



JOURNAL FOR IRANIAN STUDIES

Specialized Studies

A Peer-Reviewed Biannual Periodical Journal

Year 9, Issue 22, October 2025

ISSUED BY



RASANAH
المعهد الدولي للدراسات الإيرانية
International Institute for Iranian Studies

WARFARE IN THE AGE OF AI

Naveed Ahmad

Security Policy Fellow, the International Institute of Iranian Studies (Rasanah)

Abstract

Militaries possess a strong bias for the latest technologies. Artificial intelligence (AI) is no exception, and an arms race for defense AI has been ongoing for over a decade. This has become more pronounced in recent years. The paper offers an outlook on AI's embrace by nation-states, from top-tier powers to disruptive ones. It delves into the prospect of humans being taken out of the decision-making loop and the manner in which defense AI challenges the role of government leaders and military commanders alike.

Keywords: AI, warfare, defense AI, cyber, security policy, decision-making, artificial general intelligence (AGI), Gaza war, Russia-Ukraine war.

Introduction

Artificial intelligence is a natural evolution of scientific knowledge, which poses the age-old ethical and political challenges to the status quo. This study aims to review some of the notable applications of AI in warfare, sometimes referred to as Defense AI, and what policies various major powers are adopting in order to integrate AI in line with their respective values and national interests. For the most part, it delves into the manner in which the embrace of AI impacts the warfare and what role would be left for humans in the future. Abstruse questions intrigue and fascinate scientists and academics while corporations are hungry to earn every penny possible and politicians seek to amass more power. The challenge compounds further as advancements in AI gain ground.

The study, adopting realistic theory and analytical methods, examines three main topics: modern warfare in an AI environment, AI policies in the strategies of great powers and the riddle of AI in decision-making.

Warfare in an AI Environment

War is like a chameleon which alters its color to the environment, wrote Carl von Clausewitz in his seminal treatise *On War*.⁽¹⁾ The objective of war does not change; nonetheless, its character, though, is contingent on the time, the capabilities and the operational environment of the parties involved. As with nuclear weapons, war has changed as much as its nature has remained the same, a continuation of politics by other means.⁽²⁾ So will be the case in the era of AI as evidenced in the Russia-Ukraine war. In June 2025, Ukraine rewrote the rules of the game when its AI-enabled drones took out Russia's parked strategic bombers across the country's vast swaths. The audacious and elaborate attack cost the Kremlin around \$10 billion, diminishing its nuclear, offensive, conventional and surveillance capabilities. In the Middle East, Israel shielded itself from barrages of Iranian ballistic missiles and drones with AI-powered air defense systems, which manifested an extremely low failure rate. Since October 7, Tel Aviv has been deploying AI in an aggressive posture, vital to which remain its algorithmic systems, Lavender, Habsora and Gospel. By fault or intent, the AI-powered systems trained to track Hamas fighters have been far from accurate as they continued to pick civilian males, who were most certainly targeted after dark with their families. An Israeli soldier took 10 seconds to identify and approve the recommended targets.⁽³⁾ "The machine did it coldly, and that made it easier," said one intelligence officer, explaining how people were targeted for bombardment in the Gaza war.⁽⁴⁾

As the examples illustrate, AI-enabled systems can be used to effectively and potently conduct offensive attacks against significantly powerful platforms, defend against sophisticated barrages of missiles as well as deliberately kill civilians alongside probable combatants.

Incremental advances in military technology and networking via internet, satellite and sophisticated intelligence, surveillance and reconnaissance (ISR)

airborne platforms, resulting in data overload, necessitate efficient processing of information for quick and superior decision-making in the battlefield. The evolution of digital ecosystems has led to greater demand for superior data-processing power and autonomous decision-making platforms engaged in the kill chain. Militaries are tech-hungry by design and the quest for firepower is more prone to override ethical considerations. Hence, the race for Defense AI has been continuing without earnest multilateral agreement on its use. AI in warfare not only supplements tactical capabilities but can also yield strategic gains. In the context of the battlefield, AI-enabled systems are increasingly affordable, simpler and available, such as drones, land-based devices, dual-use gadgets and open-source cyber tools.

AI is a transformative force reshaping the battlefield today. AI-based algorithms, integrated within sophisticated networks, process and analyze information from a myriad of sources, which include, but are not limited to, radars, unmanned aerial vehicles (UAVs), airborne early warning aircraft, satellites, electronic detection systems, intelligence agencies and even social media platforms.

Consider the radar data from multiple sources, for instance, a network of coastal radars, an airborne early warning aircraft and satellites. AI algorithms can harmonize it, eliminating redundancies and false positives, to present a clear, real-time picture of potential threats. Far beyond merely data processing, it is intelligence synthesis, a critical capability in today's complex threat environment.

AI can pilot UAVs, or drones, monitor their systems and make real-time decisions based on pre-programmed parameters. In real-time, AI analyzes the data these drones collect — from thermal imaging to high-resolution photography — identifying patterns and anomalies that might otherwise go unnoticed.

Airborne early warning aircraft and satellites, which constantly gather data from vast expanses, often in hostile environments are aided by AI not only to manage and analyze the information but also to alert operators to potential threats concurrently, for example, by detecting a sudden change in radio frequencies and warning the command instantly.

AI's role in command and control extends to the most crucial and controversial domain of decision-making. Does it just recommend a better course of action or actually decide on behalf of its operators? This is where leaders, commanders and theorists are starkly split. By continuously analyzing patterns, AI-enabled systems update potential courses of action, prompting decision-makers to take optimal courses. If the algorithm is adequately trained, it can make a difference in victory and defeat.

For air defense and ballistic missile defense, AI algorithms calculate the most effective combination of weapons and firing times without human intervention, optimizing resource use and ensuring a robust defense.

AI algorithms trained to counter cyberthreats mimic potential cyberattacks, discover system vulnerabilities and execute preventive measures in real-time.⁽⁵⁾ AI can be used to develop unconventional weapons and cyberattacks, including

disabling military communications, manipulating satellite systems or disrupting power grids. This proactive approach to security can protect battlefield systems from a wide array of cyberattacks, deployed only after an extensive testing process. Moreover, AI supercharges online echo chambers, spreading disinformation and encouraging scapegoating. Its use in cyberattacks will likely become more pervasive and harder to detect.

Advanced natural language processing (NLP) — which is vital for large language models (LLMs) — and deep learning are enabling the creation of sophisticated deepfakes, posing significant risks.⁽⁶⁾ AI-powered disinformation can provoke international conflicts, fabricate diplomatic crises or incite civilian panic.

AI is projected to become a strategic asset transforming military operations, decision-making and commanders' roles and workload. Defense AI is fundamentally reshaping military operations by assuming the roles of enabler, disrupter and force multiplier. Its ability to enable autonomous weapons systems and provide real-time data analysis is revolutionizing decision-making, enhancing situational awareness and improving mission outcomes. While AI's potential in human-machine teaming and decision support is empowering military leaders with better-informed choices, it also creates grim ethical dilemmas regarding compliance with the Geneva Conventions, the UN Charter⁽⁷⁾ and international humanitarian law.

The specter of global transition from computer-assisted operations to AI-enabled or -executed functions at scale has led to the emergence of three schools of thought: enthusiasts, deniers and pragmatics.⁽⁸⁾ AI enthusiasts argue that AI will transform warfare by empowering autonomous systems and enhancing data analysis, increasing the pace of combat operations and reducing uncertainty, potentially revolutionizing the nature of war and geopolitics. Deniers argue that AI's immaturity, data scarcity and black box problem significantly limit its military utility and impact on the nature of a war.⁽⁹⁾ Organizational hurdles, like the need for AI's integration into broader contexts and structures, further slow its adoption. Conversely, AI might increase battlefield uncertainty and "fog," potentially undermining the advantages it offers. Clausewitzian traditionalists and pragmatics agree that AI's military impact is evolutionary, not revolutionary.⁽¹⁰⁾ Pragmatics focus on AI's potential at tactical and operational levels in uncontested environments, emphasizing its data analysis, predictive and automated capabilities, while acknowledging risks from adversarial attacks. International politics and institutional factors may significantly influence AI adoption, and while it can assist in strategy development as a "strategic counsellor," it remains a human-led endeavor.⁽¹¹⁾

AI in the Security Policy of Major Powers

In its 2017 national strategy paper titled "New Generation Artificial Intelligence Development Plan," China underscored the critical importance of AI technology, classifying it as a strategic capability.⁽¹²⁾ China's deployment of Defense AI

particularly aims to enhance situational awareness in realms of better intelligence, surveillance and reconnaissance (ISR). China is focusing on seven key areas: intelligent vehicles, intelligence and surveillance, predictive maintenance, electronic warfare, simulation, command and control and automated target recognition.⁽¹³⁾ The categorization linked to Beijing's broader ambition to become a global leader in AI by 2030 is being realized with stunning innovation and complemented with fast-food-style assembly lines. For instance, China has developed the Feiyi, the world's first autonomous drone capable of operating both in the air and underwater. Named after a Chinese cryptid, it launches from a submarine, concealing its travel beneath the surface before ascending for surveillance or AI-driven tasks.⁽¹⁴⁾ China is developing various systems like the FH-97A. These are answers to the United States' loyal wingman, in which one or more autonomous aircraft follow and assist as a team (swarm) with a crewed aircraft.⁽¹⁵⁾ The People's Liberation Army (PLA) deployed an AI-powered robot dog at their Golden Dragon joint military drills in Cambodia in 2024, months ahead of the US Army which sent its own killer robo-dog — Quadrupedal-Unmanned Ground Vehicle (Q-UGV) — to the Middle East for evaluation.⁽¹⁶⁾

With its massive innovation-powered IT sector and vast defense budget, the United States remains an IT superpower with a significant margin, though it is faced with a fast-advancing near-peer. Wary of losing its lead, Washington keeps refining its regulations, organizational hierarchy, AI-integration command, decision-making and battlefield deployment processes as envisioned in its Joint All-Domain Command and Control Strategy.⁽¹⁷⁾ Since LLMs are vital for data centric warfare, the US Army has contracted with Scale AI for its platform Donovan to assist with Joint All-Domain Command and Control.⁽¹⁸⁾ According to the Pentagon's Third Offset Strategy, the superiority to be maintained must be at par with nuclear weapons and long-range precision strike capabilities.⁽¹⁹⁾ Building on previous guidelines, the US Congress resolved in 2017 that the United States must pioneer AI technology in order to maintain its dominant military power. Like the Cold War era and because of the secrecy of China's AI investments and designs, the United States is gearing up innovation, development and integration in fear of losing the race. The Pentagon is banking heavily on Project Maven, which was conceived to pave the way for wider use of AI-enabled technologies that can autonomously detect, tag and track objects or humans of interest from still images or videos captured by surveillance aircraft, satellites and other means. Originally launched in 2017, the project's responsibilities were split among the National Geospatial-Intelligence Agency, the Pentagon's Chief Digital and AI Office and the Office of the Undersecretary of Defense for Intelligence and Security.⁽²⁰⁾ Already, the US military has earmarked a \$36 billion overhaul of its forces for increased reliance on lethal autonomous weapon systems (LAWS). NATO aspires to build a "drone wall" on its eastern borders — extending more than 1,800 miles from Norway to Poland — against Russia.

Bogged down in Ukraine, Moscow's urgency for AI applications in the military is largely dictated by Kyiv. Russia's military doctrine on AI use is not as articulated as China's but experts deduce that it centers on information warfare as a pivotal tool. The Kremlin's strategy emphasizes AI's potential in shaping information at the strategic level, hence, leveraging disinformation to influence politics and societies. AI-enabled psychological warfare aims to create large-scale chaos for adversaries by manipulating narratives to influence societies and create instability through algorithmic disinformation and cyber disruptions. In its military doctrine, cyberwarfare is under the domain of information warfare. To make up for its deficiency in the latest technologies and weak supply chain for sophisticated military hardware, Russia may also opt for the deployment of its Defense AI in disabling an adversary's command-and-control systems to use hybrid combat weapons. The Russian military banks on a heavily encrypted network of computers powered with AI-enabled codebreaking to hack, disable or disorient an adversary's military equipment and decision-making ability.⁽²¹⁾

According to the French Defense Strategy Document, AI systems are prioritized as must have systems for superiority in the field of operations.⁽²²⁾ The French Armed Forces Ministry has established a ministerial committee named the Defense Artificial Intelligence Coordination Unit (CCIAD) to address ethical issues and coordinate AI integration while fostering strategic partnerships and facilitating industrial upscaling to leverage cutting-edge AI research for military and civilian applications.⁽²³⁾ While France is not holding itself back from deploying Defense AI, it aspires to champion the technology's regulation in military applications.⁽²⁴⁾ Given the fractured nature of great power relations and an active, all domain war in Ukraine imposed by Russia, the chances of AI regulation and agreement for AI arms control are grim.

Iran and North Korea, Russia's allies and disruptors, follow the peer's lead in resorting to AI to achieve low-cost, high-impact military outcomes in order to make up for their financial and technological constraints. Tehran has long pursued Defense AI and exaggerated its capabilities before they were exposed in Ukraine, as well as repeated skirmishes with Israel, finally culminating in the 12-Day War. Yet, Iran, as well as North Korea, have successfully used AI in cyberattacks. Though Iran maintains a more boisterous image-building policy to establish a semblance of deterrence, North Korea's AI landscape is shrouded in mystery. Yet, from the available information through leaks and its military exercises, it can be safely concluded that it is actively applying AI and machine learning (ML) in sensitive areas such as wargaming and surveillance.⁽²⁵⁾

Other more mainstream players like Germany, Türkiye, Pakistan, India and South Korea are steadily integrating AI systems within their respective militaries in relation to their peculiar threat-perception scenarios. Their pursuit of Defense AI appears to be defensive in nature as the above-mentioned states have to feverishly project deterrence. Israel has been deploying AI-powered systems against civilians as well as ambiguous targets, leading to an overwhelming number of

casualties, which may prompt other adversaries and major powers to abandon restraint on technology's integration within their offensive platforms.

The Riddle of Decision in Making Defense AI

Of the three broad categories of autonomous weapons systems: human in the loop systems, human on the loop systems and human out of the loop systems, the system without any human oversight has not been fielded yet. Notwithstanding its various potential benefits and absence of global regulations, leaders and commanders are reluctant to relinquish oversight.

"When we think about nuclear enterprise and our nuclear capabilities, as well as the assured communications that we absolutely have to have, we have to have a human in the loop. As good as AI is, as good as computer processes and things like that could be, it's really only as good as the data that is fed into it," according to US Space Force Colonel Ryan Rose.⁽²⁶⁾

The problem of trust and fear of miscalculation cannot be solved easily and soon.⁽²⁷⁾ Where a human pilot, tank or missile battery commander would be sceptical to fire, LAWS — confident of their safety, accuracy and information — would not hold back.⁽²⁸⁾ Besides, the autonomous systems' decision-making is unintelligible to humans unlike other training simulators or training manuals they use. Such a lack of transparency leads to doubts and suspicion over the autonomy of AI systems. Besides, the training of algorithms has yet to include numerous unexpected scenarios. A widely quoted instance sums up the challenge succinctly: lightly camouflaged personnel could not be detected by an AI-powered security system of US Marines.⁽²⁹⁾ During the 12-Day War, Israel's air defense systems misfired at hostile projectiles in some instances while US Aegis and Patriot systems also targeted unintended objects.⁽³⁰⁾

Even if the systems' algorithm, accuracy and sustainability can be relied upon, the specter of adversaries' countermeasures, which may include adversarial AI, poisoning and conflicting the info-sphere, could lead to adverse unforeseen consequences.⁽³¹⁾

Such attacks meddle with the data pool, input features or change data labels in the algorithm's training phase, which is akin to system poisoning. It can also happen through publicly available information sources ranging from the likes of Wikipedia, Facebook, Twitter and LinkedIn. Thus, there is an urgent need for the creation of dedicated databanks for the military.⁽³²⁾ An absolutely objective and unbiased AI system is nearly impossible; hence, autonomous decision-making would inherently carry elements of mistrust amongst its employers.

"You know, in WarGames, it has this machine called the WOPR (War Operation Plan Response, pronounced 'whopper'). So, the WOPR actually was that AI machine that everyone is scared of. And guess what? We do not have, you know, a WOPR in STRATCOM headquarters. Nor would we ever have a WOPR in STRATCOM headquarters," US Air Force General Anthony Cotton, head of US Strategic Command (STRACOM), said in October 2024.⁽³³⁾

Even if Defense AI is deployed, the chances of conflict increase exponentially due to either side's assessment of self-superiority. Perception of possessing a disproportionate benefit over the adversary sets the course for offense to exploit first-mover advantage.⁽³⁴⁾ It is nearly impossible for one side to exactly assess the other side's Defense AI and fairly assume parity or inferiority. The first-mover advantage is an incentive enough to start a war unless the adversary is relaying in detail its deterrent parity.

The future of Defense AI is a reality but what is not certain is the extent to which humans, heads of state and commanders would rely upon it. Gradually, the technology is advancing to Generative AI, which may lead to various tedious, vital but not extremely sensitive tasks being performed by machines, such as planning of routes and writing of operation orders. However, the military structures, hierarchies and their standard operating procedures (SOPs) tend to be overly complex. Integrating them into AI capabilities would further fatigue the trust matrix. The militaries evolve slowly; hence, doctrinal, hierarchical, structural and operational shifts are confronted with institutional and cultural biases and resistance. Since all of this would be happening for the first time at a swifter pace than the military is accustomed to, the question of trained and trusted manpower creates a separate imbroglio.⁽³⁵⁾

Yet another dilemma confronting the transition is the gulf between strategy and its first contact with battlefield reality. Palantir and other AI drivers demonstrate their technologies in a serene and calm battlespace where the adversary is predictable as well as inferior. The noise and chaos of war create their own ground realities, which AI is too new to factor in, at least for now.⁽³⁶⁾ Digital poisoning, adversarial AI and fog of systems can bring forth unforeseen consequences and grave outcomes.⁽³⁷⁾

Unlike the Cold War, private technology corporations are leading innovation and mass production. In the age of techno-feudalism, the military establishments are catching up to technological advancement, too slow to grasp and regulate but rather to bend and adapt. The case studies of the Russia-Ukraine war, Israel's military assault in Gaza and the policies adopted by the United States, China, Russia and other major and some disruptive powers exhibit one commonality: submission to AI.

Conclusion

In today's world, polarized along political, economic and ethnic axes, unleashing free-range Defense AI could upend the global order. It might create a perception of inadequacy, rather than parity, fostering distrust and hyper-nationalism, reminiscent of the uncertainty of the 1960s. Driven by scientific innovation and ideological polarization, the chance of an AI arms race leading to pragmatism seems slim until respective adversaries can see each other's capabilities with relative clarity.

With only a handful of global arms control agreements still in place, the prospect of Defense AI altering the rules of the game could not be brighter. Since technological advancements are still a few years away from achieving Artificial general intelligence (AGI), perhaps half a decade, there remains a slim silver lining. Technology companies, scientists and academics continue to explore solutions to challenging questions. Meanwhile, heads of state, grand strategists or generals could engage in negotiations. As someone who negotiated the world out of a nuclear war once said, “Let us never negotiate out of fear. But let us never fear to negotiate.”⁽³⁸⁾ And a Soviet visionary who signed nuclear arms limitation treaties to end the Cold War proposed, “What we need is Star Peace and not Star Wars.”⁽³⁹⁾ Owing to such statesmen, the world did not have to face the reality of nuclear or “Star Wars.”

Endnote

- (1) Carl von Clausewitz, *On War*, ed. trans. Michael Howard Peter Paret (New Jersey: Princeton University Press), 89, accessed September 15, 2025, <https://www.usmcu.edu/Portals/218/EWS%20On%20War%20Reading%20Book%201%20Ch%201%20Ch%202.pdf>
 - (2) *Ibid.*, 87
 - (3) Emma Graham-Harrison Yuval Abraham, "Revealed: Israeli Military's Own Data Indicates Civilian Death Rate of 83% in Gaza War," *The Guardian*, August 21, 2025, <https://bit.ly/48Vx46l>; Anthony Downey, "The Alibi of AI: Algorithmic Models of Automated Killing," *Digital War* 6, no. 9 (2025),
 - (4) Bethan McKernan and Harry Davies, "'The Machine Did It Coldly:' Israel Used AI to Identify 37,000 Hamas Targets," *The Guardian*, April 3, 2024, accessed September 15, 2025, <https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes>.
 - (5) Kevin Krewell, "IBM, AI and the Battle for Cybersecurity," *Forbes*, September 17, 2020, accessed September 15, 2025, <https://www.forbes.com/sites/tiriasresearch/2020/09/17/ibm-ai-and-the-battle-for-cybersecurity/>.
 - (6) Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," *Wired*, March 17, 2022, accessed September 15, 2025, <https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/>.
 - (7) Jean-Marc Rickli, "The Strategic Implications of Artificial Intelligence," *Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications*, eds. Al Naqvi and J. Munoz Mark (London: Anthem Press, 2020), 48.
 - (8) Jean-Marc Rickli and Federico Mantellassi, "Military Uses of AI and Their International Security Implications," in *The AI Wave in Defense Innovation*, eds. Michael Raska and Richard A. Bitzinger (New York: Routledge, 2023), 18.
 - (9) The "black box" problem, common in AI, hinders understanding of how models generate outputs. This opacity, due to complex architectures and optimization processes, impedes performance improvement and risk mitigation. For more, see Steven Bills, Nick Cammarata, Dan Mossing, Henk Tillman, Leo Gao, Gabriel Goh, Ilya Sutskever, Jan Leike, Jeff Wu, William Saunders, "Language Models Can Explain Neurons in Language Models," *OpenAI*, May 9, 2023, accessed September 15, 2025, <https://openaipublic.blob.core.windows.net/neuron-explainer/paper/index.html>.
 - (10) Daniel Egel, Eric Robinson, Charles T. Cleveland, and Christopher Oates, "AI and Irregular Warfare: An Evolution, Not a Revolution," *War on the Rocks*, October 31, 2019, accessed September 15, 2025, <https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/>.
 - (11) Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence," *Journal of Strategic Studies* 39, no. 5–6 (November 2015): 793–819, doi:10.1080/01402390.2015.1088838.
 - (12) "New Generation Artificial Intelligence Development Plan," *Digi China*, August 1, 2017, accessed September 15, 2025, <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>.
 - (13) Ryan Fedasiuk Jennifer Melot & Ben Murphy, "Harnessed Lightning: How the Chinese military is adopting Artificial Intelligence," *Center for Security and Emerging Technology*, October 2021, accessed September 15, 2025, <https://cset.georgetown.edu/wp-content/uploads/CSET-Harnessed-Lightning.pdf>; Laura Podda, "China's Drive to Dominate the AI Race," *Atlas Institute of International Affairs*, April 14, 2025, accessed September 15, 2025, <https://atlasinstitute.org/chinas-drive-to-dominate-the-ai-race/>.
 - (14) John Scott Lewinski, "These Are the Lethal Autonomous Weapons That Terrify the US Military," *Popular Mechanics*, June 3, 2025, accessed September 15, 2025, <https://www.popularmechanics.com/military/weapons/a64826047/lethal-autonomous-weapons-race/>.
 - (15) David Lague, "In US-China AI contest, the Race Is on to Deploy Killer Robots," *Reuters*, September 8, 2023, accessed September 15, 2025, <https://www.reuters.com/investigates/special-report/us-china-tech-drones/>.
- Note: An autonomous unmanned aerial vehicle (UAV) swarm is a cohesive assembly of cooperative, independent robots that collectively respond to battlefield dynamics at machine speed Drone in a swarm act like an integrated weapon system while perform various AI-coordinated operations and roles.
- (16) Matt Berman, "The US Is Already Fighting the World's First AI War—And China Is Winning," *Popular Mechanics*, March 11, 2025, accessed September 15, 2025, <https://www.popularmechanics.com/military/weapons/a64131751/ai-warfare/>.
 - (17) "Joint All-Domain Command & Control (JADC2) Strategy," *US Department of Defense*, March 2022, accessed September 15, 2025, <https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF>.
 - (18) "Scale AI Partners With XVIII Airborne Corps for First LLM Deployment to a US Government Classified Network," *Business Wire*, May 10, 2023, accessed September 15, 2025, <https://bit.ly/4o9qYnh>.
 - (19) Gian Gentile, Michael Shurkin, Alexandra T. Evans, Michelle Gris , Mark Hvizda and Rebecca Jensen, "A History of the Third Offset, 2014–2018," *RAND*, March 31, 2021, accessed September 15, 2025, https://www.rand.org/pubs/research_reports/RRA454-1.html.

- (20) Brandi Vincent, "Growing Demand' Sparks DOD to Raise Palantir's Maven Contract to More Than \$1B," *Defensescoop*, May 23, 2025, accessed September 15, 2025, <https://defensescoop.com/2025/05/23/dod-palantir-maven-smart-system-contract-increase/>
- (21) Samuel Bendett and Mathieu Boulègue, "Advanced Military Technology in Russia," *Chatham House*, November 2, 2021, accessed September 15, 2025, <https://bit.ly/42y1iZd>.
- (22) "Artificial Intelligence in Support of Defense," *Report of the AI Task Force of French Ministry of Defense*, September 2019, accessed September 15, 2025, <https://bit.ly/4nHTA7j>.
- (23) National Defense Review 2025, *The Secretariat of the National Defense and Security Council of France*, July 13, 2025, accessed September 15, 2025, <https://bit.ly/3WyxRK>.
- (24) Héloïse Fayet, "French Thinking on AI Integration and Interaction With Nuclear Command and Control, Force Structure, and Decision-Making," *European Leadership Network*, November 2023, accessed September 15, 2025, <https://bit.ly/3KHORFZ>.
- (25) Adarsh, "ChatGPT for Cyber Espionage: North Korea's AI-Driven Phishing Campaign," *Sify*, September 25, 2025, accessed September 15, 2025, <https://www.sify.com/ai-analytics/chatgpt-for-cyber-espionage-north-koreas-ai-driven-phishing-campaign/>
- (26) Joseph Trevithick, "How The Military Wants AI To Help Control US Nuclear Arsenal," *The War Zone*, March 7, 2025, accessed September 15, 2025, [HTTPS://WWW.TFWZ.COM/NUCLEAR/THIS-IS-HOW-THE-MILITARY-WANTS-AI-TO-HELP-CONTROL-AMERICAS-NUCLEAR-ARSENAL](https://www.tfwz.com/NUCLEAR/THIS-IS-HOW-THE-MILITARY-WANTS-AI-TO-HELP-CONTROL-AMERICAS-NUCLEAR-ARSENAL).
- (27) John Christianson, Di Cooke, and Courtney Stiles Herdt, "Miscalibration of Trust in Human Machine Teaming," *War on the Rocks*, March 8, 2023, accessed September 15, 2025, <https://warontherocks.com/2023/03/miscalibration-of-trust-in-human-machine-teaming/>.
- (28) Jai Galliot and Austin Wyatt, "Risks and Benefits of Autonomous Weapon Systems: Perceptions among Future Australian Defense Force Officers," *Journal of Indo-Pacific Affairs*, Air University, November 24, 2020, accessed September 15, 2025, [HTTPS://BIT.LY/46HJ1EV](https://bit.ly/46HJ1EV).
- (29) "Deception and Destruction Can Still Blind the Enemy," *The Economist*, January 27, 2022, accessed September 15, 2025, <https://bit.ly/42A9Vma>.
- (30) Emanuel Fabian, "IDF Probing Possible Interceptor Missile Misfire," *Times of Israel*, December 2, 2023, accessed September 15, 2025, <https://bit.ly/3WAvuzj>; Rory McCarthy and Oliver Burkeman, "Patriot in New 'Friendly Fire' Incident," *The Guardian*, April 4, 2023, accessed September 15, 2025, <https://bit.ly/48F2M83>.
- (31) Chris M. Ward, Josh Harguess, Julia Tao, Daniel Christman, Paul Spicer, and Mike Tan, "The AI Security Pyramid of Pain," *Arxiv*, February 16, 2024, accessed September 15, 2025, <https://arxiv.org/pdf/2402.11082>.
- (32) Shilin Qiu, Qihe Liu, Shijie Zhou and Chunjiang Wu, "Review of Artificial Intelligence Adversarial Attack and Defense Technologies," *Applied Sciences* 9, no. 5 (March 2019): 909 <https://doi.org/10.3390/app9050909>
- (33) Ibid
- (34) Zachary Burdette, Karl P. Mueller, Jim Mitre and Lily Hoak, "Six Ways AI Could Cause the Next Big War, and Why It Probably Won't," *The Bulletin of Atomic Scientists* 81, no. 4 (July 2025): 305-312, DOI: 10.1080/00963402.2025.2515793.
- (35) Ian Reynolds, Ozan Ahmet Cetin, "War Is Messy. AI Can't Handle It," *The Bulletin of Atomic Scientists*, August 14, 2023, accessed September 15, 2025 <https://thebulletin.org/2023/08/war-is-messy-ai-cant-handle-it/>.
- (36) Ibid.
- (37) Ian Reynolds, Ozan Ahmet Cetin, 'War is messy. AI can't handle it,' *The Bulletin of Atomic Scientists*, August 14, 2023, accessed September 15, 2025, <https://thebulletin.org/2023/08/war-is-messy-ai-cant-handle-it/>.
- (38) "Inaugural Address of President John F Kennedy," John F. Kennedy Presidential Library and Museum, January 20, 1961, accessed September 15, 2025, , <https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/inaugural-address-19610120>.
- (39) Steven R. Weisman, "Gorbachev calls for Star Peace," *The New York Times*, November 28, 1986, accessed September 15, 2025, <https://www.nytimes.com/1986/11/28/world/gorbachev-calls-for-star-peace.html>.