ieee.es
Instituto Español de Estudios Estratégicos

Document
Analysis

81/2024 17/12/2024

José Pardo de Santayana

Artificial intelligence and the war in Ukraine

Artificial intelligence and the war in Ukraine

Originally published in:
Artificial intelligence in geopolitics and conflicts
Issued in June 2024

Abstract:

In the geostrategic context of intense rivalry between China and the United States, the struggle for technological innovation in the field of artificial intelligence (AI) is emerging as the key to future military supremacy.
The war in Ukraine is accelerating the process of developing this technology for warfare purposes and, although the character of this war is not yet determined by AI, such armed conflict resembles a laboratory in which major powers and companies in the sector can constantly train and test AI systems for a wide range of capabilities, functionalities, and applications.
The involvement of Washington -whose companies dominate AI advances- in this war gives it an advantage over Beijing. China is thus closely following everything related to the war. Moscow provides Beijing with operational information on its expertise in this war and, most particularly, on AI, while China cooperates with Russia for high-tech military development.
Since the war in Ukraine is likely to continue for some time, the sides involved are working to gain an advantage over each other and AI will play an increasingly important role in the military contest.

Keywords:

Artificial Intelligence, War, Innovation, Russia, Ukraine, China, United States.

How to cite this document:

PARDO DE SANTAYANA, José. *Artificial intelligence and the war in Ukraine*. IEEE 81/2024 Analysis Document. IEEE web link and/or[3] link (consulted day/month/year).

Introduction

We live at the dawn of a new era of warfare due to the impact of a number of new technologies, of which artificial intelligence (AI) is the most critical, with a major impact on global security issues.

As was seen with the nuclear weapon at the end of World War II, the state that is able to master this technology more quickly and efficiently for military use will have a huge advantage in being able to prevail in the coming wars. The prediction is that in ten years AI will be the dominant military vector (De Vynck, 2023).

This digital age arms race has already begun and some fear that China may be ahead of the pack both for purely technological reasons and for the functioning of an authoritarian state that can direct all energies and capabilities in the desired direction. On the other hand, although US technology companies are leading the global AI sector, they are acting in their own interests and not those of their government, trying to escape state control.

On the other hand, there is also a great fear that, just as AI brings many benefits to the life of societies, it can also have a negative and dangerous impact, which is leading to the need for important regulations.

The debate about the dangerousness of AI is currently raging, with Kissinger (2023) going so far as to state that:

> "We are in a classic pre-World War I situation in which neither side has much room for political concession and in which any disturbance of the balance can have catastrophic consequences [...]. The fate of humanity depends on whether America and China can get along [...]. The rapid progress of artificial intelligence, in particular, leaves them only 5 to 10 years to find a way forward".

The development of AI in the field of defence has its own characteristics. For military use, data from the internet is not enough; most of this data has to come from the

military's own capabilities, sensors and collaboration with technology companies. In addition, military leaders need to know how to use this data for military purposes.

Currently, the war in Ukraine is attracting the focus of military use of AI more than any other armed conflict, making it the great testing ground for future warfare. The close involvement of the US government and US companies in support of Ukraine in this armed conflict gives Washington an advantage over Beijing in drawing lessons applicable to the military use of AI.

For the time being, the application of this technology has allowed Kiev, with a military capability significantly inferior to Moscow's, to seriously challenge it. Before the war, Russia spent an estimated $65 billion on defence, while Ukraine spent only $6 billion.

Technological capabilities such as drones, AI target designation and imagery intelligence, as well as state-of-the-art man-portable anti-aircraft and anti-tank weapons, have enabled Ukraine to stop the Russian onslaught and even fight back during the first year and a half of the war. Similarly, AI is having a significant impact on the defence of Ukrainian critical infrastructure against Russian drone and missile attacks.

At this stage of AI development, the parameters of what is possible are still being explored, but the critical importance of military response to AI technology is undeniable. Although much of the information on the subject is not accessible in open sources, this paper aims to explore the use of AI in the Ukrainian war and the impact this may have on the development of military art in the coming years, recognising that in the Ukrainian war AI has taken a back seat.

Strategic framework

Right now, there are only two AI superpowers: the United States and China are the only countries with the talent, research institutions and massive computing capacity to train the most sophisticated AI models. These are the protagonists of the film, even if the war in Ukraine has a very uneven involvement on both sides.

Before the outbreak of this armed conflict, AI had already triggered a security revolution that was just beginning to unfold. The US military was using AI to optimise everything from equipment maintenance to budget decisions. Intelligence analysts relied on AI to quickly scan mountains of information and identify relevant patterns to enable them to make better and faster decisions (Flournoy, 2023).

Apart from having a very useful tool for improving the efficiency of the US military organisation, there was the concern that China would surpass the United States in AI, especially in military applications. The thinking in Washington was that, if it did, Beijing would have a much more powerful military, capable of increasing the tempo and impact of its operations beyond what the US could match.

Beijing has no intention of ceding technological dominance to Washington and is working hard to develop its own advanced military AI applications. China is making a huge effort in many of the same areas of AI use as the US, such as surveillance, target identification and drone swarms. The difference is that it may not be subject to the same ethical constraints as the US and its allies, especially when it comes to using fully autonomous weapons systems.

> "China has some obvious advantages. Unlike Washington, Beijing can dictate its country's economic priorities and allocate the resources it deems necessary to achieve AI goals. China's national security policy encourages Chinese hackers, officials and employees to steal Western intellectual property, and Beijing has no qualms about trying to recruit leading Western technologists to work with Chinese institutions. Because China has a policy of 'civil-military fusion', which removes barriers between its civilian and military sectors, the People's Liberation Army can draw on the work of Chinese experts and companies whenever it wants. And by 2025, China will produce nearly twice as many science, technology, engineering and mathematics PhDs as the United States, flooding the Chinese economy with talented computer scientists" (Flournoy, 2023).

Thus, the Asian giant already surpasses the United States in computer vision AI and in large ChatGPT-type linguistic models. In terms of military deployment, it is making

a tenfold effort in defence budgets, with the People's Republic of China spending three times more than the US state as a whole, bearing in mind that it is the technology companies there that bear the brunt of the effort. Also counting in Beijing's favour is its supremacy in data and, in a war dominated by AI, everything depends on data, the new ammunition for the wars of the future (Bergengruen, 2023).

However, Washington has advantages over Beijing that derive mainly from the dynamism and technological leadership of its companies in the sector, such as Microsoft, Google, Amazon, Meta, OpenAI. These are engaged in a gladiatorial struggle with each other that is undoubtedly driving innovation.

This competitive dynamic, in the context of deep mistrust and intense rivalry between the two superpowers, drives a race for supremacy in military-grade AI. Whichever side does not go all out to win it is certain to be defeated. The war in Ukraine, lending itself as a testing ground, also tends to accelerate this process.

At the same time, there are many voices expressing concern that this new arms race of the digital age will end up having very serious consequences.

> "Over the past two years, these issues have been discussed with a group of technology leaders at the forefront of the AI revolution, and the conclusion has been reached that the prospects for catastrophic consequences for the United States and the world from unlimited AI advancement are so compelling that government leaders should act now" (Kissinger and Graham, 2023).

In current proposals for ways to contain AI, there are many echoes of the nuclear past. Billionaire Elon Musk's call for a six-month pause in AI development, AI researcher Eliezer Yudkowsky's proposal to abolish AI and psychologist Gary Marcus' call for AI to be controlled by a global governing body essentially repeat proposals from the nuclear age that failed. They are not realistic approaches; never in history has a great power, fearing that a competitor might apply a new technology to threaten its survival and security, given up on developing that technology for itself (Kissinger and Graham, 2023).

In March 2023, RAND President and CEO Jason Matheny testified before the US Senate Committee on Homeland Security and Governmental Affairs on the effects of AI on US national security and competitiveness. He stated that AI poses serious challenges for which the US is unprepared, including the development of new cyber weapons, large-scale disinformation attacks and the design of advanced biological weapons (RAND Corporation, 2023).

The questions then arise:

> "Will machines with superhuman capabilities threaten humanity's status as master of the universe? Will AI undermine the monopoly of nations over the means of mass violence? Will AI enable individuals or small groups to produce viruses capable of killing on a scale previously exclusive to great powers? Could AI erode the nuclear deterrents that have been a pillar of the current world order?" (Kissinger and Graham, 2023).

While governments led the development of nuclear technology, entrepreneurs, technologists and private companies are driving advances in AI. As these private actors make risk-benefit calculations, national interests take a back seat. Moreover, AI is digital, its main evolutions occurring in the minds of human beings. Its applicability evolves in laboratories and its deployment is difficult to observe. Nuclear weapons are tangible; the essence of artificial intelligence is conceptual. Finally, AI is advancing and spreading at a speed that makes long negotiations impossible.

An added danger is that it is technology that determines ethics, as already argued by influential authors such as Yuval Harari, and not ethics that determines the use of technology, as Eduardo Olier (2023) argues with great force in his recent book.

This serious global security dilemma would require, fundamentally, a new dynamic in relations between antagonistic great powers. The war in Ukraine is not facilitating this at all.

On the other hand, what all AI concepts have in common is the vision of a truly networked battlefield, where data moves at the speed of light to connect not only sensors to shooters, but also the totality of deployed forces and platforms.

While the character of that war has not yet changed, Ukraine is the laboratory in which the foundations for the next form of warfare are being laid. This is not a laboratory on the sidelines, but a relentless and unprecedented effort to refine, adapt and improve AI or AI-enhanced systems for immediate deployment. That effort is paving the way for AI warfare in the future (Fontes and Kamminga, 2023).

General aspects

AI is emerging as an important asset in the current Russian-Ukrainian conflict. As it evolves, its application on the battlefield is translating into more accurate and powerful responses to adversary forces, movements and actions. However, it must be recognised that AI is an enabler rather than the defining element in this conflict, as the war is being fought on the ground with infantry, artillery and other weapons in a manner more reminiscent of World War I than World War II, where territory is won and lost in slow, gruelling battles.

The Russia-Ukraine war does not fit these future scenarios. However, it clearly brings these futuristic visions of war closer to reality. The conflict is an unprecedented testing ground for AI. In some areas, its use has been evident. For example, the now ubiquitous use of drones and loitering munitions - also known as kamikaze/suicide drones or smart missiles - for both sides offers AI-enhanced autonomous capabilities in flight, targeting and firing.

Even before its inception, AI had a major impact on the war, helping US intelligence analysts predict Russia's invasion of Ukraine months in advance. This allowed Washington to warn the world and deny Russian President Vladimir Putin the element of surprise.

One of the main aspects of the Russian invasion of Ukraine and the subsequent war is the enormous amount of data being generated by different sources, in volumes far

beyond what humans are capable of analysing quickly and accurately. This also presents itself as an opportunity for experimentation and development of an expanding technology that needs these increasing volumes of specific quality data in order to grow.

Currently, the use of AI in Ukraine is human-centric, with operators ultimately making the final decisions on units, weapons and systems, with the help of AI-driven analytics. This human-centred approach is essential to the ethical use of this technology, as is the need for agreement on how AI can be used by the US and its allies following its inaugural introduction in Ukraine.

Artificial intelligence is used for data analysis to aid decision-making in Ukraine; to analyse a massive amount of imagery and detect objects that would be unmanageable with human means; to monitor an area and detect changes or movement; and for more efficient logistical processes. In short, to establish a global operational picture of the battlefield, with the intention of quickly accessing and reacting to constantly changing combat conditions.

In addition, AI is playing an important role in electronic warfare and encryption. This illustrates how AI systems are constantly retraining and adapting, for example, to deal with idiosyncrasies in a personalised way (Fontes and Kamminga, 2023).

One aspect of enormous strategic significance is the use of AI to help warn US analysts about the movement of Russian nuclear-armed missiles that, in the past, often evaded detection. The US Strategic Command is using an AI programme developed by Rhombus Power (Flournoy, 2023) for this purpose.

A characteristic feature of this war is the rapid evolution of combat technologies and the adaptation of key tactics and concepts by both sides. If the war drags on for too long, we can expect to see a very different operational model at the end.

In particular, many Russian and Ukrainian drones for reconnaissance and combat missions fly in groups, with one or several operators piloting them. An expected evolution of these tactics is to enable true swarms of UAVs to fly autonomously towards targets, thanks to AI technologies. These tactics could even emerge not only from official military research and development institutions, but also from volunteer

organisations that are assisting each side in developing and acquiring technology. Drones used include military-designed UAVs, but also commercial drones such as DJI's Chinese-made Mavic series, which are much cheaper and easier to obtain.

Air defence is another area where significant advances could be made with AI. This responds to the need to effectively combat the growing number of vehicles - manned and unmanned - in the airspace and the decreasing reaction time, in particular, but not exclusively, due to the impact of hypersonic weapons. This would be a real revolution that would end up completely transforming the air-ground battle with some significant risks of loss of control of decision-making processes.

In any case, it should be clear that AI-enhanced weapon systems are only the tip of the *iceberg.* Most AI is and will be deployed in systems far from the battlefield, in cloud computing and data analytics systems related to areas such as planning, logistics and preventive maintenance. This is an often hidden facet of the AI-driven revolution in warfare that is already underway and will not stop.

The particular case of disinformation

In the run-up to Russia's invasion of Ukraine, and throughout the ongoing conflict, social media has served as a battleground for states and non-state actors to disseminate competing narratives about the war and to present the ongoing conflict on their own terms.

Disinformation is being massively used both for operational purposes and in the cognitive battle for narrative. The ability to create fake images, audio and text that are very difficult or even impossible to distinguish from the real thing has greatly enhanced this resource.

For example, at the beginning of the Russian invasion of Ukraine, the Kremlin used a fake video of President Zelensky calling on the Ukrainian people to surrender, which was viewed more than 120,000 times on Twitter. At the time, the technology was not sufficiently advanced and the hoax was not credible. A similar video with Putin calling on Russians to surrender had 50,000 followers. However, advances are coming so

fast and at increasingly affordable prices that the landscape has essentially changed (Pérez and Nair, 2022).

As the war drags on, digital ecosystems have become flooded with disinformation. Strategic propaganda campaigns, including disinformation campaigns, are not new to warfare, but the shift to social media as the primary distribution channel is transforming how information warfare is waged, as well as who can participate in ongoing conversations to shape new narratives.

AI and its subcomponents, such as algorithms and machine learning, are serving as powerful tools to generate and amplify misinformation about the Russia-Ukraine war. The underlying algorithms, which social media platforms use to determine what content is allowed and which posts get the most views, are driving differences in users' perceptions of events. In recent years, both Facebook and YouTube have come under scrutiny from US and EU regulators concerned with preventing their algorithms from prioritising extremist content and properly weeding out misinformation.

AI and its tools also offer effective means to combat disinformation. The sheer volume of information uploaded daily to social media makes it essential to develop AI tools that can accurately identify and eliminate misinformation. Who controls the one who controls us, who determines what is true and what is not, and can we trust our own "Big Brother"?

Twitter users upload more than 500 000 messages per minute, far more than human censors can monitor. Social media platforms are beginning to combine human censors with AI to monitor false information more effectively. Facebook, for example, developed an AI tool called SimSearchNet at the beginning of the COVID-19 pandemic to identify and remove fake posts.

Artificial intelligence in Ukrainian operations

Compared to the use made by the Russians, Kiev seems to be gaining the upper hand. So far, Ukraine has managed to maintain a human-centred approach, with the operators making the final decisions (Benedett, 2023).

Ukraine's use of AI in combat is being made possible by the efforts of both the government and the private sector, with the essential contribution of technologies and concepts for their use offered by its Western allies. While the country's high-tech sector managed to develop key information-sharing *software*, such as Kropyva, even under the stress of war, as well as a Reface notification application to recognise Russian troops from satellite imagery, it is the support received from outside that is proving decisive.

US companies, researchers, technology developers and geographic information systems professionals have made a great effort to provide information to Ukraine, the United States and its NATO allies.

> "In fact, the CEO of Palantir, one of the world's leading AI companies, recently admitted that his company is responsible for most of the targeting in Ukraine, such as tanks and artillery, thanks to the timely information they obtain from satellites and social media to visualise friendly and enemy positions, understand troop movements and conduct battlefield damage assessments. Western companies such as Planet Labs, BlackSky Technology and Maxar Technologies also produce satellite imagery of conflicts and share data and analysis with the Ukrainian government and military" (Benedett, 2023).

This has a major operational impact, as a key role of AI for the Ukrainian military is the integration of target and object recognition with satellite imagery, which has led Western commentators to point out that Ukraine has an advantage in geospatial intelligence. AI is also used to geolocate and analyse open-source data, such as social media content, to identify Russian soldiers, weapons, systems, units or movements.

According to open sources, neural networks are used to combine ground-level photos, video footage from numerous drones and UAVs, and satellite imagery to provide faster intelligence analysis and assessments that yield strategic and tactical intelligence advantages.

A new *machine learning* algorithm is being used on a large scale for damage assessment in key areas affected by military operations. It rapidly analysed more than 2000 km^2 and identified more than 370 000 structures, including thousands not identified by other open data sources, focusing on Kiev, Kharkov and Dnipro, providing this information directly to the wider AI community (Wang, 2023).

Russia's invasion of Ukraine has led to the first recorded use of facial recognition in combat: the Ukrainian military is using US-based Clearview AI to identify dead Russian soldiers, uncover Russian assailants and combat disinformation. Public reports also place AI at the centre of allied efforts in electronic warfare, cyberwarfare and encryption. US company Primer has deployed its AI to analyse unencrypted Russian radio communications, using natural language processing to understand the specific ways Russian soldiers use to communicate. In 2022, the US company Microsoft reported that Ukrainian cyber defences had been successful thanks to advances in AI-enhanced threat intelligence and the rapid distribution of protection *software* to cloud services and other computer networks (Benedett, 2023).

Commercial AI solutions that help the Ukrainian effort are also quickly adopted by militaries that need to think on the fly, without the luxury of long procurement cycles or years-long test and evaluation programmes.

Artificial intelligence in Russian operations

Prior to the invasion of Ukraine, the Russian military had already placed a strong emphasis on AI as a decision-making and data analysis tool and appears to have used it for that purpose in preparation for what Putin called Special Military Operation.

On the Russian side, however, there is less evidence and even less information on the use of AI in actual warfare. Like its Ukrainian counterpart, the Russian high command expects AI to provide data analysis and decision-making capabilities to the fighter with an operator-centric approach to better and faster targeting and decision-making on the battlefield.

However, some Russian military experts anticipate that decision-making in combat operations will eventually be carried out by robotic systems, removing the human operator from key roles and responsibilities. Thus, the push towards the use of AI in autonomous, unmanned and robotic systems is one of the most visible aspects of the country's high-tech research, development, testing and evaluation efforts.

AI is seen as a means to eventually replace human combatants in dangerous situations. For example, the supplanting of manned fighter jets by military robots that can act more quickly, accurately and selectively than people.

The Russian Ministry of Defence's research and development ecosystem includes technical vision, pattern recognition, the application of AI in robotics and the improvement of information systems that process large data sets as the most practical introduction of such technology during ongoing hostilities.

> "In June 2023, Russian-language Telegram channels reported that the Lancet-3 loitering munition uses convolutional neural networks to collect, classify and analyse images and video content obtained by this UAV during flight. Using such neural networks, a Lancet reconnaissance drone can detect enemy targets and transmit its images to the "kamikaze" Lancet, which then carries out an attack [...]. Such claims often lack definitive evidence or even public acknowledgement by the Ministry of Defence, making it difficult to determine whether AI is being used in such a way in the Russian military' (Benedett, 2023).

Russia's flagship project in computer vision, natural language processing, navigation, autonomous movement and group vehicle control is the Marker unmanned ground combat vehicle. This vehicle was handed over to a volunteer organisation based in eastern Ukraine to be tested and evaluated in real combat conditions (Benedett, 2023).

The Russian Ministry of Defence has also gone on record as saying that it monitors AI developments around the world, which of course includes Ukraine's use of this technology.

An essential, if lesser-known, aspect is Russian-Chinese collaboration in this area, and, very specifically, how China is taking advantage of the knowledge derived from this war. In the wake of the tariff war between Washington and Beijing, initiated by President Trump in 2018, China and Russia not only expanded military cooperation, but also extended technological cooperation to fifth-generation telecommunications, AI, biotechnology and the digital economy (Bendett and Kania, 2019). Since then, military technology cooperation has continued to deepen.

In a visit by Xi Jinping to Moscow shortly after the outbreak of the war in Ukraine, the presidents of the two powers agreed to develop new models of cooperation in industries such as AI, internet of things, 5G, digital economy and low-carbon economy and proposed to further enhance their strategic partnership in specific industries, combining their research and industrial capabilities (Thurbon, 2023).

The ongoing war is allowing for two-way cooperation. Moscow provides Beijing with first-hand knowledge of operations, while China helps Russia develop its own AI capabilities and both powers seek to keep a close eye on US AI achievements.

Conclusions

The development of AI for warfare began before the armed conflict in Ukraine in the context, primarily, of the geostrategic rivalry of China and the United States with the potential to transform the way war is waged.

Mistrust between the two superpowers is intensifying this digital arms race and hindering the necessary understanding between the parties to reduce the dangers arising from this dynamic.

The war in Ukraine is accelerating the process of developing AI for military purposes and, although the character of the war is not yet determined by AI, the Russia-Ukraine war resembles a laboratory in which many companies and governments can constantly train and test AI systems for a wide range of capabilities, functionalities and applications.

Companies in the industry are gaining unprecedented access to the real-world application of AI in combat in a conventional conflict between similar adversaries, something previously only possible in simulations.

It is important to recognise that Ukraine's success in using AI has been made possible by US and Western assistance.

The advanced US development of civilian and military AI technologies is setting the global pace for their use in combat.

US AI achievements are also closely followed by the Russian military, which is incorporating US artificial intelligence development practices.

China is also closely following the war and, in particular, technological developments. Although there is little information on this, it can be said that there is two-way cooperation. Moscow provides Beijing with operational information on AI, while China cooperates with Russia on high-tech military development.

As the war in Ukraine is likely to continue for some time, both sides are working to gain an advantage over the other and AI will play an increasingly important role in this war.

This is the tragic paradox. Every day that conflict continues, and humans lose their lives in horrific ways, AI systems are trained with real data from a real battlefield, not to stop the suffering and end the war, but to be more effective in fighting the next one: the AI war (Fontes and Kamminga, 2023).

Bibliography

Benedett, S. (2023). Roles and Implications of AI in the Russian-Ukrainian Conflict. *Russia Matters*. [Accessed: 2023]. Available at: https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict.

Bendett, S. and Kania, E. (2019). A new Sino-Russian high-tech partnership. *ASPI*. [Accessed: 2024]. Available from: https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership.

Bergengruen, V. (2023). Tech Leaders Warn the U.S. Military Is Falling Behind China On AI. *TIME*.

De Vynck, G. (2023). Some tech leaders fear AI. ScaleAI is selling it to the military. *The Washington Post*.

Flournoy, M. A. (2023). AI Is Already at War. How Artificial Intelligence Will Transform the Military. *Foreign Affairs*.

Fontes, R. and Kamminga, J. (2023). Ukraine A Living Lab for AI Warfare. *National Defense Magazine*. [Accessed: 2024]. Available at: https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare

Kissinger, H. (2023). Henry Kissinger explains how to avoid world war three. *The Economist*.

Kissinger, H. and Graham, A. (2023). The Path to AI Arms Control. America and China Must Work Together to Avoid Catastrophe. *Foreign Affairs*.

Olier, E. (2023). *The debacle of the West. The wars of the 21st century*. Sekotia.

Perez, C. and Nair, A. (2022). Information Warfare in Russia's War in Ukraine. *Foreign Policy*. [Accessed: 2024]. Available at: https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

RAND Corporation (2023). U.S. Cooperation with China and Russia, Artificial Intelligence, War in Ukraine. *RAND Weekly Recap.* [Accessed: 2024]. Available at: https://www.rand.org/pubs/articles/2023/weekly-recap-march-10.html

Thurbon, R. (2023). Russia and China want to become world leaders in tech, security, and AI. *TECHSPOT*. [Accessed: 2024]. Available at: https://www.techspot.com/news/98032-russia-china-want-become-world-leaders-tech-security.html.

Wang, A. (2023). War, AI and the New Global Arms Race. *Ted Talk*. [Accessed: 2024]. Available at: https://www.youtube.com/watch?v=EpipswT-LuE.

*José Pardo de Santayana**
Colonel of the Army
IEEE Research Coordinator