From Ukraine to Gaza: Artificial intelligence in war

Amélie Ferey, Laure de Roucy-Rochegonde

In Politique étrangère 2024/3 No 243 , pages 39 to 50
Publisher Institut français des relations internationales

ISSN 0032-342X
DOI 10.3917/pe.243.0039
Uploaded: 09/27/2024

From Ukraine to Gaza: Artificial intelligence in war

By **Amélie Férey** and **Laure de Roucy-Rochegonde**

Amélie Férey leads the Laboratoire de recherche sur la défense (LRD) (Defense Research Unit) at the Institut français des relations internationales (Ifri) (French Institute of International Relations). **Laure de Roucy-Rochegonde** is head of the Centre Géopolitique des technologies (Center for Geopolitics of Technology) at Ifri.

The use of artificial intelligence (AI) on the battlefield has been highly pervasive in the wars in Ukraine and Gaza. This technology has numerous uses, from the analysis of intelligence to targeting, as well as logistics and communication. The tempo of operations is accelerating at such a rate that the time that humans have to make decisions about whether or not to open fire is dwindling to just a few seconds. To stop this escalating spiral, the military applications of AI must be regulated.

Politique étrangère

In an article that appeared in *Defense One* in Spring 2024,[1] the American strategist Peter Singer compared current conflicts with the Spanish Civil War. In 1936, he explained, the two camps used rifles and dug trenches. However, at the same time, tanks, radios, and airplanes began to appear in the conflict. The use of preexisting methods did not therefore preclude a major shift from emerging at the same time. In reality, he concluded, the ongoing wars in Ukraine and Gaza, as testing grounds for future conflicts, tell us more about the *next* war, just as the Spanish Civil War foreshadowed the nature of the Second World War. Among the technological developments observed in these two theaters of war, the large-scale use of artificial intelligence (AI) is probably the one that has elicited the most surprise and raised the most questions.

First used in 1965 in the work of logician John McCarthy, the expression “artificial intelligence” covers all theories and techniques seeking to better understand human intelligence, and to imitate it using computer programs that simulate its function. In a more generic sense, AI refers to the capacity of systems to accomplish tasks that would normally require human reason.

---

1. Peter Singer, “The AI Revolution is Already Here: The U.S. Military Must Grapple with Real Dilemmas That Until Recently Seemed Hypothetical,” *Defense One*, April 14, 2024, https://www.defenseone.com/ideas/2024/04/defense-one-radio-ep-149-state-army/395693/.

This technology is constantly insinuating itself further into our personal and professional lives, especially since the commercial success of the ChatGPT chatbot developed by OpenAI and the boom in generative AIs, i.e., those that can create new content based on preexisting data sets. On the battlefield as elsewhere, the promises of AI are whetting appetites and innovations are multiplying, but not without raising a multitude of strategic, political, legal, and ethical questions.

The military applications of AI are numerous and versatile. From logistics to targeting as well as intelligence and assistance with decision-making within command-and-control structures, AI permeates contemporary military systems. Some even view it as a new revolution in military technology of the same magnitude as gunpowder and nuclear weapons before it.

Over the last decade, the major powers have understood the potential of military AI and exponential progress has therefore been made. Its benefits have already been widely demonstrated and take many different forms: Some of the places AI has been integrated include loitering munitions, aerial, terrestrial, and maritime drones, sentry guns, and anti-drone and anti-aircraft systems. Beyond the specter of "killer robots," it is thus important to reflect on the consequences of the weaponization of AI: Could it transform the nature of war?

AI has been identified as a "force multiplier" by the US Department of Defense for over a decade. Although military AI already has a long history and has been evolving conceptually for some time, analyzing the deployment of AI by the Ukrainian and Israeli armies shows how game-changing this technology is proving in theaters of operations. While the Israel Defense Forces (IDF) have been investing for years in the development of military AI and now use it to cement their technological superiority over Hamas fighters, in Ukraine it is being used by the weak against the strong, by integrating technological building blocks in real time that are essential to the fight against the Russian behemoth. However, these new uses come with increasing reductions in human oversight.

The promise of militarized AI

According to the American strategist Andrew Marshall, a "revolution in military affairs" consists of a radical upheaval in the art of war and the conduct of operations due to the introduction of new technologies. AI and its applications fit this description.

The augmentation of the number of sensors, i.e., all equipment that collects information—from the optronic balls on aerial drones to civilian smartphones—, means a plethora of sources of localized information, not

only on the battlefield but also across the territory of any given country, whether friendly, enemy, or neutral. They collect a colossal amount of heterogeneous data, which AI can compile and analyze. Officers can take advantage of this in order to take more informed decisions on the battlefield, the latter also becoming more "transparent."

AI is essential in light of the accelerating speed of operations

AI can also label the data collected by attaching it to a target; using radar or electromagnetic signatures, or by image recognition or the identifications of "patterns of life," i.e., recurrent behaviors that help to identify individual enemies. The decision to open fire can thus be taken more quickly by speeding up the observe, orient, decide, and act (OODA) loop, as the sensors that detect a target are directly linked to officers via increased connectivity and the networking of different equipment and command centers. Thus, the integration of AI in weapons systems allow it to engage with operational situations that combine a fast pace, a complex environment, and a large number of goals. AI thus becomes essential in light of the accelerating speed of operations, which seems likely only to increase, according to the predictions of General John Allen in 2017 on hyperwar.[2]

The integration of AI techniques into weapons systems gives rise to the possibility of swarms of robots. These operate using remote, distributed, and miniaturized computing, allowing vectors—primarily drones—to communicate at high speed over small distances among themselves, while maintaining low-speed communication with their operator, who can be a significant distance away. AI enables the emergence of autonomous functioning by reducing the dependence on the operator on the ground, who leaves the swarm to decide the best mode of action itself.

As an example, during Operation Guardian of the Walls in Gaza in spring 2021, the Israeli army used a swarm of small multicopter drones to locate, identify, and target members of Hamas. Although this seems to have been the first use of a swarm of drones in combat, the trial proved so effective that the IDF immediately announced its intention to use it in other units. A support company in its parachute brigade was thus given a drone swarm unit. Their commander confirmed that it had carried out more than thirty successful missions, including against targets several kilometers away from the border between Gaza and Israel.[3]

From a military perspective, such capacities are highly advantageous in confronting adversaries and forcing them to respond to multiple threats at a time. Drone swarms hold a great deal of promise in terms of numbers,

2. John Allen and Amir Husain, "On Hyperwar," *Proceedings* 143/7/1,373 (2017).
3. Zak Kallenborn, "Israel's Drone Swarm Over Gaza Should Worry Everyone," *Defense One*, July 7, 2021, https://www.defenseone.com/ideas/2021/07/israels-drone-swarm-over-gaza-should-worry-everyone/183156/.

secrecy, stealth, and saturation. They multiply load capacity while reducing the number of human operators, making them very advantageous from a cost perspective. Moreover, their high levels of autonomy and dynamic allocation of tasks makes them resilient to anti-drone measures.

Ukraine: From weak to strong

The First AI War: such was the billing the American magazine *Time* gave to the Russo-Ukrainian war on the cover of its issue of February 26, 2024. Before the invasion of Ukraine on February 24, 2022, Russia was considered to be one of the most advanced military powers in terms of its weaponization of AI, due to various experiments it had conducted on Ukrainian and Syrian territory. Against all expectations, it has been the Ukrainian army that has been most noteworthy for its use of weapons enhanced by AI.

From the Ukrainian perspective, Russia's size advantage can be counteracted through technological solutions that increase the efficiency of military operations. This equalization strategy explicitly seeks to gain the upper hand through innovation. According to the weekly *Dzerkalo Tyzhnia*, the Ukrainian army uses AI across ten different domains: weapons systems autonomy, observation and reconnaissance, identification and classification of targets, analysis and prediction of threats, logistics and supply, cybersecurity, electronic warfare, simulation and training, troop health, and assistance with decision-making.

This new arsenal has been most noticeable in the role played in the conflict by remotely operated systems. The annexation of Crimea in 2014 previously demonstrated the degree to which drones were vulnerable to jamming techniques. The use of AI can thus compensate for any loss of connection between a weapons system and its operator, and allow the mission to be continued even when the electromagnetic environment is contested. AI vastly expands the capacity of electronic warfare, while also improving the response to the vulnerabilities such warfare entails.

Kyiv compensates for its inferior strength with the mass deployment of drones

Confronted with an adversary with superiority both of arms and of troop numbers, Kyiv compensates for its inferior strength with the mass deployment of drones. What is most interesting about these is that they not only carry out tasks, but also capture data. The data collected by these intelligent drones must therefore be processed, and this is extremely time consuming. For comparison, as early as 2009, the American drones deployed in Afghanistan and Iraq had recorded so many images that the CIA thought that it would take twenty-four years to look at them all. Here

too, AI techniques allow these sometimes heterogeneous data points to be aggregated as a basis for recommendations, notably in terms of targeting.

One of the key roles of AI in Ukraine is in fact to integrate target and object recognition with satellite imagery. The aim is to geolocate and analyze open-source data, such as social network content, in order to identify Russian soldiers, weapons, systems, units, and their movements. Neural networks are used to combine photographs taken at ground level, video footage from drones, and satellite images, thus speeding up the analysis and evaluation of intelligence and in so doing generating strategic and tactical advantages.[4]

Ukrainians have not faced the challenge of weaponizing AI in their war against Russia alone. They have been supported by numerous American technology giants. The CEO of Palantir, Alex Karp, visited Kyiv in June 2022 to offer the company's services to President Volodymyr Zelensky for free.[5] Following in his footsteps, Microsoft, Amazon, Google, and Starlink have flocked to Ukraine, where they have been able to trial their AI systems as applied to intelligence and combat. The Ukrainian army thus uses the Skykit system, developed using Palantir's MetaConstellation software. Acting like a mobile intelligence center, Skykit analyzes satellite images and develops strike plans that can be carried out without contact with the chain of command.

Behind this generosity from American Big Tech sits the companies' own self-interest. First, running to the aid of the Ukrainians has allowed some businesses with controversial methods—such as Palantir and Clearview AI[6]—to launder their public images, previously besmirched by suspicions of mass surveillance. At the same time, they were able to capitalize on a bonanza of operational data, which was exactly what they lacked to make their military applications of AI more robust. By rapidly integrating feedback from the field, they were also able to innovate quickly and improve their models in real time. Finally, these new combat-proven systems are destined for lucrative commercial markets: "Tested in Ukraine" has become a selling point, as evidenced at the Eurosatory arms fair, held on June 17–20, 2024.

---

4. Samuel Bendett, "Roles and Implications of AI in the Russian-Ukrainian Conflict," *Center for a New American Security*, July 20, 2023, https://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict.
5. Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab," *Time*, February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/.
6. Clearview AI is a company specializing in AI-assisted facial recognition that has been criticized for gathering data by scraping billions of publicly available photographs from the internet, violating privacy rights, and selling access to them to police forces. In Ukraine, it has notably allowed Ukrainian forces to identify hundreds of thousands of Russian soldiers. Vera Bergengruen, "Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company," *Time*, November 14, 2023, https://time.com/6334176/ukraine-clearview-ai-russia/.

In Gaza: The strong against the weak

Since 2017, the Israeli army has viewed AI as the "key to modern-day survival." In 2018, it announced that it had developed machines that were "outsmarting humans," and two years later it noted the role of AI as the key to military innovation in its Momentum modernization plan. As early as 2021, it referred to Operation Guardian of the Walls as the "first AI war."

This drive to use AI to acquire military advantage has resulted in the use of a variety of software. The most well-known are Depth of Wisdom, which maps the Gaza Strip in order to spot Hamas tunnels, and Habsora, which identifies buildings that may be being used for military purposes, for example launching rockets, training, or stockpiling weapons.

More recently, the investigative newspaper *+972* described two other pieces of software, Lavender and Where's Daddy?. Lavender measures the probability that a Gazan is part of an armed group by comparing their communication patterns (regularly changing their telephone number, contacts with numbers associated with these groups, etc.) with those of known members of Hamas or Palestinian Islamic Jihad. Where's Daddy?, on the other hand, localizes targeted individuals when they return to their homes, and then alerts officers to their presence in the identified buildings so that the soldiers can open fire, even though civilians may be present.

This use of AI is therefore based on a system of mass surveillance, collecting a significant volume of data in order to train algorithms, aggregating communication data with data from satellites, drones, closed-circuit television cameras, and even social networks.

This gamble on military AI had disastrous consequences during Operation Iron Swords. In the event, the IDF combined at least three sets of errors. First and foremost, it had configured its algorithms badly, using a data set that was not robust: The communication data patterns used to recognize Hamas members—for example the fact that they regularly changed their phones—were also demonstrated by a wider group including human rights activists, journalists, and also people who had been displaced by bombings and collected phones from wherever they could find them in order to contact their families. Another problem was a bias toward "overconfidence" in the rationality of algorithms. Given the mood of the Israeli population in the days that followed October 7, the pressure to hit back fast and hard could not have been greater. Human verification of software recommendations was therefore reduced to a minimum, with officers spending just twenty seconds to verify the validity of a human target suggested by Lavender, despite the error rate ascribed to the system being 10 percent. Some people, for example, were identified as

belonging to Hamas simply because they had the same name as a known militant or were in the same WhatsApp group as one. Ultimately, the use of AI has rationalized a targeting doctrine that is at the very least suspect with regard to international law, in particular the principle of proportionality, by authorizing a large amount of "collateral damage."

Another domain of AI use that needs to be underlined is that Israeli strategic command used new technologies to produce images justifying its military operations, as well as to amplify content that supports its "narrative." The images illustrating the Hamas command post allegedly situated under the al-Shifa hospital, for example, sowed confusion about the boundary between reality and fiction. Another example, the video *Come Visit Beautiful Gaza*, published online by the National Public Diplomacy Directorate, part of the Israeli prime minister's office, depicts what Gaza might have been without Hamas, displacing the responsibility of widespread destruction onto Hamas rather than the Israeli army. AI has also been deployed as part of information operations in order to amplify content that supports Israeli strategic communications on social networks, or to suppress pro-Palestinian messages through scanning content on the profiles of activists.

New threats

The great promise offered by integrating AI into weapons systems comes with new vulnerabilities, however, mainly linked to the erosion of human control over the use of force.

First, the use of AI techniques presents risks relating to the convergence between cyber warfare and electronic warfare. Electronic warfare methods can gain access to enemy information systems that have restricted external connectivity. As AI systems are IT systems like any others, they could be an electromagnetic route through which data could pass to make an attack. Their spread therefore risks increasing the number of vulnerable points, both for the systems themselves and the networks in which they operate.[7] At the same time, AI integration makes systems vulnerable to cyberattacks and information piracy, which could give rise to deception or sabotage operations—for example, poisoning algorithms using altered data. With this type of cyberattack, the enemy could trick a drone, or even take control of it remotely.

The question of "metacognition" also arises, in scenarios where systems continue to learn during missions, in order to adapt to changing

7. Jenny Jun, "How Will AI Change Cyber Operations?," *War on the Rocks*, April 30, 2024, https://warontherocks.com/2024/04/how-will-ai-change-cyber-operations/.

environments. Without effective oversight, what these systems "learn" could give rise to unexpected or undesirable responses that do not correspond with their intended use. More broadly, machine learning systems that are capable of evolving during their operational deployment, prompt not only questions of control over their configuration, but also of whether their trustworthiness can be guaranteed in the long term.

Finally, it is worth highlighting the risks of these technologies proliferating and spreading into the hands of hostile actors. As AI makes possible smaller, cheaper weapons systems that reduce risks to their operators, while also improving their productivity and security, such technology could be especially dangerous if terrorist groups managed to acquire it.

Furthermore, France's defense strategy for artificial intelligence mentions the fact that certain "revisionist" powers, such as Russia or China, believe that the international status quo could be overturned to their advantage thanks to emerging technologies that use military AI. Such technologies, being relatively low-cost and easy to master, reduce power asymmetries. At the same time, other actors could "enter the game" by acquiring technologies that, although complex, are becoming less and less expensive and therefore ever more accessible. This dissemination would thus allow weaker parties to shift the balance between themselves and their adversaries.

What role for humans?

Beyond these technical issues, new fears emerge, linked to what Peter Singer has described as "the end of humans' monopoly on war."[8] On the one hand, the increased tempo of war and the "flood of data" that accompany the weaponization of AI might be to the detriment of human judgment, as such operations tend to become too fast for humans to understand. The operator risks "drowning" in a flow of information, incapable of using their own understanding given the reaction speed of the system.[9] Humans are thus no longer in a position to understand and control the system, nor to fully understand the environment in which it is deployed.

The Israeli experience is informative from this perspective. According to Meron Rapoport, editor-in-chief of the Israeli online magazine *Local Call*—who worked with *+972* on its investigation into the IDF's use of AI—"the human verification step, which ought to ensure that the right person is targeted, has been reduced to the minimum, not more than

8. Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (Penguin Press, 2009), 10.
9. Paul Scharre and Kelley Sayler, *Autonomous Weapons and Human Control* (Center for a New American Security, April 2016), https://www.cnas.org/publications/reports/autonomous-weapons-and-human-control.

twenty seconds in some cases, to such an extent that the soldiers in charge of this verification feel like they simply have to approve the choices made by the machine."[10]

Is it really possible for humans to use their own judgment?

In addition to this problem of speed, there is also a well-known aspect of algorithms, the "black box" effect, i.e., the fact that AI systems sometimes produce results that their programmers cannot explain. Moreover, although the operators know what kind of data the algorithm has used to produce a recommendation—satellite or drone images, phone tapping, electronics intelligence, etc.—they do not know the exact content of this data. Without full understanding of the situation, is it really possible for humans to use their own judgment?

This lack of understanding goes hand in hand with automation bias, which refers to the way operators tend to place too much confidence in machines. Because they cannot grasp the system's reasoning and they assume it makes much more sophisticated calculations than they could themselves, military personnel are for the most part happy to endorse the choices it makes.

Fears about the interaction between humans and machines have existed since the nineteenth century. In 1956, in his *Die Antiquiertheit des Menschen: Über die Seele im Zeitalter der zweiten industriellen Revolution* (The Obsolescence of Man: On the Soul in the Age of the Second Industrial Revolution), the philosopher Günther Anders proposed the concept of the "Promethean gap." Like the Titan of Greek mythology who was condemned to eternal torture after having stolen the sacred flame from Mount Olympus in order to give it to humans, explains Anders, modern humans have expanded the limits of nature through technology. However, in the end it outstrips us: We lose control over it. The Promethean gap denotes the distance between the feats enabled by technology and the limited capacities of humans—in particular in relation to our sense of proportion and our responsibility.

Anders argues that all we can now do is envisage the risks of a particular phenomenon and take meager precautions to avoid them. It is, however, impossible to consider the phenomenon of technology as a whole. Technology thus imposes its own criteria, first among them efficiency, replacing all other values. Due to its complexity, it becomes literally incomprehensible: It "goes beyond understanding."

10. **Translator's note**: Our translation. Unless otherwise stated, all translations of cited foreign language material are our own.

Although the German philosopher developed this concept to think about nuclear weapons, it is strikingly relevant to the questions posed today by the use of AI in conflict. AI techniques make plausible a form of "war without conscience," as part of an ever-increasing phenomenon of detachment.

Controlling intelligent weapons

Both Israel and Ukraine foster discourses that frame their conflicts with their enemies as existential wars. Such fights for survival authorize them to disregard a certain number of ethical quandaries, as demonstrated by the problematic uses of AI observed on contemporary battlefields. It is important to note, however, that current applications set precedents that could open the way to practices that are yet more dangerous and vulnerable to being operationalized by bad actors, whether states or otherwise. It is therefore essential to reflect on the arms control of these new weapons.

The weaponization of AI has already given rise to many ethical and legal concerns. In November 2018, at the first Paris Peace Forum, the Secretary-General of the United Nations, António Guterres, called for states "to ban these weapons, which are politically unacceptable and morally repugnant." There are doubts about the capacity for AI techniques to abide by the law of war as well as about their compatibility with the right to life and the respect of human dignity. Their opponents also fear that they will lower the threshold for entering into conflict and give rise to destructive escalations, and that it will be impossible to assign responsibility for any war crimes that occur.

This is why the question of the oversight that should be exercised over weapons that use AI is now under discussion in multilateral forums. At the international level, the debate on the regulation of autonomous weapons was begun by a group of non-governmental organizations who came together to form the Stop Killer Robots coalition in 2012. The question was then discussed by the UN Human Rights Council and then within the framework of the Convention on Certain Conventional Weapons, with the decision being made in 2016 to create a group of governmental experts with a mandate to discuss this issue.

The role of humans in the processes leading up to the use of lethal force by autonomous weapons is at the center of the discussions of this group of experts. As Noel Sharkey, roboticist and pioneer of the Stop Killer Robots movement, says "the real question is to ascertain what level of control we

as humans are ready to hand over to the machines."[11] In this regard, the operational experience of militarized AI, both in Ukraine and Gaza, tends to show that the fact of retaining a human "in the loop" is insufficient to guarantee meaningful control over weapons systems.

* * *

In debates over the moral consequences of technological improvements of weapons systems, there have usually been two opposing positions. One considers technology to be neutral: It is simply a more efficient means of accomplishing the same mission. Destroying a tank using an anti-tank mine or a swarm of drones makes no moral difference. The other says that technology is "performative." The technology affects the actual content of the missions assigned to troops, by greatly extending the field of operations.

With regard to the wars in Ukraine and Gaza, far from contributing to a "cleaner" war that is more compliant with international law, AI has instead led to force being used on a much wider scale, and at a much greater speed. To put it in bald terms, it allows more people to be targeted more quickly, at a lower cost, and with the appearance of rational justification. Its use therefore requires urgent regulation.

Translated and edited by Cadenza Academic Translations
Translator: Caroline Leonard, Editor: Marie Cloux, Senior Editor: Mark Mellor

Key words:
Artificial intelligence
War in Ukraine
War in Gaza
Military innovation

11. Laure Belot, "Noel Sharkey: 'Lorsque des machines répondront à des algorithmes secrets, personne ne pourra prédire l'issue d'un conflit,'" *Le Monde*, July 22, 2015, https://www.lemonde.fr/sciences/article/2015/08/03/noel-sharkey-lorsque-des-machines-repondront-a-des-algorithmes-secrets-personne-ne-pourra-predire-l-issue-d-un-conflit_4710098_1650684.html.