The Israeli Military's Use of AI in Gaza: Operational Efficiency at the Cost of Humanity

Noah Sylvia
Research analyst for C4ISR and Emerging Tech
The Royal United Services Institute for Defence and Security Studies (RUSI), London

Recent reporting from *+972 Mag* revealed the development of a ChatGPT-like capability for the Israeli Defense Force (IDF) to surveil Palestinians. This Large Language Model (LLM), created by the secretive Unit 8200, is understood to be trained on the Arabic conversations of Palestinians that were obtained through IDF surveillance. The model can then be asked questions about specific individuals, permitting analysts to interrogate surveillance data with greater ease.
However dystopian this may sound, it is not the first, nor the most dangerous, use of AI by the IDF. Indeed, much attention has been directed at the IDF's use of AI systems to assist in its targeting operations during its war on Gaza. This article explores this topic in greater depth, describing what can be currently understood about the IDF's use of AI systems, the global system enabling it and what lessons can be gleaned from this case study.

Reporting of IDF AI Use

AI has been in use for several years by advanced militaries – including the IDF – for both combat and support functions. Notably, 2021 operations against the Gaza Strip marked the combat debut of their "Fire Factory" system, which analysed droves of data to enable rapid operational planning for airstrikes.
In December 2023 and April 2024, investigative reporting revealed the use of the "Gospel" and "Lavender" systems, respectively. The reports indicated that these models are used to assist in intelligence fusion functions that are used to create target profiles, with "Gospel" used for fixed targets such as buildings, while "Lavender" aided in the creation of human target profiles. These target profiles are then analysed and potentially struck, mainly through air operations.
A number of concerns have been raised, including flawed data, model biases, a high tolerance for model error, a low threshold for target identification and targeting, a low level of meaningful human involvement, a high tolerance for civilian casualties, and a lack of post-operation assessments to improve usage.

AI in Military Targeting

While discussions on the military use of AI conjure up images of killer robots, most AI use cases are far less sensational, from predictive maintenance to signal analysis tools. The AI systems employed by the IDF to aid in targeting fall under the category of "Decision-support systems" (DSS) – technologies which assist commanders and analysts in their decision-making processes. AI DSS in the targeting process may be used for gathering and cleaning raw data from sensors, searching for actionable intelligence, generating target details and/or for operational planning of strikes.
The use of AI in the targeting process is not inherently inhumane, but it does have greater risks given that it is directly used in processes that enable killing. Yet these risks depend entirely on how models are trained, tested and employed. Biases, errors and hallucinations must be minimized through rigorous testing, while commanders and analysts must understand the benefits, risks and limitations of these complex technologies. Most militaries also require a level of "meaningful human control" over the actions of systems in operations, meaning that there are hu-

mans who understand how the system operates, can exert a level of control over the actions of the system and are accountable for the system's actions. Even once successfully deployed, models must be continuously reassessed, not only to further ensure model accuracy, but also to prevent model drift over time.

Most militaries also require a level of "meaningful human control" over the actions of systems in operations

Theoretically, if models are responsibly developed, trained, tested and employed, AI could be used to enhance precision, accuracy and discrimination in targeting operations. Using AI technologies to process greater quantities of data than humanly possible, analysts could have far more rigorous depictions of potential targets, permitting much higher accuracy in decision-making. Yet, as seen below, the operating procedures of the military in question ultimately determine the impact of any AI systems being employed. For example, the threshold for positive identification of a target shapes the discrimination of a campaign: assuming high-fidelity systems, a high threshold for identification would reduce the risk of civilian deaths due to target misidentification, while a low threshold could result in an effectively indiscriminate campaign against a population.

The IDF's (Ir)responsible Use of AI

The IDF has yet to permit access to its systems, so the nature of their functionality and capabilities cannot be determined with specificity. However, given the information available, it is clear that the IDF is not using AI to refine their targeting, but instead to expand and expediate its targeting cycle (Sylvia, 2024). The IDF has claimed that the use of AI systems like Gospel and Lavender is as mere intelligence management tools for aiding analysts in their functions, rather than creating targets autonomously. Yet media reports have cast doubt upon the likelihood of a careful, human-centred process, instead describing human control as a perfunctory check lasting under a minute, with little indication that analysts truly understand the capabilities and limitations of models. Furthermore, the sheer number of targets struck by the IDF – especially in the initial weeks of the war – lends weight to the argument that humans are not meaningfully in control of all stages of the targeting cycle.
Yet human considerations are crucial to understanding these systems, as any AI systems in use would exhibit the biases inherent in the IDF itself. At every stage in their lifecycle, from model creation, to training, to testing, models incorporate the biases of those humans shaping the system's functions. Not only do biases affect the accuracy of the system, but they can also exacerbate existing practices within operations. For example, the decades of Palestinian dehumanization by both the IDF and Israeli society increases the collateral damage considered acceptable in their normal operational planning, leading to higher cost in civilian lives and infrastructure. Simply through being embedded with the IDF, AI systems would undoubtedly incorporate a measure of these biases and therefore contribute to inflicting disproportionate and often indiscriminate harm onto the Palestinian population.
Ideally, models would be continually assessed once in operation to continue mitigating such biases that survived the testing stage. A responsible military would perform post-operation assessments to determine operation success as well as how to improve future civilian harm mitigation. These "post-mortems" produce insights into the functionality of any AI systems in use, allowing a feedback loop to continually improve the models. However, the IDF does not appear to be attempting to learn lessons from its strikes. Not only did reporting attest to the IDF tolerating a high error rate in Lavender (~10%), but the IDF does not appear to recognize the continued large-scale killing of innocents as errors requiring correction. Any changes to IDF procedures occur as a result of rare backlash from the dwindling list of Israeli allies rather than a desire to safeguard Palestinian lives.

Enabling Israeli AI

While the AI models used by the IDF – like Lavender and Gospel – have drawn widespread scrutiny,

The IDF does not appear to recognize the continued large-scale killing of innocents as errors requiring correction

the systems themselves are only part of the picture. Behind them lies a vast, often opaque infrastructure provided by some of the most powerful tech firms in the world. AI systems require massive compute resources, storage capacity and engineering support – capabilities that the IDF has not developed independently.

Major US tech firms such as Microsoft, Amazon Web Services (AWS), Google and Palantir have all contributed directly or indirectly to the IDF's AI capabilities. Despite facing internal protests and human rights campaigns against their continued relationships with the IDF, there has been no indication that they will be dissuaded from taking these lucrative contracts. Palantir has publicly highlighted its relationship with the IDF in supporting a number of surveillance and targeting functions, while investigations earlier this year revealed that Microsoft expanded its support for the IDF in the aftermath of October 2023. The latter's services are provided across the military and include engineering support, cloud storage and compute, as well as broad access to GPT-4. Google similarly deepened its provision of AI-enabled data analytics to the IDF, although the exact usage of these tools is yet to be reported.

Lessons to Draw

The IDF's operations in Gaza reveal a troubling convergence: advanced technological capability coupled with ethically reprehensible military conduct. This fusion has enabled the disproportionate application of force against a civilian population. The lessons are clear – responsible military AI requires more than technical proficiency; it demands a commitment to wartime legal standards and basic humanity that the IDF, and its supporters, have thus far refused to uphold.

This case study should serve as a stark warning to the international community about the risks brought forth by the irresponsible use of AI technologies in warfare. The first step to avoiding such a future is to provide greater transparency about the models in use, from development and training to deployment and use. Militaries must ensure technological literacy in operators and analysts, limiting automation bias and ensuring that systems are not seen as "black boxes." Crucially, commanders and analysts need to maintain accountability mechanisms during automated stages of the targeting cycle, guaranteeing that a human is always held responsible for machine decision-making. Most critically, compliance with international humanitarian law must remain absolute. No machine, no matter how sophisticated, absolves humans of responsibility. And when those in command act with disregard for these obligations – as we have seen – the use of AI only deepens the injustice.

Major US tech firms such as Microsoft, Amazon Web Services (AWS), Google and Palantir have all contributed directly or indirectly to the IDF's AI capabilities

International dialogue around AI and warfare must involve greater enforceable international accountability mechanisms – whether through existing bodies like the UN or new multilateral frameworks –, otherwise rogue actors will continue to exploit AI with impunity. Without meaningful accountability, technological advancement will not make war more humane; it will simply make atrocity more efficient.

Bibliography

Abraham, Yuval. "'Order from Amazon': How Tech Giants Are Storing Mass Data for Israel's War." *+972 Magazine*, 4 August 2024. www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/.

Abraham, Yuval. "Leaked documents expose deep ties between Israeli army and Microsoft." *+972 Magazine*, 23 January 2025. www.972mag.com/microsoft-azure-openai-israeli-army-cloud/.

Abraham, Yuval. "Israel Developing ChatGPT-like Tool that Weaponizes Surveillance of Palestinians." *+972 Magazine*, 6 March 2025. www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/.

Bo, Marta and Dorsey, Jessica. "Symposium on Military AI and the Law of Armed Conflict: The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians." *Opinio Juris*, 4 April 2024. https://opiniojuris.org/2024/04/04/symposium-on-military-ai-and-the-law-of-armed-conflict-the-need-for-speed-the-cost-of-unregulated-ai-decision-support-systems-to-civilians/.

Buttu, Diana. "Blaming the Victims." *Journal of Palestine Studies*, 44(1), 91-96, 2014. www.tandfonline.com/doi/abs/10.1525/jps.2014.44.1.91.

Davies, Harry and Abraham, Yuval. "Revealed: Microsoft deepened ties with Israeli military to provide tech support during Gaza war." *The Guardian*, 23 January 2025. www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft.

De Vynck, Gerrit. "Google Provided AI Tools to Israeli Military in Early Weeks of Gaza War." *The Washington Post*, 21 January 2025. www.washingtonpost.com/technology/2025/01/21/google-ai-israel-war-hamas-attack-gaza/.

Elliott, Christopher. "Expedient or Reckless? Reconciling Opposing Accounts of the IDF's Use of AI in Gaza." *Opinio Juris*, 26 April 2024. https://opiniojuris.org/2024/04/26/expedient-or-reckless-reconciling-opposing-accounts-of-the-idfs-use-of-ai-in-gaza/.

Frantzman, Seth J. "Israeli Air Force struck 31,000 targets in four months of war." *Breaking Defence*, 20 February 2024. https://breakingdefense.com/2024/02/israeli-air-force-struck-31000-targets-in-four-months-of-war/.

Frenkel, Sheera. "Israel Deploys Expansive Facial Recognition Program in Gaza." The *New York Times*, 27 March 2024. www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html.

Grim, Ryan and Ahmed, Waqas. "The Israeli Military Is One of Microsoft's Top AI Customers, Leaked Documents Reveal." *Dropsite News*, 23 January 2025. www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud.

Human Rights Watch. "Questions and Answers: Israeli Military's Use of Digital Tools in Gaza." *Human Rights Watch*, 10 September 2024. www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza.

Israel Defense Forces. "April 3, 2024 IDF Response as Sent to the Guardian." *IDF Official Website*, 3 April 2024. www.idf.il/189654.

Mullane, Hannah and Josephs, Jonathan. "Google Sacks Staff Protesting Over Israeli Contract." *BBC News*, 18 April 2024. www.bbc.co.uk/news/articles/c3gqw1d37l4o.

Renic, Neil and Schwarz, Elke. "Inhuman-in-the-loop: AI-targeting and the Erosion of Moral Restraint." *Opinio Juris*, 19 December 2023. https://opiniojuris.org/2023/12/19/inhuman-in-the-loop-ai-targeting-and-the-erosion-of-moral-restraint/.

Schmitt, Michael N. and Merriam, John J. "The Tyranny of Context: Israeli Targeting Practices in Legal Perspective." *University of Pennsylvania Journal of International Law* vol. 37:1, 53-139, 2015. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1905&context=jil.

Sylvia, Noah. "The Israel Defense Forces' Use of AI in Gaza: A Case of Misplaced Purpose." *RUSI Commentary*. Royal United Services Institute, 4 July 2024. www.rusi.org/explore-our-research/publications/commentary/israel-defense-forces-use-ai-gaza-case-misplaced-purpose.