

AI INTEGRATION INTO THE ARMED FORCES: THE EXPERIENCE OF THE US, CHINA, AND ISRAEL

<https://doi.org/10.5281/zenodo.20344427>

Narzullaev Shukhrat Uchqun ugli

*Head of the Artificial Intelligence and Cybersecurity Department,
Institute of Land Forces*

Annotation

This article examines the integration of artificial intelligence (AI) technologies into the armed forces of the United States, China, and Israel. The study analyzes the main directions of military AI implementation, including autonomous combat systems, intelligence and reconnaissance, operational planning, cyber warfare, and decision-support technologies. Special attention is given to the strategic approaches adopted by each country: Israel's operational use of AI in asymmetric conflicts, the United States' model of public-private cooperation and technological leadership, and China's state-controlled military-civil integration strategy. The article also highlights ethical, legal, and technological challenges associated with military AI, such as cybersecurity risks, data limitations, autonomous decision-making, and compliance with international humanitarian law. A comparative analysis demonstrates that despite differences in political systems and military doctrines, all three countries are moving toward integrated AI-supported command systems, autonomous combat platforms, and closer cooperation between the defense and technology sectors. The research concludes that AI has become one of the decisive factors shaping future military superiority and global security architecture.

Keywords

artificial Intelligence, Armed Forces, Military Technologies, Autonomous Weapons, Cyber Warfare, Decision Support Systems, Military-Civil Integration, Intelligence Systems, Drone Swarms, Defense Innovation, Operational Planning, Israel Defense Forces, United States Military, People's Liberation Army, AI Governance

With the advent of AI systems, humanity has crossed another technological milestone, a breakthrough that has also become a military breakthrough. The potential capabilities offered by artificial intelligence (AI) are comparable to those of nuclear-armed countries. However, AI systems currently do not pose a threat comparable to a nuclear apocalypse.

Unlike many technologies that have migrated from the battlefield into everyday life, AI's path has been rather the opposite. While the current AI boom is largely driven by investment and research in the commercial sector, military organizations quickly recognized its potential. Its high adaptability and ability to

quickly analyze large amounts of data in real time were bound to attract the military's attention.

Today, several key areas of AI integration into military systems can be identified:

1. Autonomous and robotic combat systems. The development and improvement of unmanned aerial vehicles, ground robots, maritime drones, and other platforms capable of performing tasks ranging from reconnaissance to direct use of force with a high degree of autonomy, minimizing direct human intervention.

2. Intelligence, surveillance, reconnaissance, and data analysis. AI is adaptable to process multimodal data (satellite imagery, intelligence, media reports, etc.). Algorithms can detect hidden patterns, identify targets and objects, and conduct terrain reconnaissance, providing command with an up-to-date operational picture.

3. Decision support and operational planning. Based on comprehensive data analysis, AI systems can predict the development of situations on the battlefield, modeling the consequences of certain decisions.

4. Cyberwarfare and information operations. AI is used to automate both defensive (searching for vulnerabilities and repelling cyberattacks) and offensive cyber operations. In addition, neural networks Deepfakes are used in information warfare to influence the enemy population.

This article presents a comparative analysis of the experience of implementing artificial intelligence technologies in the armed forces of Israel, the United States, and China. The choice of countries is justified by the following factors: Israel, due to the ongoing military conflicts in the Middle East, has practical experience in the operational implementation and use of AI on the battlefield by its own armed forces; the United States maintains a dominant position in the IT sector largely due to technology companies from Silicon Valley (as evidenced by the United States' first place in the [Global rankings. AI Index](#), which evaluates countries based on key indicators such as research and development (R&D), infrastructure, talent pool, investment, government strategy, and commercial adoption of technologies), China, which according to Bank of America will invest between \$84 billion and \$ [98 billion](#) in AI development by 2025, not only competes with the United States at the strategic level but also represents an example of a successful government-led model in this area.

Israel: Operational Effectiveness in the Face of Asymmetric Threats

Israel is deliberately pursuing a policy of integrating AI systems into its armed forces, seeking to compensate for the imbalance between ever-growing intelligence data sets and the limited human resources available to analyze them. Of the key areas of AI integration in military systems previously mentioned, Israel has focused on developing AI systems for decision-making and operational planning. The very logic of Israel's AI-based military technology development suggests that Israel's primary goal in this area is to significantly improve the efficiency of the command

decision-making cycle. Analysis methods used before the "AI era" can no longer cope with the flood of data, which creates the risk of delaying responses to critical information. Israel is therefore using AI to reduce the time between data acquisition, target identification, and the delivery of a lethal strike.

[Unit 8200](#), established in 1952 and part of the IDF's Military Intelligence Directorate, plays a key role in the development and implementation of AI systems in the Israeli Armed Forces. It does not participate in ground combat, focusing primarily on cyberwarfare.

Overall coordination of high-tech efforts (including AI) has historically been under the jurisdiction of Israel's National Cyber Directorate. However, developments are conducted in close collaboration with Israeli institutions (e.g., the Technion, Tel Aviv University, the Weizmann Institute of Science), commercial companies, and, as revealed by [an investigation](#) by Israeli publications +972 Magazine and Local Call, Israeli engineers conscripted into the army after the October 7 attack, previously employed by Google and Microsoft.

[According to data](#) released by Israeli journalist Yuval Abraham, Israel uses at least three AI-based systems on a regular basis: The Gospel / Habsora (Gospel), Lavender (Lavender) and Where's Daddy? (Where's daddy?) All of them were developed by Unit 8200.

"Gospel" automatically identifies and prioritizes attack targets, primarily military installations and infrastructure. Like all other systems, it was trained on databases collected [over decades](#) by Israeli intelligence. "Gospel" is capable of quickly analyzing years of raw data (satellite imagery, drone data, communications interception, cyber intelligence, thermal imaging, etc.).

According to former IDF Chief of Staff [Aviv Kochavi](#), the Gospel system allowed for a radical increase in the number of targets: while before its introduction the IDF identified around 50 targets per year, afterward, during Operation Guardian of the Walls (May 2021), the Gospel system generated up to 100 targets per day, using a unit of around 100 people.

"Lavender" was the next step in the evolution of "Gospel." It was created to locate individuals suspected of belonging to Hamas. The system, based on intercepted signals, including those obtained through Pegasus and similar software, and "indirect intelligence indicators" (being in the same WhatsApp group with known militants, frequently changing residence or phone number, and repeating other behavior patterns typical of Hamas members), assigns a rating from 1 to 100 to a suspect, reflecting the likelihood of their affiliation with Hamas, and also notes their location. [According to an investigation](#) by +972 Magazine and Local In the first weeks after the attack on October 7, 2023, the system included up to 37,000 Palestinians living in Gaza among potential targets.

The Israeli army's use of the Lavender missile has been accompanied by accusations of war crimes. Experts [point](#) to the high risk of error in selecting targets for elimination, given the constantly changing battlefield environment and the need

for rapid decision-making. Specifically, it is alleged that at the beginning of the war, targets for elimination were approved after a cursory check by operators. Approximately 20 seconds were allocated for selecting and evaluating each target, just enough time to ensure that the target was male, as there are no women in Hamas's military wing. This approach, with a margin of error of over 10%, dramatically increased the number of indiscriminate strikes, resulting in collateral damage among women and children.

The "Where's Dad?" system is tightly integrated with "Lavanda." It is designed to track the real-time geolocation of targets previously identified by "Lavanda." "Where's Dad?" calculates when the target returns home and determines the time window for a strike. Journalists [confirm](#) frequent cases of strikes targeting residential buildings, resulting in the deaths of not only the militants but also their entire families.

A dramatic shift in the use of AI systems in combat occurred during Operation Iron Swords. A political decision was made to target any member of Hamas's military wing, regardless of their position in the hierarchy. The number of targets increased exponentially, making it [impossible for](#) a human operator to accurately verify them.

Unit 8200's developments represent some of the most advanced, yet also legally and ethically controversial, military programs in the world. International humanitarian law is based on the principles of distinction, proportionality, and precaution in the conduct of warfare. Systems like "Lavender" and "Where's Daddy?", which identify combatants through algorithms with an error rate of over 10% and tag their locations in residential buildings, clearly violate all of these principles, adding further support to human rights activists' condemnation of Israel's warfare methods. Israel's refusal to sign the [2023 Hague REAIM Declaration](#) on the responsible use of AI in military affairs has sent a clear signal that Israel will not accept restrictions in this area, despite this running counter to international opinion and moral and ethical norms.

At the same time, the use of AI systems in high-intensity operations, such as in Gaza, is entirely consistent with Israel's own military strategy, the Dahiya Doctrine, which calls for the use of massive, disproportionate force and the destruction of civilian infrastructure to demoralize the enemy. In line with the Dahiya Doctrine, the IDF [plans](#) to integrate AI into half of its military systems by 2028, including further automation of reconnaissance and fire control.

The United States: Public-Private Symbiosis and Global Leadership

The US Department of Defense first [published](#) a strategy guiding the military use of AI in 2018. The document stated that AI technology was key to "fighting and winning future wars." Currently, the document defining the US national strategy for AI development is Executive Order [14101](#), "Removing Barriers to American Leadership in Artificial Intelligence," issued on January 23, 2025. Its implementation was further detailed in [the action plan](#) "Winning the AI Race: A US

AI Action Plan," released by the White House on July 23, 2025. It emphasized the need to cut through bureaucracy, increase investment, and strengthen collaboration between the public and private sectors. These documents have ensured government support for rapidly developing AI technologies in the US, including commercial developments that can be used on the battlefield.

The most ambitious public-private initiative was Project Stargate , [announced](#) in January 2025 by US President Donald Trump. The project unites OpenAI, SoftBank, Oracle , and the investment firm MGX to create a network of advanced data centers for AI processing and training in the US by 2029.

The military remains the primary beneficiary of government investment in AI. For example, the Pentagon accounted for approximately [75%](#) of US government spending on AI-related projects from 2013 to 2023. Coordination of US military AI efforts falls to several key agencies:

1. The Defense Advanced Research Projects Agency (DARPA). Created in 1958 in response to the Soviet Union's launch of the first artificial satellite, DARPA has now become a key Pentagon agency responsible for the development and implementation of new technologies in the US military.

2. The Defense Innovation Unit (DIU). Based in Silicon Valley, it is responsible for the Pentagon's contacts with IT startups. The DIU engages the private sector in defense innovation projects and essentially [serves as a "bridge"](#) between the Pentagon and the dynamically developing AI sector.

3. National Laboratories. Scientific centers such as the Lawrence Livermore National Laboratory Livermore National Laboratory (LLNL) and Los Alamos National Laboratory (LANL) , known for developing nuclear weapons in the mid-20th century, are now also actively [involved](#) in the development of AI systems, including dual-use ones. Some of this research is carried out in close collaboration with IT startups.

Many advanced American military AI systems have civilian roots. It has become common practice to develop a civilian prototype first, then adapt it to military needs in the second phase. For example, the Microsoft headset HoloLens (including HoloLens 2 and the accompanying Azure cloud services) was initially developed as a commercial AR product for training, remote assistance, and working with 3D models, and then the technical developments and cloud infrastructure became the basis for the development of the [Integrated Visual Augmentation System program](#) - an augmented reality system for the US Army.

A sign of growing private sector collaboration with the Pentagon, four executives from major tech companies were commissioned into the U.S. Army Reserve. In June 2025, they were sworn in and promoted to lieutenant colonel: Shyam Sankar (Palantir) , Andrew Bosworth (Meta , recognized as extremist and banned in Russia) , Kevin Weil (OpenAI) , Bob McGrew (Thinking Machines Lab and OpenAI). Top managers led the new military unit , [Detachment 201](#) .

Leaders of leading IT companies are expected to recruit individuals with technology expertise to work for US national security. IT reservists will serve 120 hours per year, have a flexible schedule, and be exempt from military training.

All these events have signaled a paradigm shift in the relationship between the state and the technology sector. Just ten years ago, IT companies avoided working on technologies that could be used for military purposes. Now, for example, [Google](#) and [Open Source AI companies](#) are lifting internal protocols prohibiting the use of their AI developments in weapons production, paving the way for closer cooperation with the defense industry.

This strategic pivot has found practical application in hot spots. The Ukrainian conflict [has become a testing ground](#) for American military AI systems. From the very beginning of the SVO, IT startup executives from Silicon Valley began visiting Ukraine. One of the first was the CEO of Palantir. Technologies, Alex Karp. This company [created the](#) MetaConstellation platform, which models a comprehensive digital battlefield. It integrates and analyzes data from satellites, including Starlink, Maxar, Airbus, ICEYE, Capella, and NOAA, among others, reducing the detection of troop concentrations, equipment, or artillery positions to 2–3 minutes.

Among other American startups that have made a name for themselves in Ukraine, Primer stands out. AI and Clearview AI. Primer AI that specializes in natural language processing and machine translation. Primer Developments AI can overcome language barriers, decrypt, denoise, and translate intercepted tactical radio communications. [Clearview AI has created a biometric image identification system with a claimed recognition accuracy of 99%.](#) Clearview Database The AI has more than 40 billion facial images (during the SVO it was increased by 400%), collected from open sources - profiles on social networks Facebook, Instagram (owned by the Meta company, which is recognized as extremist and banned in Russia) , VKontakte. Privacy Group International claims that the Ukrainian Armed Forces are using this system to identify dead and captured Russian servicemen.

Ukrainian Minister of Digital Transformation Mykhailo Fedorov oversees the overall work with American AI startups willing to provide their systems to the Ukrainian Armed Forces. He openly discusses testing foreign technologies in Ukraine, with an emphasis on testing innovations on the battlefield in real-time. "We are ready to assist companies from partner countries in developing, testing, and refining technologies that actually work on the battlefield. This is an opportunity to gain experience that simply cannot be simulated in a lab," the Ukrainian minister [emphasized](#) .

The launch of the SVO coincided with a global boom in the AI industry, and many American AI startups are offering their developments to the Ukrainian army [free of charge](#), not only for practical testing, but also, likely, to build a reputation as a company whose developments have been used in military operations.

The Pentagon is also actively investing in autonomous systems and agent-based AI processes, focusing on systems capable of performing tasks with minimal human intervention. The following areas are receiving particular attention:

- [Autonomous drones](#). The Replicator program, which aims to deploy thousands of autonomous drones by 2026, has been underway since 2023. The Pentagon [has awarded contracts](#) to Shield to implement this program. AI (\$167 million) and Anduril to improve swarm management algorithms.

[Collaborative Combat Aircraft](#). The US Air Force is systematically introducing combat wingman drones operating in conjunction with manned F-35 fighter jets.

The US's efforts to integrate AI into its military are driven by the need to outpace China, which the United States views as its main [competitor at all levels](#). The US National Security Commission on AI, established in 2021, [predicts](#) that China could become the leader in AI within ten years.

These concerns stem from the fact that China is investing more in military AI projects than the United States. The exact figures for China's military spending on AI are classified, but [a study](#) by the US-based Center for Security and Emerging Technologies (CSET), analyzing publicly available PLA contracts, estimated China's minimum annual purchases of AI-based systems at \$1.6 billion. Actual investments may be significantly higher.

China: State-led integration and total intellectualization

China, recognizing the high transformative potential of AI, is placing a premium on creating an intelligent military. Its approach is also based on a policy of military-civilian integration, but state oversight of the development of military AI systems is incomparably stricter than in the United States. In China, military AI development is directly controlled by the state through a policy of military-civilian integration, which obliges private companies to collaborate with the military, and through centralized five-year planning. For example, the 14th Five-Year Plan, implemented from 2021 to 2025, explicitly [directs](#) the PLA to "accelerate the comprehensive development of the mechanization, informatization, and intelligence" of AI systems. While in the United States, private companies like Google retain significant autonomy and can [challenge](#) military contracts under public pressure, Chinese companies are [legally](#) subject to party directives. Furthermore, the PRC Data Security [Law](#) grants the state direct access to company data, whereas in the United States, such practices are limited by judicial and public oversight.

The development of dual-use AI systems began around the 1980s, with the launch of [the 863 Plan](#), which included a wide range of intelligent robotics projects. Today, this development is carried out by [the National Key Research and Development Program](#), which funds projects in the field of machine learning. The implementation of China's military AI strategy is ensured through close coordination between military and civilian agencies, including:

1. PLA Academy of Military Sciences.

2. State-owned defense corporations. For example, Nornico (Northern Industry Corporation of China) [designs](#) autonomous systems, in particular, Intelligent Precision Strike System (a complex for regulating a swarm of drones and simulating the battlefield), and China Electronics Technology Group Corporation [participates](#) in the development of AI systems for electronic warfare, communications, signal interception and processing.

3. Private technology companies attracted as part of the [military-civilian integration vector](#). Baidu produces autonomous driving and cloud computing technologies. iFLYTEK specializes in speech recognition and natural language processing. Its products are used by the PLA to [automate eavesdropping](#) and intercept communications. PIESAT [sells](#) geospatial data obtained through AI-powered object recognition, which is used for real-time location mapping, and also provides satellite monitoring and data analysis services for surveillance and reconnaissance.

The PLA is implementing AI in a wide range of military applications:

1. Autonomous and unmanned systems.

China is developing highly autonomous [Attack UAVs](#) (Dark Sword, Star Shadow, and Sharp Sword) with autonomous flight capabilities, target identification, and weapon deployment. Work is underway on UAV swarm technology.

In addition to autonomous aerial systems, China is working on land and maritime drones. One of the first functioning land robots was demonstrated during exercises in Cambodia back in 2021. "Robot dogs" demonstrated the ability to carry and fire autonomous small arms. Among maritime systems, notable ones include unmanned boats such as [the Jinghai](#), designed for autonomous patrol of waters, and [the D3000 unmanned corvettes](#) with surface combat capabilities.

2. Management, communications, intelligence and cyber operations.

The PLA Strategic Support Forces are using AI for cyber defense, including image recognition to defend against attacks and detect network intrusions. Furthermore, active work is underway to develop AI systems to collect data from various sources and accelerate decision-making. The stated primary goal is [to create](#) an "all-weather multidimensional situational awareness network."

It is worth noting that, in parallel with China, the United States [is developing a similar network](#) that unites various platforms and domains within the framework of the Joint Agency Command and Control (JADC2) concept.

3. Modeling and exercises.

China is developing digital twins and intelligent simulators for education and training. In May 2024, the journal Common Control & Simulation presented the "Virtual Commander" AI system, which simulates the decision-making style of PLA commanders in computer combat simulations. In doing so, it demonstrates the ability not only to quickly analyze a situation but also to generate action plans and evaluate their effectiveness.

While actively developing AI, China advocates for the responsible and regulated use of military AI. In 2021, China presented [a document at the UN](#), "On Governing the Military Use of Artificial Intelligence," and in 2023, it proposed a global [Initiative](#) on Artificial Intelligence Governance, which was not publicly supported by the US and Israel but [was endorsed by](#) many countries in the Global South. In these documents, China proposes the following provisions, combining technological development and ethical norms: maintaining human control, adhering to international humanitarian law in the development and use of AI in the military sphere, and preventing an arms race in the AI sector.

Comparative analysis

The analysis reveals three distinct trends in the militarization of AI. Israel has chosen a narrowly focused model, focused on solving specific problems at the expense of international law. The United States is pursuing an open innovation model, relying on the strength of the private sector. China remains committed to a socialist market economy, where the state directs the efforts of all sectors to the implementation of high technologies in the military, while developing national standards.

The experiences of Israel, the United States, and China demonstrate that implementing AI systems in the armed forces is fraught with significant challenges. A comparative analysis identified the following challenges facing AI developers everywhere:

1. Lack and/or unavailability of relevant data. The main challenge is the lack of sufficient data directly related to military operations. Much data critical for training AI systems is either not collected digitally (e.g., recorded on paper) or is classified.

Furthermore, the issue of data fragmentation is acute, with information exchange between different branches of the military extremely difficult. This creates "information islands," hindering the creation of a unified training base.

2. Vulnerability of new AI systems. Many experts [acknowledge](#) existing AI systems as highly vulnerable to targeted cyberattacks and sabotage. Attackers can manipulate data and algorithms during the system's training phase. Specifically, they can "poison" training data, introducing hidden biases that lead to systematic errors in the system's operation, the root of which lies in the algorithm itself. The large volume of data, which is difficult to protect, poses an additional challenge. Experts note the impossibility of reliably detecting adversary intrusions into one's own networks.

3. Network limitations. The modern battlefield generates a colossal amount of information: images, drone videos, etc. Existing communication channels are not always capable of transmitting this information in real time. Even with sufficient bandwidth, data transmission delays reduce response times.

The specific environments of air and water pose particular challenges. For example, creating a reliable network for a swarm of UAVs, which requires constant

information exchange between multiple "nodes," is more difficult than controlling individual drones via a point-to-point link. Communication underwater is even more limited due to signal absorption. Furthermore, both UAVs and underwater autonomous vehicles often rely on ground or airborne repeaters, which are vulnerable to missile attacks.

4. Difficulties in testing and evaluation. Establishing trust in AI systems, especially those for military use, requires comprehensive testing to confirm their combat effectiveness. However, it is clearly impossible to test autonomous weapons systems in all possible real-world warfare scenarios. Such modeling requires time and resources and cannot be exhaustive. The very process of testing autonomous systems, especially in combat-like conditions, can pose safety risks.

Overall, despite significant differences in strategic approaches, the experiences of Israel, the United States, and China in implementing AI in the armed forces reveal a number of universal technological and operational trends that are global in nature and determine general trends in the development of the military industry.

First, a focus on creating integrated decision support systems. Israeli developments like "Evangelion" and "Lavender," American programs like Palantir's MetaConstellation, and Chinese projects to create an "all-weather multidimensional situational awareness network" demonstrate a common paradigm shift from human analysts to human operators monitoring algorithms.

Secondly, the development of autonomous and swarm combat systems. This trend reflects the global search for demographic limits through the delegation of tactical functions to autonomous systems.

Third, the emergence of advanced forms of military-civilian integration. For example, the United States has created institutional "bridges" (DIU , Unit 201) that attract civilian startups, China is integrating private companies into defense programs, and Israel is tapping into the pool of developers from tech giants. The methods vary, but the essence remains the same: no country can develop military AI in isolation from the civilian technology sector, which creates new partnerships between private IT companies and the military.

All three directions define the following vectors for the development of modern military-technical policy: the total digitalization of intelligence, the delegation of functions to AI systems while maintaining human control, and the institutional integration of military departments with the IT sector. The experience of Israel, the United States, and China demonstrates that the future of military superiority is determined by the ability to quickly implement this triad of interconnected changes, rather than simply focusing on individual breakthrough technologies.

REFERENCES:

1. United Nations. "On Governing the Military Use of Artificial Intelligence," 2021.
2. Defense Advanced Research Projects Agency. Official publications and reports on AI military systems.
3. Defense Innovation Unit. AI and defense innovation reports.
4. Palantir Technologies. Information on MetaConstellation platform and battlefield AI systems.
5. OpenAI. Publications related to AI infrastructure and Project Stargate.
6. National Cyber Directorate. Israeli cyber and AI security strategies.
7. Unit 8200. Materials on AI-assisted intelligence operations.
8. Center for Security and Emerging Technology. Research on China's military AI investments.
9. Lawrence Livermore National Laboratory. AI and national security research reports.
10. Los Alamos National Laboratory. Publications on defense-related AI development.