

House Foreign Affairs Committee
Tom Lantos Human Rights Commission

Hearing:
Artificial Intelligence in the Military Domain: Implications for Human Rights

Date:
Wed, 07/01/2026 - 2:00 PM

Oral Statement of Amanda Klasing, National Director of GR & Advocacy
Amnesty International USA

I want to start by thanking Co-Chairs McGovern and Smith for calling this hearing today, and to also thank them for first putting this important issue on the Lantos Commission docket in 2018. It demonstrates their commitment and leadership to ensuring human rights concerns are at the heart of a government response to artificial intelligence. As the use of artificial intelligence by militaries around the world proliferates, it is important to center not only the immense humanitarian law (IHL) implications of these tools, but also the human rights considerations. In my remarks, I will focus on the human rights concerns inherent to the design and development of the generative AI tools used to support militaries with target generation and prioritization, so that we better understand how these concerns are carried into deployment of these systems in a manner that may exacerbate risks of violating international humanitarian law in conflict. However, I will be very happy to discuss the IHL concerns in follow up questions, including the impact of a compressed kill chain supported by these technologies, rubber-stamping killing at speed and scale that poses a fundamental challenge to international law.

Current generative AI systems are not just risky when deployed by militaries—they are often structurally incompatible with human rights by design.

By their nature these systems are problematic—these are machine learning tools that have been trained on massive datasets, often without the knowledge and consent of those from whom the data originates, and usually it is through unlawful web scraping. These technologies rely on practices that abuse privacy rights, enable discrimination, and threaten freedom of expression and thought. Further, most current generative AI systems are highly susceptible to unpredictability, inaccuracy and risk to human rights. Finally, there are significant accountability gaps that prevent remedy, while monopolies drive additional challenges for constraint.

Indiscriminate mass surveillance, including with AI-driven tools, is never a proportionate interference with the right to privacy. Web scraping to train some generative AI tools

constitute rely on mass invasions of privacy by design, as vast amounts of personal, behavioral, and creative data are continuously collected and processed—violating principles of consent, necessity and proportionality and risking violations of privacy laws and the rights enshrined within them.

Generative AI reproduces and amplifies systemic biases, such as racial, gender, cultural among others, present in training data, threatening people's rights to equality and non-discrimination. Outputs often misrepresent or marginalize groups, reinforce stereotypes, and disproportionately harm historically excluded communities. These harms can then be replicated through discriminatory decision-making, to devastating outcomes in the context of conflict or other military uses. For example, in the occupied Palestinian territory (OPT), investigative reports revealed the devastating use of AI for target acquisition (detecting and identifying targets for military operations) in the context of the genocide in Gaza, through the Gospel system and later Lavender and Where's Daddy.

GenAI also impacts critical human discernment. Scholars have long warned that a reliance on such technology for decision-making could lead to atrophy in our capabilities for moral reasoning. I look forward to hearing from other witnesses today about these ethical and moral concerns. AI technology, including LLMs, deployed in more high-risk environments, such as in the military kill chain, risk sanitizing discrimination, humanitarian law breaches, and even international crimes behind a veneer of sophisticated automation.

And, when something goes wrong, accountability gaps exacerbate human rights harms. Lack of accountability does not have to be inherent to AI technology, but can easily occur when operators choose to devolve responsibility to design errors. There currently is opacity and lack of transparency about training data, model design, and decision-making processes, with companies and government users often withholding information about what data is used and how it is processed. Affected communities are left unable to meaningfully understand or challenge AI outputs, including errors or harms. A veneer of technicality heightens the opacity around who is responsible for harms. When systems are not transparent, simply keeping a human in the loop does not mean victims can get justice.

For example, question marks have been raised about where liability lies if there is a deadly error in target generation; at what point does it implicate the data scraping from the public, data labeling, cloud infrastructure and/or hardware production? These layers enable actors across the supply chain, including operators, to attempt to fragment responsibility, with companies often distancing themselves from harms, with militaries increasingly doing the same. International law, however, is clear: those who choose to

deploy AI systems that are used to commit international crimes—in spite of the design incompatibilities with international law mentioned above—must be held criminally responsible.

Amidst the attempts at offloading responsibility, victims are left with little practical ability to seek justice or compensation for harms that are made difficult to trace or prove. This is compounded by companies who are failing to conduct human rights due diligence across the AI lifecycle. Together, these concerns create a system where serious human rights harms occur without transparency, oversight, and accountability—often before the tools have even been deployed in the military realm, or at its most extreme, in conflict.

By the time AI technology is operationalized in military contexts for decision-making and target acquisition, human rights redlines likely have already been crossed. Companies must, however, continue to exercise leverage where their products and services are used for violations of international law, even once they have entered military contracts. In practice, however, they are falling woefully short.

As a result, we are seeing some companies changing their posturing on military usage of AI in the face of public fall out, but this often comes too late. And, companies are not the only drivers of military use of AI. States including India, Singapore, Taiwan, Denmark and the Netherlands are also increasingly pursuing “sovereign” AI projects through the pursuit of homegrown LLMs. Governments have rushed to invest in and integrate AI (including generative AI, but also other AI technologies) into a wide range of government processes and services, in and outside of the military domain.

Even if States want to put safeguards in place, the sheer size of some big tech companies makes this difficult. These companies wield extraordinary influence over the infrastructure, services, and norms that shape our online lives, with largely unchecked power across various digital sectors. These companies are moving to consolidate their power further in artificial intelligence, and their anti-competitive behaviors may make it difficult to take steps to prevent human rights harms, regulatory capture, and harmful monopolies from forming.

I would be remiss not to mention that creating and operating the vast physical infrastructure necessary to achieve industry and investor goals on AI, including the building of data centers, has led to increasing exploitation of natural resources, environmental degradation and the erosion of labor rights.

Ultimately, if we want to ensure military use of artificial intelligence is consistent with international law, we have to start at the beginning of the AI lifecycle, before a system is even deployed and continue through the entire course its lifecycle and use.

Governments should enact binding, enforceable and human rights-based regulations to govern AI systems, including a ban on the development and deployment of AI systems that are incompatible with international human rights and humanitarian law, particularly in the high-risk military realm.

With the leadership support of the Lantos Commission, Congress should immediately regulate AI systems designed and deployed for military use to ensure compatibility with human rights standards and international humanitarian law, including providing a clear means to pursue effective remedy and a requirement of transparency on how AI is currently being used in the conduct of hostilities. Congress should demand the administration work through multilateral institutions for global regulation of these tools. Until then, Congress should demand a halt to the use of AI tools, including large language models, in the conduct of military targeting.

As our conversation continues today, I will be very happy to talk about the human rights and humanitarian law concerns we see with deployment in conflict.

Thank you. I look forward to your questions.