certainly going to be the case for privately funded and developed systems intended for commercial sale off the shelf. Exploitable designs may already be at a relatively mature stage of development before they receive support from UKDI or other parts of government that would trigger a formal Article 36 review.

5.2. Incentives and obstacles

The later the legal assessment of an AI system takes place, the more time, effort and resource will have been invested into its development before concerns over its compatibility with the law of armed conflict may be identified. This could pose significant problems. Should it turn out that the system cannot be used consistently with the UK's obligations, it must either be redesigned or be deployed subject to whatever restrictions

will ensure compliance. Such redesigns could be costly, wasteful and time-consuming, while deployment restrictions could significantly diminish the system's military utility. In extreme cases, it may transpire that a system is not legally viable at all or that its lawful deployment is possible only in such limited circumstances that it offers no real operational benefit. In such situations, the financial, operational and opportunity costs will either have to be absorbed or the capability will have to be abandoned entirely.

The higher these costs and the more pressing the need for the capability, the more likely it is that scrupulous compliance with the law of armed conflict will be seen as an obstacle standing in the way of operational readiness. Calls for cutting legal corners and for forward-leaning interpretations of the rules will grow louder, most likely fuelled by concerns that taking the law of armed conflict too seriously will simply hand adversaries not committed to respecting the rules a strategic advantage (cf. Karp and Zamiska 2025, 51; National Security Commission on Artificial Intelligence 2021, 95; Special Competitive Studies Project 2024, 19). Assessing compliance at a late stage in the AI development cycle therefore runs the risk of creating a binary choice between either accepting costs and capability shortfalls or playing fast and loose with the rules. Neither of these is a good option.

As we have noted earlier, the law of armed conflict does not compel industry to design and develop only AI systems that are consistent with the applicable rules, while indirect obligations to do so are limited and often not particularly effective (e.g. Stavrianakis 2023). However, other incentives may encourage compliance. Several companies have positioned themselves as defenders of democracy, liberal values or the West more generally. Palantir notes that its business has its "origins and identity in the defense of the values and traditions of liberal democratic societies" (Palantir 2024). Helsing declares that it was founded to "protect our democratic values and open societies" (Helsing 2025). Anduril describes its mission as "rebooting the arsenal of democracy" (Anduril 2022). The appeal to these values would seem to imply a commitment to the rule of law and to humanitarian principles. In some cases, this is acknowledged in express terms. Palantir, for example, accepts that it has a responsibility to ensure that the capabilities it builds and workflows it enables are "informed" by its customers' obligations under the law of armed conflict (Palantir 2025). Accepting such a responsibility also makes commercial sense (Allenhöfer 2026). At the end of the day, if compliance with the law of armed conflict is a non-negotiable requirement for the customer, then AI capabilities and workflows that are incompatible with the law will not sell. For this reason, enterprises that take a proactive approach to compliance may also gain a competitive advantage over rivals that fail to engage with legal concerns.

However, voluntary compliance by industry faces considerable obstacles. Since it is uncertain how the law of armed conflict applies to the use of military AI systems, what exactly the law requires, and how individual States interpret these requirements in their role as customers, is not clear. Most businesses lack the capacity to engage with this question. The vast majority of the UK's AI sector is made up of microenterprises and small to medium enterprises (Department for Science 2025). Many of these businesses do not have access to in-house legal support at all, while companies that do employ lawyers tend to prioritize other, more pressing practice areas, such as commercial law, intellectual property and dispute resolution. While Defence primes and large multinational AI enterprises may benefit from in-house support on questions of international law, it is

simply not realistic to expect most technology start-ups and other small businesses to have access to the legal expertise necessary to engage with the law of armed conflict at a level and depth required to ensure compliance. In any event, it is ultimately for States to determine what the law demands (see Droege and Giorgou 2022). Industry cannot make up the UK's mind as to what its obligations are in relation to military AI: that is Government's prerogative and responsibility.

The nature of the industry also creates powerful disincentives for voluntary compliance. Industry's overwhelming imperative is to innovate at speed and scale. Leaders of major companies reiterate time and again that innovating faster and better is the key to developing capabilities that will deter adversaries and ensure peace (Luckey 2025; Schmidt 2023). The ability to "rapidly build and deploy critical new capabilities" at scale also happens to be the primary goal of the venture capital funds investing in the sector (Lonsdale 2023), as this is what ultimately secures their return on investment (Schwarz 2025). Seen from this perspective, compliance with the law of armed conflict starts to look more like a regulatory burden that could impose substantial costs and delays, rather than a source of competitive advantage. Indeed, the normative commitments made by industry are guarded. Palantir suggests that it has a responsibility to ensure that its products and services are "informed" by the law of armed conflict (Palantir 2025), but this is not necessarily the same as accepting a responsibility to ensure compliance. Helsing emphasizes its commitment to "put ethics at the core of defence technology development" (Helsing 2025), but ethical considerations are distinct from the law of armed conflict.

5.3. The responsibility of government

Ultimately, in the absence of sufficient expertise and overriding incentives, it cannot be expected that industry will design and develop its products and services to be compliant with the law of armed conflict. To avoid ending up in a position where it must choose between costly redesigns or risking non-compliance, government must step up.

First, stakeholders across Defence must recognize that a significant knowledge gap exists when it comes to the application of the law of armed conflict to military AI systems. This starts with accepting that the legal and ethical considerations involved are distinct matters. The Ministry of Defence intends JSP 936 to help industry understand clearly what responsible AI adoption entails (UK Ministry of Defence 2025f, 5). Yet the idea that JSP 936 has clearly articulated the requirements that flow from the law of armed conflict is overly optimistic. Given the lack of legal detail in JSP 936, industry appears to treat that document merely as a statement of the Ministry's ethical standards (cf. Google Cloud 2025). Government itself seems to think that JSP 936 is concerned only with ethical expectations (House of Commons Defence Committee 2025a, para. 29). Moreover, key aspects of the relationship between the five ethical principles and the law of armed conflict remain unclear. The Ministry of Defence has rightly acknowledged that the five principles do not override its legal obligations (UK Ministry of Defence (2022b), 9). However, the law of armed conflict does not consist solely of obligations, but also includes permissions (Quintin 2020). For example, whereas States are bound not to deliberately target civilians,[79] they are not *obliged* to prosecute lawful targets, but are *at liberty* to do so. In the implementation of the principle of human centricity, JSP 936

demands that an assessment must be made of the impact that AI could have on all stakeholders, including humans targeted by military action, to ensure that the effects on them "are as positive as possible and justified as outweighing negative effects where these may arise" (UK Ministry of Defence (2025c), para. 52). Does this mean that the principle of human centricity requires an ethical assessment and justification for using lethal force against persons liable to attack that is distinct and more stringent than the legal requirements that render such an attack permissible? In other words, does killing enemy combatants and other persons liable to attack require special ethical assessments where this involves the use of AI capabilities?[80]

There remains an urgent need for the Ministry to identify the implications the law of armed conflict has for military AI. JSP 936 declares that "[i]ndustry and developers will need to obtain their own legal advice as to the legal framework that applies to their development of the product" (UK Ministry of Defence (2025c), para. 47). Of course, private enterprises must obtain legal advice about their own obligations when they develop products and services, for instance on commercial matters or intellectual property rights. However, it is not industry's responsibility to seek legal advice to clarify what the law of armed conflict requires from the UK and to translate this into performance requirements: that ball lies firmly in the Ministry's court. Important work is already under way within the Ministry, including formulating a general framework of principles to guide compliance efforts and addressing the legal implications of military AI as part of the ongoing revision of the UK's *Manual on the Law of Armed Conflict*. These and related efforts in the Ministry must be accelerated, fully resourced and followed up to transform the current high-level guidance into specific performance requirements and expectations for individual use-cases.

Second, the scale and the nature of the challenges involved in applying the law of armed conflict to military AI must be properly understood. There appears to be a tendency to assume that the rules simply await implementation and that this is going to be straightforward. The Defence Artificial Intelligence Strategy notes that the law of armed conflict "provides a robust, principle-based framework," "imposes positive obligations that take into account core principles," such as distinction, and that "nothing about AI fundamentally changes" the UK's obligations under international law (UK Ministry of Defence (2022a), 52). This is all true, but it overlooks the fact that how the law applies is subject to considerable uncertainty and that this directly impacts the development of AI for military use. Without acknowledging and addressing this uncertainty, the Ministry of Defence will not be able to offer clear guidance to industry and to formulate detailed expectations as to what performance criteria and other conditions individual AI systems and services must meet so as to enable commanders and other operators to comply with their obligations under the law of armed conflict. It is important to emphasize that it is not only lethal systems that raise law of armed conflict concerns, as is sometimes assumed (e.g. National Security Commission on Artificial Intelligence 2021), but also other use-cases, including AI decision-support systems, and how these fit into broader decision-making processes, for instance the targeting cycle.

Third, the Ministry of Defence must communicate its expectations to industry and put in place processes and procedures to ensure that these expectations inform the design and development of AI systems at the appropriate stage (see also Goussac and Boulanin 2026, 26). The Ministry cannot rely solely on legal

reviews conducted under Article 36 of Additional Protocol I, as traditionally understood, for these purposes. As we have noted, not all AI systems fall within the scope of Article 36 and formal reviews may come too late in the lifecycle of those systems that do. If the Ministry wants to encourage businesses to design and develop systems that are compliant with its obligations, it will need to proactively engage with industry. This requires raising awareness within the AI sector about the need to take law of armed conflict considerations into account, providing detailed guidance on what the legally compliant design and development of AI entails and working with individual businesses to address the legal challenges that specific systems and use-cases raise. These are not tasks that should be left to individual commands and their legal advisors, as they are ill-equipped to carry them out other than in an *ad hoc* fashion (cf. Knack et al. 2025, 8–9). Instead, they demand a centralized approach that brings together the resources, technical expertise and depth of understanding necessary to offer effective advice and support to the sector, ensure consistency and build institutional knowledge.

The legal branch of what until recently was Defence Futures is already spearheading some of this work. The branch is responsible for conducting Article 36 reviews and in this capacity is raising awareness about the legal aspects of capability development among stakeholders, such as Defence Science and Technology. The team understand the need for agility and endeavours to offer guidance to Defence clients at an early stage, before Article 36 reviews are initiated. The need for early legal assessments has been recognized by other organizations too. For example, the Army Artificial Intelligence Centre has deliberately sought to involve legal advisors in its AI assurance work and application of JSP 936, so that legal concerns are identified as early as possible in the design and development process. However, gaps remain. While the legal branch of former Defence Futures engages with existing Defence suppliers, it does not have a mandate to interact with industry more generally, including start-ups and other businesses that are new to the defence sector and have the greatest need for guidance. Nor does it have a mandate to provide support to industry, which as we saw is expected to obtain its own legal advice. However, not only is it the Ministry's responsibility to clarify what requirements flow from its own obligations under the law of armed conflict, but it also needs to provide industry with an interlocutor to offer practical guidance and advice if it wants businesses to take these requirements into account in the design and development of new capabilities. The legal team at former Defence Futures, which consists of experienced legal advisors from the three services, would be a natural fit for this role. However, it would have to be properly resourced to handle any increase in its responsibilities, as its capacity is limited and already stretched. Close links would have to be established with DAIC, UKDI, Main Building, Front Line Command AI leads and other stakeholders, including industry and academia, to ensure consistency of effort and complementarity. This includes giving careful consideration not only to the division of responsibilities, but also to process. Since innovation-led approaches to AI capability development are driven by a desire to remove traditional procurement barriers and to speed up the acquisition process, demanding that stakeholders slow down and consider legal matters seems contrary to the start-up ethos that is taking hold. Nevertheless,

space will have to be carved out to enable the law of armed conflict to be properly considered at an early stage.

6. Conclusion

The widespread adoption of AI capabilities presents a significant opportunity to enhance the operational effectiveness of the British armed forces. However, it also raises difficult questions under the law of armed conflict. The law is technology-agnostic and therefore applies to AI systems. This much is certain. However, what the rules require in specific cases remains unclear, due to the contextual nature of the law and the distinct features of AI technologies.

Government is committed to the safe and responsible use of AI for military purposes and to always comply with its international obligations (House of Lords Select Committee on AI in Weapon Systems 2024, para. 5). Respect for the law of armed conflict is therefore a non-negotiable baseline requirement. However, a commitment to compliance and clarity about what this entails are not the same thing. The uncertainty surrounding the application of the law of armed conflict to military AI means that sweeping assertions about the need to respect the law, however sincere, are insufficient to carry this respect into practice without detailed guidance.

This brings into focus a structural challenge that affects the development of military AI in the UK. The technical expertise resides predominantly in the commercial sector with the businesses developing the algorithms, platforms and services that Defence seeks to rely upon. Yet the legal expertise and interpretative authority concerning the law of armed conflict resides at the level of the Ministry of Defence and wider government. It is for government to determine what its obligations require and to communicate these requirements to industry to inform the design and development of their products and services. Important steps have been taken in this direction, with various lines of effort being pursued, but these do not go far enough. The first part of JSP 936, the Ministry of Defence's directive on responsible AI development, devotes scant attention to legal matters. The recently published AI Practitioner's Handbook (AIPH), which forms the second part of JSP 936, offers extensive guidance on ethical assurance, but at the time of writing, its section on legal governance remains to be published.[81] In the context of lethal autonomous weapons systems, the UK has explained in some detail how "context-appropriate human involvement" should be understood at the conceptual level,[82] yet there is little to no guidance in the public domain to clarify what exact forms and levels of human involvement the government considers appropriate for what specific use-case and circumstances. Industry cannot be expected to design systems to be compliant with the law if it does not know what compliance entails. This knowledge gap has real consequences: AI systems could be developed at considerable expense only to prove legally unviable or commanders could be asked to deploy systems with insufficient reassurance that they can do so consistently with their legal obligations.

The Ministry of Defence must accelerate ongoing work in this area to bridge this gap by determining what exactly compliance with the law of armed conflict requires, clearly communicate to industry the legal expectations that flow from this and provide businesses with practical guidance and support to meet these requirements. Legal concerns must be identified and addressed early in the AI lifecycle, before substantial resources

have been invested. This requires a coordinated, coherent and properly resourced approach that is best centred around the legal team at former Defence Futures, working in close collaboration with DAIC, UKDI and other key stakeholders. The path forward requires government to commit to compliance not merely as a matter of principle, but to encourage, support and, where necessary, mandate industry to design systems with compliance in mind, enabling commanders to deploy those systems secure in the knowledge that they can do so whilst respecting their obligations under the law of armed conflict.

Notes

1. UN General Assembly Resolution 79/239, Artificial Intelligence in the Military Domain and its Implications for International Peace and Security, 24 December 2024, para. 1.
2. NATO, Summary of the NATO Artificial Intelligence Strategy, 22 October 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.
3. Bureau of Arms Control, Deterrence, and Stability, "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy" (United States Department of Defense 2023) https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/.
4. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), 8 June 1977, 1125 UNTS 3, Article 48.
5. Additional Protocol I, Article 48.
6. Additional Protocol I, Article 57(2)(c).
7. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (Geneva Convention I), 12 August 1949, 75 UNTS 31, Article 12.
8. International Committee of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (Cambridge University Press, 2016), para. 1348.
9. International Committee of the Red Cross, *Commentary on the First Geneva Convention*, para. 747.
10. See Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, CCW/GGE.1/2019/3, 25 September 2019, para. 17(b).
11. e.g. Additional Protocol I, Articles 41, 51(3) and 52(2).
12. In particular, precautionary obligations: Additional Protocol I, Article 57.
13. Additional Protocol I, Article 1(3).
14. Additional Protocol I, Article 49(1).
15. Additional Protocol I, Article 57(2)(a)(ii).
16. Ermittlungsverfahren gegen Oberst Klein und Hauptfeldwebel W. (Kunduz) (2010), 16 April 2010, 46–47 (Generalbundesanwalt) (declaring proportionality to be inapplicable, despite civilian casualties, as the accused expected no incidental civilian harm); confirmed by Hanan v. Germany, App. No. 4871/16, Judgment, 16 February 2021, paras 211–18 (Grand Chamber).
17. Additional Protocol I, Article 57(2)(a)(i).
18. See United Kingdom, Statement on Ratification of AP I, 28 January 1998, 2020 UNTS 75. See also Danish Ministry of Defence, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations* (Defence Command Denmark, 2016), 323; New Zealand Defence Force, *Manual of Armed Forces Law: Law of Armed Conflict* (2nd ed., Volume 4, 2022), § 8.7.2.
19. UK Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict (JSP 383)* (Oxford University Press 2004), paras 2.5.3 and 16.45.2. See also United States Department

of Defense, *Law of War Manual* (updated ed., 2023), §§ 5.3.1 and 5.5.3; Danish Ministry of Defence, *Military Manual*, 326.
20. See Danish Ministry of Defence, *Military Manual*, 323–25.
21. Additional Protocol I, Articles 50(1) and 52(3).
22. United States Department of Defense, *Law of War Manual*, § 5.4.3.2.
23. UK Ministry of Defence, *Manual of the Law of Armed Conflict*, para. 5.36 (fn. 224). See also Protocol II, Article 3(4), Protocol III, Article 1(5) and Amended Protocol II to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, 10 October 1980, 162 UNTS 1342 1980.
24. International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (2008), 76.
25. UK Ministry of Defence, *Manual of the Law of Armed Conflict*, para. 5.32.2.
26. Additional Protocol I, Article 50(1).
27. Additional Protocol I, Article 57(2)(a)(i).
28. Additional Protocol I, Article 41(2)(b).
29. Additional Protocol I, Article 40.
30. Additional Protocol I, Article 51(4)(b). See International Committee of the Red Cross, *Autonomous Weapon Systems and International Humanitarian Law: Selected Issues* (2025), 7.
31. Prosecutor v. Stanislav Galić (2003) Judgment and Opinion, IT-98–29-T, 5 December 2003, para. 60 (ICTY Trial Chamber).
32. Rome Statute of the International Criminal Court, 17 July 1998, 2187 UNTS 90, Article 8(2)(b)(i).
33. Additional Protocol I, Articles 57(2)(a)(ii) and (iii).
34. See Chairman of the Joint Chiefs of Staff, *No-Strike and the Collateral Damage Estimation Methodology*, CJCSI 3160.01A (2012).
35. Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann, eds., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Leiden: Martin Nijhoff, 1987), para. 1402. See also International Committee of the Red Cross, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977* (2006), 9–10.
36. Australian Government, *Australia's Guide to the Legal Review of New Weapons, Means or Methods of Warfare* (2024), 3.
37. Sandoz, Swinarski, and Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, para. 1402. See also International Committee of the Red Cross, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, 9–10.
38. See Additional Protocol I, Article 51(5)(a) (referring to "an attack by bombardment by any methods or means").
39. Sandoz, Swinarski, and Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, para. 2208.
40. Prosecutor v. Stanislav Galić (2003), para. 58. See also the statements and declarations made on ratifying Additional Protocol I by Canada, 20 November 1990, 1591 UNTS 462; Germany, 14 February 1991, 1607 UNTS 526; United Kingdom, 28 January 1998, 2020 UNTS 75.
41. Norwegian Ministry of Defence, *Manual of the Law of Armed Conflict* (Norwegian Chief of Defence 2013), para. 2.24; Danish Ministry of Defence, *Military Manual*, 324.
42. International Criminal Tribunal for the Former Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia* (2000), para. 50.
43. United Kingdom, Statement – Topic 3, 9 March 2023, Group of Governmental Experts on Lethal Autonomous Weapons Systems, 1.

44. International Committee of the Red Cross, *Autonomous Weapon Systems and International Humanitarian Law: Selected Issues*, 5–6.
45. Geneva Convention I; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Geneva Convention II), 12 August 1949, 75 UNTS 85; Convention Relative to the Treatment of Prisoners of War (Geneva Convention III), 12 August 1949, 75 UNTS 135 and Convention Relative to the Protection of Civilian Persons in Time of War (Geneva Convention IV), 12 August 1949, 75 UNTS 287.
46. 2017 c. 6.
47. e.g. *R. v. Alexander Wayne Blackman* [2017], EWCA Crim 190.
48. *UK Ministry of Defence, Defence in a Competitive Age* (2021), 8.
49. e.g. Luke Pollard, HC Deb. 30 June 2025, Vol. 770, Col. 18; David Lammy, HC Deb. 16 October 2024, Vol. 754, Col. 52WS. See also House of Commons International Development Committee, *Protection not Permission: The UK's Role in Upholding International Humanitarian Law and Supporting the Safe Delivery of Humanitarian Aid*, Fifth Report of Session 2024–25, HC 526 (2025), paras 14–18.
50. See Foreign, Commonwealth and Development Office, "UK and Partners Unite to Sanction Ministers inciting West Bank Violence," 10 June 2025; Foreign, Commonwealth and Development Office, "The Evidence of Russia's Violations of International Humanitarian Law is Substantial and Growing: UK Statement to the OSCE," 3 October 2024; and Foreign, Commonwealth and Development Office, "Joint Statement on Attacks against Civilians and Humanitarian Workers in Sudan," 6 June 2025.
51. UK Ministry of Defence, *UK Defence Doctrine (JDP 3–46)* (2022c), paras 2.49–2.51.
52. British Army, *The Aitken Report: An Investigation into Cases of Deliberate Abuse and Unlawful Killing in Iraq in 2003 and 2004* (2008), para. 5.
53. Jean-Marie Henckaerts and Louise Doswald-Beck, eds., *Customary International Humanitarian Law, Volume I: Rules* (Cambridge: Cambridge University Press 2005), Rule 139.
54. Vienna Convention on the Law of Treaties, 23 May 1969, 1155 UNTS 332, Article 26.
55. Geneva Convention IV, Article 27(4).
56. International Committee of the Red Cross, *Commentary on the First Geneva Convention*, paras 164–73.
57. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory Advisory Opinion, 2004 ICJ Rep. 136, para. 158; Alleged Breaches of Certain International Obligations in respect of the Occupied Palestinian Territory (Nicaragua v. Germany), Provisional Measures, Order 2024 ICJ Rep. 560, para. 23.
58. *Al-Haq v. Secretary of State for Business and Trade* [2025], EWHC 1615 (Admin), para. 49.
59. AFPS and PLO v. Alstom and Veolia (2013) 52 ILM 1161, 1177–79 (Versailles Ct. App).
60. 1957 c. 52, s. 1(1).
61. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem 8 December 2005, 2404 UNTS 261.
62. Geneva Convention IV, Article 147; Additional Protocol I, Article 85(3)(b) and (e).
63. See Swedish Prosecution Authority, "Prosecution for Complicity in Grave War Crimes in Sudan," 11 November 2021; Cour de cassation, criminelle [Supreme Court for Criminal Matters], Appeal No 19–87.367 (2021) ECLI:FR:CCASS:2021:CR00868, 7 September 2021, para. 80 (Lafarge).
64. International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission to the General Assembly, UN GAOR, 56th Sess., Supp. No. 10, Article 8, UN Doc. A/56/10 (2001).
65. 2002 c. 28.
66. Anne-Marie Trevelyan, HC Deb. 8 December 2021, HCWS449.
67. United Nations, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (2011), 14.

68. UK Government, *Good Business: Implementing the UN Guiding Principles on Business and Human Rights*, Cm 9255 (2016).
69. Organisation for Economic Co-operation and Development, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct* (2023), para. 45.
70. Declaration on International Investment and Multinational Enterprises, as amended on 27 October 2023, OECD/LEGAL/0144, Article IV.
71. International Committee of the Red Cross and Switzerland, *The Montreux Document: On Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* (2008), 9. The International Code of Conduct for Private Security Service Providers includes within its definition of security services the "operational and logistical support for armed or security forces, including training and advice, intelligence, surveillance and reconnaissance activities." See Switzerland, *International Code of Conduct for Private Security Service Providers* (2010), B. The UK Government has fully participated in the drafting of the Code. See UK Government, *UK Voluntary Report on the Implementation of International Humanitarian Law at Domestic Level (Second Edition)* (2024), 78
72. International Committee of the Red Cross and Switzerland, *The Montreux Document*, paras 3, 22 and 26(a).
73. Additional Protocol I, Article 36.
74. UK Ministry of Defence, "Defence and Security Accelerator," https://www.gov.uk/government/organisations/defence-and-security-accelerator.
75. UK Ministry of Defence, "NATO DIANA UK Accelerator: Welcome to the UK Accelerator," https://www.gov.uk/government/organisations/defence-and-security-accelerator.
76. International Committee of the Red Cross, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, 4.
77. Sandoz, Swinarski, and Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, para. 1471.
78. e.g. Convention on Cluster Munitions, 30 May 2008, 2688 UNTS 39.
79. Additional Protocol I, Article 51(2).
80. The fact that JSP 936 declares that the "concept of harmful effects is distinct from the intended military effects of certain capabilities" (para. 55) may suggest that the answer is negative, but it is not clear whether this "concept of harmful effects" is meant to be a reference to the "negative effects" mentioned earlier (para. 53) or which kind of AI capabilities are meant by "certain capabilities."
81. See https://www.digital.mod.uk/policy-rules-standards-and-guidance/aiph/, 21 May 2026.
82. e.g. United Kingdom, Expert Paper: The Human Role in Autonomous Warfare, 18 November 2020, CCW/GGE.1/2020/WP.6.

Acknowledgments

We are grateful to colleagues in government, industry and academia for comments on earlier versions of this paper. We also thank the reviewers for their comments. All views expressed are our own and do not necessarily represent the position of any institution.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Aurel Sari is a Professor of Public International Law at the University of Exeter and Non-Resident Senior Research Fellow, Corvinus Institute of Advanced Studies (CIAS), Corvinus University of Budapest. His research focuses primarily on international conflict and security law, including the law of armed conflict. He is a core contributor to the *West Point Manual on the International Law Applicable to Artificial Intelligence in Warfare*. He is a former Senior Fellow of the United States Military Academy and Fellow of Supreme Headquarters Allied Powers Europe.

Geraint Evans is an Honorary Professor at the University of Exeter. His research interests include applied systems theory, capabilities development, information theory, organizational science and the socio-technical dynamics of AI integration. He has previously led AI research and capability development with the public and private sector. He is an Honorary Fellow of the Strategy and Security Institute at Exeter, having previously been a Senior Research Fellow at the Defence Data Research Centre.

References

Allenhöfer, A. 2026. "Procuring Tomorrow: IHL Compliance as a Strategic Factor in Military AI Procurement." In *18th International Confernece on Cyber Conflict: Security Tomorrow*, edited by C. Kwan, M. Cvetko, A. Dollimore, M. Tolppa, and B. M. Åkesson, 51–70. Tallinn: NATO CCDCOE.

Anduril. 2022. "Rebooting the Arsenal of Democracy: Anduril Mission Document." 6 May 2022. https://www.anduril.com/article/rebooting-the-arsenal-of-democracy-anduril-mission-document/.

Anduril. 2025. "Mission." https://www.anduril.com/mission/.

Australian Government. 2024. "Australia's Guide to the Legal Review of New Weapons, Means or Methods of Warfare." Canberra. 10 April 2024.

Baruch, P. S., and N. Neuman. 2011. "Warning Civilians Prior to Attack Under International Law: Theory and Practice." *International Law Studies* 87:359–414.

Beauhurst. 2025. *Defence and Security Accelerator: Growth Impact Report 2025*. UK Defence Innovation and Defence and Security Accelerator. 13 May 2025.

Bennett, B., and G. C. Anthony. 2021. "Automated Common-Sense Spatial Reasoning: Still a Huge Challenge." In *Human-Like Machine Intelligence*, edited by Muggleton, Stephen, and Nicholas Chater, 405–429. Oxford: Oxford University Press.

Bergengruen, V. 2024. "How Tech Giants Turned Ukraine into an AI War Lab." Time. 8 February 2024. https://time.com/6691662/ai-ukraine-war-palantir/.

Bondar, K. 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*. Washington, DC: Center for Strategic and International Studies.

Boothby, B. 2025. "AI Warfare and the Law." *International Law Studies* 104:1–540.

British Army. 2008. *The Aitken Report: An Investigation Into Cases of Deliberate Abuse and Unlawful Killing in Iraq in 2003 and 2004*. 25 January 2008.

Bruun, L., and M. Bo. 2025. *Bias in Military Artificial Intelligence and Compliance with International Humanitarian Law*. Stockholm: Stockholm International Peace Research Institute.

Burrell, J. 2016. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." *Big Data & Society* 3 (1): 1–12. https://doi.org/10.1177/2053951715622512.

Chairman of the Joint Chiefs of Staff. 2012. "No-Strike and the Collateral Damage Estimation Methodology." CJCSI 3160.01A, Washington, DC. 12 October 2012.

Choi, Y. 2022. "The Curious Case of Commonsense Intelligence." *Daedalus* 151 (2): 139–155. https://doi.org/10.1162/daed_a_01906.

Coco, A., and D. Talita. 2024. "'Handle with Care': Due Diligence Obligations in the Employment of AI Technologies." In *Research Handbook on Warfare and Artificial Intelligence*, edited by Geiß, Robin, and Henning Lahmann, 234–260. Cheltenham: Edward Elgar.
Cohen, A., and D. Zlotogorski. 2021. *Proportionality in International Humanitarian Law: Consequences, Precautions, and Procedures*. Oxford: Oxford University Press.
Contrary Research. 2025. "Helsing." 23 March 2025. https://research.contrary.com/company/helsing.
Copeland, D. 2024. *A Functional Approach to the Legal Review of Autonomous Weapon Systems*. Leiden: Brill.
Cranny-Evans, S. 2025. "Project ASGARD: The British Army's Path to Doubling Lethality." *Calibre Defence*. 21 July 2025. https://www.calibredefence.co.uk/project-asgard-the-british-armys-path-to-doubling-lethality/.
Danish Ministry of Defence. 2016. *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*. Koppenhagen: Defence Command Denmark.
Defence Equipment and Support. 2025. "Autonomous Collaborative Platform Tranche 2." 29 July 2025. https://www.find-tender.service.gov.uk/Notice/044033-2025.
Department for Science, Innovation and Technology. 2025. "Artificial Intelligence Sector Study 2024." 3 September 2025. https://www.gov.uk/government/publications/artificial-intelligence-sector-study-2024/artificial-intelligence-sector-study-2024.
De Silva, D., and D. Alahakoon. 2022. "An Artificial Intelligence Life Cycle: From Conception to Production." *Patterns* 3 (6): 1–13. https://doi.org/10.1016/j.patter.2022.100489.
Dienelt, A. 2018. "The Shadowy Existence of the Weapons Review and Its Impact on Disarmament." *Security and Peace* 36 (3): 126–132. https://doi.org/10.5771/0175-274X-2018-3-126.
Droege, C., and E. Giorgou. 2022. "How International Humanitarian Law Develops." *International Review of the Red Cross* 104 (920–921): 1798–1839. https://doi.org/10.1017/S1816383122000893.
Dstl. 2024. "AI Ethics Playing Cards." https://ai.militaryethics.uk/.
Focarelli, C. 2010. "Common Article 1 of the 1949 Geneva Conventions: A Soap Bubble?" *The European Journal of International Law* 21 (1): 125–171. https://doi.org/10.1093/ejil/chq017.
Fontes, R., and J. Kamminga. 2023. "Ukraine: A Living Lab for AI Warfare." National Defense, 24 March 2023. https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare.
Foreign, Commonwealth and Development Office. 2025a. "The Evidence of Russia's Violations of International Humanitarian Law Is Substantial and Growing: UK Statement to the OSCE." 3 October 2024. https://www.gov.uk/government/speeches/the-evidence-of-russias-violations-of-international-humanitarian-law-is-substantial-and-growing-uk-statement-to-the-osce.
Foreign, Commonwealth and Development Office. 2025b. "Joint Statement on Attacks Against Civilians and Humanitarian Workers in Sudan." 6 June 2025. https://www.gov.uk/government/news/joint-statement-on-attacks-against-civilians-and-humanitarian-workers-in-sudan.
Foreign, Commonwealth and Development Office. 2025c. "UK and Partners Unite to Sanction Ministers Inciting West Bank Violence." 10 June 2025. https://www.gov.uk/government/news/uk-and-partners-unite-to-sanction-ministers-inciting-west-bank-violence.
Geiß, R. 2015. "The Obligation to Respect and to Ensure Respect for the Conventions." In *The 1949 Geneva Conventions: A Commentary*, edited by Clapham, Andrew, Paola Gaeta, and Marco Sassòli, 111–134. Oxford: Oxford University Press.
Gillard, E.-C. 2006. "The Position with Regard to International Humanitarian Law." *Proceedings of the American Society of International Law* 100, 130–135.
González, R. J. 2024. *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*. Providence, RI: The Watson School of International and Public Affairs. 17 April 2024.
Google Cloud. 2025. "Google Cloud Awarded Landmark Sovereign Cloud Contract with UK Ministry of Defence." 11 September 2025. https://www.googlecloudpresscorner.com/2025-09-11-Google-Cloud-Awarded-Landmark-Sovereign-Cloud-Contract-with-UK-Ministry-of-Defence.

Goussac, N., and V. Boulanin. 2026. *Responsible Procurement of Military Artificial Intelligence*. Stockholm: Stockholm International Peace Research Institute.
Grand View Research. 2025. *Artificial Intelligence in Military Market (2025–2030)*. https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-military-market-report .
Heim, E., and C. Frank. 2025. "Out of Distribution Detection: Knowing When AI Doesn't Know." *Carnegie Mellon's Software Engineering Institute*. 9 June 2025. https://doi.org/10.58012/5e1y-zq76.
Helsing. 2025. "About Helsing." https://helsing.ai/.
Henckaerts, J.-M., and L. Doswald-Beck, eds. 2005. *Customary International Humanitarian Law, Volume I: Rules*. Cambridge: Cambridge University Press.
Henderson, I. 2009. *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack Under Additional Protocol I*. Leiden: Martinus Nijhoff.
Henderson, I., and K. Reece. 2021. "Proportionality Under International Humanitarian Law: The "Reasonable Military Commander" Standard and Reverberating Effects." *Vanderbilt Law Review* 51 (3): 835–855.
Hinton, P. 2023. *Adversarial AI: Coming of Age or Overhyped?* London: Centre for Emerging Technology and Security.
House of Commons Defence Committee. 2025a. Government Response to Developing AI Capacity and Expertise in UK Defence. *Third Special Report of Session 2024–25, HC 812s*. London. 4 April 2025.
House of Commons Defence Committee. 2025b. Developing AI Capacity and Expertise in UK Defence. *Second Report of Session 2024–25, HC 590*. London. 10 January 2025.
House of Commons International Development Committee. 2025. Protection Not Permission: The UK's Role in Upholding International Humanitarian Law and Supporting the Safe Delivery of Humanitarian Aid. *Fifth Report of Session 2024–25, HC 526*. 12 June 2025.
House of Lords Select Committee on AI in Weapon Systems. 2024. "The Government Response to the Report by the House of Lords AI in Weapon Systems Committee: 'Proceed with Caution." Artificial Intelligence in Weapon Systems', London. 19 February 2024. Session 2023–24 HL Paper 16, CP 1023.
Hughes, D. 2020. "Differentiating the Corporation: Accountability and International Humanitarian Law." *Michigan Journal of International Law* 42 (1): 47–104.
International Committee of the Red Cross. 2006. *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*. Geneva.
International Committee of the Red Cross. 2008. *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. Geneva.
International Committee of the Red Cross. 2016. *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. Cambridge: Cambridge University Press.
International Committee of the Red Cross. 2025. *Autonomous Weapon Systems and International Humanitarian Law: Selected Issues*. Geneva.
International Committee of the Red Cross and Switzerland. 2008. "The Montreux Document: On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict." Geneva. 17 September 2008.
International Criminal Tribunal for the Former Yugoslavia. 2000. *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*. The Hague. 8 June 2000.
Israel Defense Forces. 2024. "The IDF's Use of Data Technologies in Intelligence Processing." 18 June 2024. https://www.idf.il/210062.
Jevglevskaja, N. 2021. *International Law and Weapons Review: Emerging Military Technology Under the Law of Armed Conflict*. Cambridge: Cambridge University Press.
Karp, A. C., and N. W. Zamiska. 2025. *The Technological Republic: Hard Power, Soft Belief and the Future of the West*. London: Bodley Head.

King, A. 2025. *AI, Automation, and War: The Rise of a Military-Tech Complex*. Princeton: Princeton University Press.
Klare, M. 2026. "AI Plays Major Role in the War on Iran." Arms Control Association. https://www.armscontrol.org/act/2026-05/news/ai-plays-major-role-war-iran .
Knack, A., A. Bowden, N. Karner, L. Fletcher, R. Barrett-Taylor, O. Wickens, M. Welsh, and T. Whittaker. 2025. *Defence AI Assurance: Identifying Promising Practice and a System Card Template for Defence*. London: The Alan Turing Institute.
Korteling, J. E., G. C. van de Boer-Visschedijk, R. A. M. Blankendaal, R. C. Boonekamp, and A. R. Eikelboom. 2021. "Human- Versus Artificial Intelligence." *Frontiers in Artificial Intelligence* 4 (622364): 1–13. https://doi.org/10.3389/frai.2021.622364.
Liivoja, R. 2015. "Technological Change and the Evolution of the Law of War." *International Review of the Red Cross* 97 (900): 1157–1177. https://doi.org/10.1017/S1816383116000424.
Lonsdale, J. 2023. "Our Duties as Defense Technologists." 2 November 2023. https://blog.joelonsdale.com/p/our-duties-as-defense-technologists.
Lubin, A. 2025. "AI Broke the Code – the International Code of Conduct for Private Security Service Providers and Emerging Technologies." Opinio Juris. 16 July 2025. https://opiniojuris.org/2025/07/16/symposium-on-pmscs-ai-broke-the-code-the-international-code-of-conduct-for-private-security-service-providers-and-emerging-technologies/.
Luckey, P. 2025. "The AI Arsenal That Could Stop World War III." TED. 24 April 2025. https://www.ted.com/talks/palmer_luckey_the_ai_arsenal_that_could_stop_world_war_iii/transcript .
Mačák, K. 2016. "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors." *Journal of Conflict and Security Law* 21 (3): 405–428. https://doi.org/10.1093/jcsl/krw014.
Nasu, H. 2020. "Artificial Intelligence and the Obligation to Respect and to Ensure Respect for IHL." In *Ensuring Respect for International Humanitarian Law*, edited by Massingham, Eve, and Annabel McConnachie, 132–144. London: Routledge.
National Audit Office. 2015. "Reforming Defence Acquisition." London. 23 February 2015.
National Security Commission on Artificial Intelligence. 2021. *Final Report*. Washington, DC.
New Zealand Defence Force. 2022. *Manual of Armed Forces Law: Law of Armed Conflict*. 2nd ed. Vol. 4. Wellington.
Nicol-Schwarz, K., and A. Sraders. 2025. "Why Defence Tech Startups Are Setting Up Shop in Britain." Sifted. 29 July 2025. https://sifted.eu/articles/europe-defence-tech-h1-2025 .
Norwegian Ministry of Defence. 2013. *Manual of the Law of Armed Conflict*. Oslo: Norwegian Chief of Defence.
Onderco, M. 2025. "Navigating the AI Frontier: Insights from the Ukraine Conflict for NATO's Governance Role in Military AI." *Journal of Strategic Studies* 48 (3): 602–626. https://doi.org/10.1080/01402390.2025.2463451.
Organisation for Economic Co-operation and Development. 2023. *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*. Paris.
Palantir. 2024. "Safeguarding Freedom: How Defense Efforts Align with Human Rights." Palantir Blog. 13 November 2024. https://blog.palantir.com/safeguarding-freedom-87080c30a712 .
Palantir. 2025. "About Palantir: Answers to Frequently Asked Questions about Palantir." 21 August 2025. https://blog.palantir.com/about-palantir-ddddb78aec29.
Quintin, A. 2020. *The Nature of International Humanitarian Law: A Permissive or Restrictive Regime?* Cheltenham: Edward Elgar.
Rashid, A. B., A. Karim Kausik, A. Al Hassan Sunny, and M. Hassan Bappy. 2023. "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges." *International Journal of Intelligent Systems* 2023 (1): 1–31. https://doi.org/10.1155/2023/8676366.
Research and Markets. 2025. *Artificial Intelligence (AI) in Military: Global Strategic Business Report*. https://www.researchandmarkets.com/report/military-artificial-intelligence.
Robson, V. 2020. "The Common Approach to Article 1: The Scope of Each State's Obligation to Ensure Respect for the Geneva Conventions." *Journal of Conflict and Security Law* 25 (1): 101–115. https://doi.org/10.1093/jcsl/kraa004.

Sandoz, Y., C. Swinarski, and B. Zimmermann, eds. 1987. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Leiden: Martin Nijhoff.
Scharre, P. 2019. *Military Applications of Artificial Intelligence: Potential Risks to International Peace and Security*. Washington, DC: Center for a New American Security.
Schmidt, E. 2023. "Innovation Power: Why Technology Will Define the Future of Geopolitics Essays." *Foreign Affairs* 102:38–52.
Schmitt, M. N., and M. Schauss. 2019. "Uncertainty in the Law of Targeting: Towards a Cognitive Framework." *Harvard National Security Journal* 10:148–194.
Schmitt, M. N., and S. Watts. 2020. "Common Article 1 and the Duty to "Ensure Respect"." *International Law Studies* 96:674–706.
Schwarz, E. 2025. "From Blitzkrieg to Blitzscaling: Assessing the Impact of Venture Capital Dynamics on Military Norms." *Finance and Society* 11:1–24. https://doi.org/10.1017/fas.2024.18.
Special Competitive Studies Project. 2024. *Vision for Competitiveness: Mid-Decade Opportunities for Strategic Victory*. Washington, D.C.
Statman, D., R. Sulitzeanu-Kenan, M. Mandel, M. Skerker, and S. de Wijze. 2020. "Unreliable Protection: An Experimental Study of Experts' in Bello Proportionality Decisions." *The European Journal of International Law* 31 (2): 429–453. https://doi.org/10.1093/ejil/chaa039.
Stavrianakis, A. 2023. "Debunking the Myth of the "Robust Control Regime": UK Arms Export Controls During War and Armed Conflict." *Global Policy* 14 (1): 121–130. https://doi.org/10.1111/1758-5899.13191.
Swedish Prosecution Authority. 2021. "Prosecution for Complicity in Grave War Crimes in Sudan." 11 November 2021. https://www.aklagare.se/en/for-the-media/press-releases/2021/november/prosecution-for-complicity-in-grave-war-crimes-in-sudan/.
Switzerland. 2010. "International Code of Conduct for Private Security Service Providers."
Taylor, T. 2019. "Defence Procurement: Overcoming Challenges and Managing Expectations." In *The Political Economy of Defence*, edited by Matthews, Ron, 258–283. Cambridge: Cambridge University Press.
UK Government. 2016. *Good Business: Implementing the UN Guiding Principles on Business and Human Rights*. Cm 9255. London.
UK Government. 2024. *UK Voluntary Report on the Implementation of International Humanitarian Law at Domestic Level*. 2nd ed. London.
UK Ministry of Defence. 2004. *The Joint Service Manual of the Law of Armed Conflict (JSP 383)*. Oxford: Oxford University Press.
UK Ministry of Defence. 2016. "UK Weapons Reviews." 8 March 2016.
UK Ministry of Defence. 2021. *Defence in a Competitive Age*. London.
UK Ministry of Defence. 2022a. *Defence Artificial Intelligence Strategy*. London.
UK Ministry of Defence. 2022b. *Ambitious, Safe, Responsible: Our Approach to the Delivery of AI-Enabled Capability in Defence*. London.
UK Ministry of Defence. 2022c. *UK Defence Doctrine (JDP 3-46)*. London.
UK Ministry of Defence. 2025a. "Launching the AI Model Arena." 10 November 2025. https://www.gov.uk/government/news/launching-the-ai-model-arena.
UK Ministry of Defence. 2025b. "NATO DIANA UK Accelerator: Welcome to the UK Accelerator." https://www.gov.uk//government/organisations/defence-and-security-accelerator.
UK Ministry of Defence. 2025c. *Dependable Artificial Intelligence (AI) in Defence Part 1: Directive (JSP 936)*. London.
UK Ministry of Defence. 2025d. "New Strategic Partnership to Unlock Billions and Boost Military AI and Innovation." 18 September 2025. https://www.gov.uk/government/news/new-strategic-partnership-to-unlock-billions-and-boost-military-ai-and-innovation.
UK Ministry of Defence. 2025e. "Defence and Security Accelerator." https://www.gov.uk/government/organisations/defence-and-security-accelerator .
UK Ministry of Defence. 2025f. *Laying the Groundwork: Responsible AI Senior Officers' Report* October 2025. London.

UK Ministry of Defence. 2025g. "Major £5 Billion Technology Investment Accelerates UK Defence Innovation in a European First." 2 June 2025. https://www.gov.uk/government/news/major-5-billion-technology-investment-accelerates-uk-defence-innovation-in-a-european-first .
UK Ministry of Defence. 2025h. *Strategic Defence Review–Making Britain Safer: Secure at Home, Strong Abroad*. London.
United Nations. 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*. New York and Geneva.
U.S. Department of Defense. 2023. *Law of War Manual*. updated ed. Washington, DC: Office of General Counsel.
van den Boogaard, J. 2023. *Proportionality in International Humanitarian Law: Refocusing the Balance in Practice*. Cambridge: Cambridge University Press.