AI technologies in recent wars and armed conflicts (2010–2026)

Harutyunyan T.[1]

Annotation

This article examines the rapid evolution of artificial intelligence (AI), autonomous weapons, and algorithmic battle management across global conflicts from 2010 to 2026. Analyzing key case studies – including the 2020 Artsakh War, the Russia–Ukraine conflict, the 2025 Israel–Iran "12-Day War," and the 2026 Operation "Epic Fury" – it tracks the transition of AI from experimental tools into foundational components of military power. The author unpacks the emergence of machine-speed "hyperwar" environments, and the rise of counter-network operations designed to degrade digital command ecosystems. Furthermore, the study explores how low-cost loitering munitions, vision-based autonomous drone swarms, and AI-enabled cyber operations have upended conventional combined-arms economics and doctrines. Finally, it evaluates the democratization of wartime intelligence via civilian OSINT tools alongside critical legal and ethical dilemmas, highlighting the highly fragmented state of global autonomous arms control governance.

Keywords: *algorithmic warfare, artificial intelligence (AI), autonomous weapons, "hyperwar", loitering munitions, drone swarms, sensor fusion, predictive targeting, Operation "Epic Fury", 12-Day War, cyber-kinetic coordination, open-source intelligence (OSINT), military decision compression.*

Rapid expansion of AI-enabled warfare

Since 2010, armed conflicts have increasingly incorporated artificial intelligence (AI), autonomous systems, and machine-assisted decision-making across nearly every domain of warfare. AI-enabled drones, automated ISR (intelligence, surveillance, reconnaissance) platforms, predictive targeting systems, cyber operations, and information warfare tools have evolved from experimental capabilities into operational necessities. Recent conflicts demonstrate that even relatively modest AI systems can dramatically multiply strike capacity, accelerate targeting cycles, and reshape strategic decision-making.

The 2020 Artsakh War marked a major turning point in modern drone warfare. Azerbaijan's use of Turkish *Bayraktar TB2* UAVs and Israeli *Harop* loitering munitions enabled precision strikes against Armenian armor, artillery, and air defenses [1][2]. In Ukraine (2022–2026), both Russia and Ukraine institutionalized mass drone warfare at unprecedented scale. Ukraine reportedly produced nearly 2 million combat drones in 2024 alone [3], while Russia deployed increasingly autonomous loitering systems such as the *V2U* drone[2] equipped with onboard AI target-recognition capabilities [4]. AI-assisted ISR fusion, acoustic targeting systems, and predictive analytics became integral to battlefield operations.

The Israel–Hamas war (2023–24) further expanded the role of algorithmic warfare. Investigations into Israeli systems such as "*Lavender*"[3] and "*The Gospel*"[4] suggested that AI-

[1] PhD, worked at the "Noravank" Foundation as a Deputy Director; at the Public Administration Academy of Armenia as a Head of the Center for the Regional Studies; researcher at the Institute for Armenian Studies (Yerevan State University), and at the "Enterprise Incubator Foundation" as a Program Coordinator. Specialized in science and higher education management and regional security issues.

[2] The *V2U* is a highly autonomous Russian kamikaze drone (loitering munition) equipped with artificial intelligence. It is designed to navigate, search for, and strike targets independently without relying on continuous pilot input or satellite networks.

[3] "*Lavender*" is an AI-powered database and targeting system utilized by the Israel Defense Forces (IDF). It represents a real-world manifestation of "*hyperwar*", where military intelligence processes vast amounts of data at machine speed to generate targets.

[4] "*The Gospel*" is an AI-driven decision-support system used by the Israel Defense Forces (IDF) to automatically

assisted databases and targeting algorithms were used to identify and prioritize thousands of potential targets in Gaza [5][6]. Human-rights organizations and international legal scholars raised concerns regarding civilian harm, algorithmic bias, and the erosion of meaningful human oversight in lethal targeting decisions [7].

Emergence of "hyperwar"[5] and AI-integrated interstate conflict

By 2025–2026, AI-enabled warfare entered a new phase characterized by highly integrated interstate operations combining cyber, ISR, autonomous drones, missile defense, and machine-speed decision-making. The Israel–Iran "12-Day War"[6] demonstrated the emergence of "*hyperwar*" environments in which AI systems fused satellite imagery, drone feeds, SIGINT[7], missile telemetry, and cyber intelligence into real-time operational networks [8][9]. Israeli and allied air-defense architectures reportedly relied heavily on AI-assisted interceptor prioritization and automated threat classification to counter large-scale Iranian missile and drone salvos [10][11][12].

Operation "Epic Fury" (2026)[8] represented one of the largest AI-supported coalition strike campaigns documented to date. U.S. and Israeli forces reportedly integrated AI-driven mission planning, predictive ISR analytics, cyber-kinetic coordination, and automated target prioritization during large-scale strikes on Iranian military infrastructure [13][14]. Open-source and strategic analyses described the campaign as an example of "*AI-enabled coalition warfare*", in which allied systems exchanged targeting and intelligence data through interoperable algorithmic architectures. Reports also indicated unprecedented use of cruise missiles, autonomous ISR drones, cyber operations, and real-time OSINT battle tracking during the conflict [15][16].

The 2026 U.S. intervention in Venezuela[9] illustrated how AI-assisted ISR fusion and predictive targeting are increasingly used in limited urban and regime-change operations. Satellite imagery analysis, drone reconnaissance, biometric databases, and automated communications monitoring reportedly enabled rapid precision targeting and operational coordination. These developments suggest that AI-supported "surgical strike" doctrines may become increasingly central to future interventions [17][18][19].

Operational impacts and military transformation

AI systems have significantly accelerated operational tempo and expanded military strike capacity. AI-enabled ISR fusion platforms can process enormous quantities of sensor data in real time, enabling commanders to identify, prioritize, and engage targets much faster than traditional

generate and prioritize physical infrastructure targets. It serves as the structural counterpart to the "Lavender" system, accelerating military operations into what former IDF officials have described as a high-speed "target factory".

[5] "*Hyperwar*" is a military concept describing a future conflict where artificial intelligence, machine learning, and autonomous systems fully automate command and control. The defining feature of "*hyperwar*" is warfare executed at machine speed, far exceeding human cognitive and reaction limits.

[6] https://www.britannica.com/event/12-Day-War

[7] SIGINT (Signals Intelligence) is the gathering of intelligence through the interception and analysis of electronic signals and communications. It forms the backbone of modern strategic and tactical military intelligence.

[8] Operation "Epic Fury" was the United States military code name for its joint massive military campaign alongside Israel against Iran, commencing on February 28, 2026.

[9] The 2026 United States military intervention in Venezuela, code-named Operation "Absolute Resolve", took place in the early morning of January 3, 2026. Directed by U.S. President Donald Trump, the rapid, high-impact operation resulted in the capture of Venezuelan President Nicolás Maduro and his wife, Cilia Flores, by U.S. special operations forces. Lasting exactly 2 hours and 28 minutes, it stands as one of the shortest direct military interventions in history.

command structures allow. Analysts describe this transformation as a shift toward machine-speed warfare, where AI compresses decision cycles from hours or days into minutes or seconds [20][21].

Low-cost drones and autonomous systems have also transformed the economics of warfare. In Ukraine and the Middle East, inexpensive FPV drones costing hundreds of dollars have destroyed armored vehicles worth millions. AI-supported loitering munitions, drone swarms, and precision-guided systems have increased the vulnerability of traditional armor, logistics hubs, and fixed defensive positions. Simultaneously, AI-assisted missile-defense systems such as *Iron Dome*, *David's Sling*, *Arrow*, and *Iron Beam* increasingly rely on automated threat prioritization and sensor fusion to manage saturation attacks.

Cyber warfare has likewise become deeply integrated with kinetic operations. During the 2025–2026 conflicts, AI-assisted malware generation, automated vulnerability scanning, and coordinated cyber-kinetic attacks reportedly targeted energy systems, communications infrastructure, logistics networks, and military command systems. The convergence of AI-enabled cyber operations with conventional warfare signals an important transformation in military doctrine.

Information warfare and OSINT revolution

AI has also reshaped the information domain. Generative AI systems, deepfakes, automated propaganda bots, and synthetic media increasingly influence public narratives during conflicts. During the Israel–Iran conflict and Operation "Epic Fury", civilian OSINT[10] communities used AI-enhanced geolocation tools, commercial satellite imagery, and machine-learning analytics to monitor missile launches, troop movements, and battle damage in near real time. These developments weakened the traditional monopoly states that once held over wartime intelligence dissemination.

The rapid expansion of publicly accessible AI and OSINT capabilities has introduced both transparency and instability. While open-source intelligence can expose battlefield realities more rapidly, AI-generated disinformation campaigns increasingly complicate verification and escalation management [22][23][24][25].

Legal, ethical, and strategic concerns

The growing use of AI-enabled targeting and autonomous systems has intensified legal and ethical debates. International humanitarian law requires distinction, proportionality, and accountability in the use of force, yet many AI systems rely on opaque algorithms and incomplete data. Critics argue that AI-assisted targeting systems risk dehumanizing warfare by reducing individuals to probabilistic threat scores. Human-rights organizations and UN experts have repeatedly called for "*meaningful human control*" over lethal force decisions.

Despite mounting concern, no binding international treaty currently regulates military AI systems or autonomous weapons comprehensively. Existing efforts remain fragmented, consisting primarily of voluntary declarations, export controls, and non-binding UN resolutions. At the same time, major powers continue investing heavily in AI-driven military modernization, suggesting that competition in autonomous warfare technologies will intensify [26][27][28].

[10] OSINT (Open-Source Intelligence) is the practice of legally collecting, analyzing, and synthesizing publicly available information to answer specific intelligence questions.

Future outlook

The trajectory of warfare points toward greater autonomy, deeper AI integration, and increasingly networked battle-management systems. Future conflicts will likely involve larger autonomous swarms, AI-enabled cyber offensives, predictive ISR ecosystems, and multi-domain sensor fusion linking air, land, sea, cyber, and space operations. Human-machine teaming will become increasingly central to military doctrine, while AI-assisted command architectures may further compress escalation timelines.

At the same time, these developments introduce major risks. Fully autonomous targeting, machine-speed decision-making, and AI-driven escalation dynamics could reduce opportunities for diplomacy and increase the likelihood of accidental or uncontrolled conflict escalation. The wars of 2025–2026 suggest that AI is no longer merely an auxiliary tool in warfare; it is becoming a foundational element of military power, strategic competition, and geopolitical instability in the twenty-first century.

Timeline

Date	Event	Significance / AI Warfare Development
2012	First tests of autonomous UAVs (U.S. Predator upgrades)	Early experimentation with semi-autonomous flight control and AI-assisted ISR capabilities in military UAV platforms.
2014	Russia uses Orlan reconnaissance drones in Ukraine; ISIS employs small drones for bombing missions	Marked the expansion of low-cost UAV warfare and tactical drone reconnaissance by both state and non-state actors.
2018	Shahed loitering munitions emerge; Houthi drone swarm attacks begin	Demonstrated the growing effectiveness of inexpensive loitering munitions and coordinated drone swarm tactics.
2020.09	Artsakh War: mass use of TB2 and Harop drones.	One of the first conflicts where drones and AI-assisted ISR decisively shaped battlefield outcomes and destroyed armored formations.
2021	Israeli intelligence units develop ML targeting tools for Gaza operations	Expansion of machine-learning-assisted targeting databases and predictive intelligence systems.
2022.02	War in Ukraine; large-scale drone warfare and AI analytics begin.	Massive integration of ISR fusion, FPV drones, satellite intelligence, and AI-enabled targeting support systems.
2023.10	Israel–Hamas war; AI-assisted targeting systems (“Lavender,” “Gospel”) reported.	Raised international debate over algorithmic targeting, civilian harm, and AI-assisted kill-list generation.
2024.04	UN passes non-binding autonomous weapons resolution (166 state votes).[29]	Reflected growing global concern regarding lethal autonomous weapons and meaningful human control.
2025	Russia deploys V2U autonomous swarm drones in Ukraine.	Introduction of onboard AI target recognition and semi-autonomous swarm coordination in active combat.
2025.06	Israel–Iran “12-Day War” demonstrates AI-enabled integrated air defense and “*hyperwar*” command systems.	Showed the convergence of AI-driven missile defense, ISR fusion, cyber operations, and machine-speed battle management.

Date	Event	Significance / AI Warfare Development
2025.09	Ukraine faces ~800 daily Russian drone attacks. Israel fields Iron Beam anti-drone laser.	Highlighted the scale of drone saturation warfare and operational deployment of AI-assisted directed-energy defenses.
2026.01	U.S. intervention in Venezuela uses AI-assisted ISR fusion and precision-targeting operations.	Demonstrated AI-enabled "surgical strike" doctrine integrating surveillance, predictive analytics, and rapid urban targeting.
2026.02	Operation ***Epic Fury*** begins; large-scale AI-supported U.S.–Israeli strikes on Iranian infrastructure.	One of the largest AI-supported coalition precision-strike campaigns, integrating cyber and kinetic warfare.
2026.03	AI-enabled cyber-kinetic coordination and OSINT battle tracking become central features of interstate warfare.	Civilian OSINT, AI analytics, and cyber operations increasingly merge with real-time battlefield operations.
2026.04	International legal debates intensify over algorithmic targeting and AI-assisted coalition warfare [30].	Renewed global focus on accountability, proportionality, and legal oversight in AI-driven warfare.
2026	First reported use of AI-only target coordination (confirmed or alleged); AI arms-control talks continue.	Signals the transition toward increasingly autonomous battlefield coordination and intensified diplomatic concern over AI weapons.

Autonomous weapons and loitering munitions

Loitering munitions – also known as "*kamikaze drones*" – are aircraft that patrol a target area and strike on command or autonomously. In recent conflicts, several nations have fielded these. Notable examples include Israel's *Harop* and *Orbiter* (used by Azerbaijan in 2020) and Iran's *Shahed*-series (captured by Russia in Ukraine) [31]. These systems combine autopilot navigation with sensors for target detection. For instance, Russia's new *V2U* loitering drone (fielded 2025) carries a ~3 kg warhead and an onboard NVIDIA Jetson Orin AI module running a YOLOv5 neural net to identify vehicles and people. Early *V2Us* had LTE data links, but later variants remove all radio, relying solely on on-board terrain maps and vision. These behaviors – fully autonomous target selection and simple swarm tactics – represent a new level of lethality.

Other loitering drones have seen action. Turkey's *TB2* (technically a MALE UAV[11] with guided bombs) was pivotal in Azerbaijan's 2020 victory. The *TB2*'s autopilot, precision munitions (MAM/Cirit) and HD video feed allowed strikes on Armenian armor from beyond air-defense range. Open-source analysts (*Oryx*)[12] documented Armenian T-72 tanks destroyed on camera by *TB2*'s. Israeli *Harop* and *SkyStriker* loiterers also loitered for hours, homing on radar or visually cued targets. Their impact was such that CSIS concluded Azerbaijani UAVs "*enabled forces to find, fix, track, and kill targets far beyond the front lines*", decimating Armenian artillery and defenses.

However, claims of dominance are nuanced. Independent tallies suggest around 177 Armenian tanks were lost (not the ~300 claimed). Many of those were hit by ground-launched ATGMs (e.g. Israeli *Spike*) as well – *Oryx* found at least 28 tank kills by *Spike* missiles [32][33]. In other words, drones multiplied effects but did not act alone. Analysts caution that

[11] MALE UAV (Medium-Altitude Long-Endurance Unmanned Aerial Vehicle) represents a critical class of military and civilian drones. They operate at altitudes between 3,000 and 9,000 meters and fly continuously for 24 to 48 hours.

[12] *Oryx* (*Oryxspioenkop*) is a prominent Dutch open-source intelligence (OSINT) defense analysis website. It gained international recognition for compiling visually verified equipment losses during global conflicts.

TB2's, while versatile, constituted one part of a larger combined-arms assault. Still, these UAV's clearly changed the calculus: drone-launched strikes on reserves and logistics helped break stalemates.

Drone swarms and coordination

Modern loitering munitions can operate in swarms with minimal communication. Analysts describe innovative coordination methods using vision: drones are painted with distinctive wing markings so each can visually identify its neighbors. They then fly in staggered formations (different altitudes) to maintain line-of-sight and coordinate attacks without radio. For example, CSIS notes *V2U*s flying in a vertical "ring" formation around targets, enabling collective maneuvers.

FIGURE 4

Visual Identification Markings Enabling Potential Vision-Based Swarm Coordination

Note: Illustration not to scale.

Source: CSIS. Illustration by Sabina Hung/CSIS.

CSIS

Fig.2: Visual swarm coordination. Russian V2U drones (blue) reportedly use painted markings and staggered formation to stay in visual range of each other.

Once a swarm finds a target, it can split tasks. One illustrated tactic (Fig.3) shows some drones holding position (search) while others attack the selected target. In practice, reports indicate *V2U* swarms have autonomously encircled groups of vehicles or buildings before launching a coordinated strike. Such formation tactics and "swarming" behaviors mark a step

toward human-free group decision-making. They complicate defenses: jamming or shooting a few drones may not break the swarm if they rely on vision and local AI.

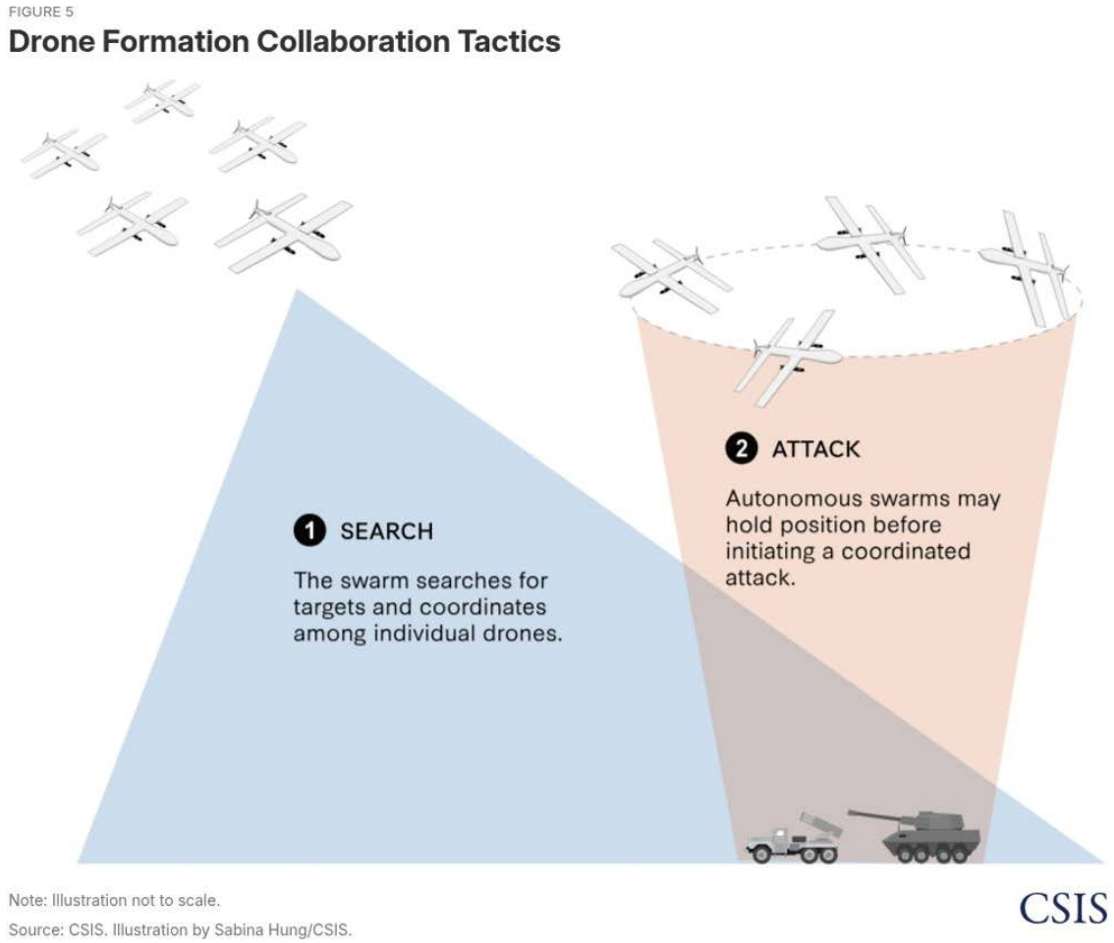

Fig.3: Autonomous drone swarm tactics. Seven Russian V2U loiterers reportedly deviated to form a circular search/attack pattern and then struck when targets were detected.

Drones, ISR, and surveillance AI

Outside of kamikaze roles, UAVs serve as flying sensors. Both sides in recent wars have used drones for **ISR** with AI augmentation. For instance, high-altitude recon drones relay imagery to analytics software (*Palantir*[13], *Delta*[14]). Machine learning now assists operators in sifting through massive data: object-detection AI (e.g. convolutional networks[15]) flags enemy vehicles or dug-in positions in drone video or satellite images. Ukrainian forces report that automated acoustic sensors and AI now alert them to incoming artillery by sound signature. Chinese surveillance balloons and synthetic aperture radars are also being evaluated with AI signal processing.

[13] *Palantir Technologies* is an American software company specializing in big data analytics, AI integration, and operational decision-making platforms for government and commercial sectors.

[14] *DELTA* is Ukraine's national military digital ecosystem for situational awareness and battle management (Command and Control, C2). Developed by the Innovation Center of the Ministry of Defense of Ukraine, the platform serves as the primary "*digital heart*" of the Ukrainian Armed Forces. It aggregates intelligence data to construct a unified, real-time map of the battlefield.

[15] In modern defense infrastructure – such as the on-board AI of the *V2U* drone, Palantir's reconnaissance algorithms, and Ukraine's DELTA ecosystem – CNNs serve as the core engine for Computer Vision (CV). They automate the detection, classification, and tracking of military assets, camouflage anomalies, and structural fortifications.

An example is Ukraine's *Delta* system, which fuses satellite imagery, intercepts, and drone feeds onto real-time digital maps. AI aids by auto-highlighting possible targets, reducing human workload. As one analysis notes, Ukrainian factories churned out ~1.5 million FPV drones in 2024, many with plug-and-play AI modules for simple obstacle avoidance or target marking. Private startups offered AI kits (vision, collision avoidance) to upfit ordinary quadcopters for combat. On the defensive side, Russia used *Orlan-10* and *Lancet* drones in Syria to find rebel positions, though with mostly remote-pilot control. ISIS and Houthi rebels have employed off-the-shelf quadcopters for reconnaissance and improvised bombs, but these lacked real AI brains beyond GPS hold and basic stabilizers.

In sum, surveillance and targeting AI has shifted from lab to field: modern conflicts increasingly see AI-enabled UAVs for spotting and tracking. But these are largely "dumb" sensors augmented by off-board AI (analysts and servers), not fully autonomous scouts. The true novelty in 2020's has been the scale of drone deployments and the addition of on-board ML chips on advanced models (as seen in Russian and Chinese drones).

Decision support and targeting AI

Armies are using AI also in their command centers. Decision-support software helps process battlefield data and propose targets. For instance, ***Palantir MetaConstellation***[16] (used by U.S./Ukraine) fuses multi-intel streams and employs edge AI to highlight potential threats. Ukraine's General Staff integrates satellite/signal intel with AI anomaly detectors to nominate firing solutions to artillery.

By contrast, some AI directly influenced targeting choices in controversial ways. Investigations into the Israel–Gaza war reveal an AI tool "*Lavender*" that ranked Gazans by suspected militant affiliation. Based on leaked reports, "*Lavender*" sifted 2.3 million Gazan profiles and generated a "kill list" of ~37,000 individuals. Allegedly, analysts then "rubber stamped" strikes – reportedly spending only ~20 seconds reviewing each AI-suggested target. The IDF claims "*Lavender*" is merely a "*database … to cross-reference intelligence*", but human rights groups warn this AI-driven method risks mass civilian harm (estimates cited 5-10 civilian deaths "acceptable" per fighter).

Aside from lethal targeting, AI aids logistics and support. Predictive maintenance (using AI to forecast vehicle failures) is being adopted by major armies. The U.S. programs (e.g. Army's *ODIN*[17]) aim to automate supply chain routing. In Ukraine, AI planning tools schedule drone recharging and allocate trucks to units. While details are less public, these systems fall under military "AI acquisition" initiatives worldwide. Similarly, cyber operations employ AI: Ukraine's Cyber Command notes Russian APT's[18] used AI to write phishing emails and

[16] *Palantir MetaConstellation* is a specialized aerospace intelligence software platform designed by Palantir Technologies. It functions as an automated orchestrator for global satellite constellations, optimizing tasking, data collection, edge computing, and real-time AI image analysis.

[17] Project *ODIN* is a cutting-edge artificial intelligence and machine learning software tool developed for U.S. Army Futures Command by the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

[18] Russian Advanced Persistent Threats (APTs) are highly sophisticated, state-sponsored cyberespionage and cyberwarfare organizations. They operate directly under Russia's primary intelligence agencies: the GRU (Military Intelligence), the SVR (Foreign Intelligence), and the FSB (Federal Security Service).

malware scripts in 2024 [34]. AI-enabled cyber defense (automated intrusion detection) is likewise on development track, though specific field examples are scant.

Information operations and deepfakes

AI has also transformed the information war. Generative AI (deepfakes, text bots) is used by all sides to spread propaganda [35]. Both Israeli and Palestinian narratives circulated AI-created posters and videos (e.g., false images of Israeli mourning or Hamas fighters). In Ukraine, both side used deepfake audio (fake conversations) and AI-crafted memes to sow doubt. The sophistication continues to rise: bipartisan reports in the U.S. warning of "*weaponized AI disinfo*" led to funding for detection tools. Analysts caution that while no large-scale AI deepfake campaign has "decided" a battle yet, the technology now routinely pollutes news cycles.

Conflict case studies

- **Artsakh (Sep–Nov 2020):** Azerbaijan's forces, equipped with *TB2* armed UAVs and Israeli loiterers, dominated the air. Open-source counts confirm heavy Armenian losses: *Oryx* tallies ~146 destroyed tanks. Dozens of those were hit by TB2 strikes, with others by anti-tank missiles. Official tallies underscore intense fighting. Despite drone success, independent analysts caution that ground ATGMs and artillery also inflicted many casualties. Azerbaijan's artillery (*Polonez* MLRS, etc.) and An-2 drone-target decoys complemented UAV usage. Armenia's older Soviet air defenses failed to stop most drones. In sum, drones gave Azerbaijan sensor-to-shooter reach, but the conflict still ended via ceasefire and ground maneuver.
- **Libya (2019–2020):** The UN-backed GNA used Turkish *TB2*'s to ambush Haftar's forces, while Haftar's side had Chinese *Wing Loong* UAS. These drones (piloted) targeted tanks and convoys, tilting the war in Libya's second civil war. Some media credited Turkish *TB2*'s with destroying 17 Haftar tanks in one ambush (though those figures come from Turkish sources). Libya also saw the first use of small "Swarm Drone Attack Teams" by GNA fighters (only remote-control, no reported AI).
- **Syria (2015–present):** Russia and the Syrian government used Iranian-supplied *Shahed-129* (drone) and *Lancet* loiterers against Turkish-sponsored groups and ISIS targets. These were mostly remote-piloted. Russia's real-time use of AI there is less documented, but it reportedly fielded experimental independent drones (*Lancet* without human). Meanwhile U.S. forces in Syria used *Predator*/*Reaper* UAVs (with human gunners) for strikes on Syrian army and ISIS, guided by AI-supported targeting pods.
- **Yemen (2015–present):** Houthi rebels employed Iranian drones (*Ababil-Q*) for strikes, and Saudis used coalition missiles. A notable incident: in 2022 U.S. *F-35*'s shot down several small Houthi drones; these may have been killed partly by AI-assisted targeting systems on the jets (though open details are limited). Overall, Yemen's technological gap was wide: few reported AI uses, aside from passive radar/electronic sensors to detect missiles and drones.

- **Russia–Ukraine (2022–present):** Ukraine has innovated rapidly. Thousands of commercial and military drones swarm battlefields daily. Ukraine's industry produced ≈1.5 million FPV drones in 2024. Many use AI: Google's TensorFlow models help process imagery; Ukrainian labs have developed AI vision modules for improvised drones. Ukrainian volunteers also adapted civilian AI (TensorRT, YOLO) to auto-target Russian forces. On the other side, Russia launched massive waves of *Shahed*/*Geran* loiterers and its own *Lancet* drones. Ukraine's defenses (*Patriots*, *Gepard AA* guns, radar-guided missiles) intercepted many but at great cost. Notably, Ukraine fielded domestically-built interceptor drones and flew the first combat laser prototypes [36].
- **Israel–Gaza (2023–present):** Israeli forces extensively use UAS and robotics in urban combat (small ground robots for tunnel clearing, many UAVs for surveillance and strike with human pilots). The conflict's unique aspect was the scale of AI-assisted targeting reports. Investigations revealed the aforementioned "*Lavender*" and "*The Gospel*" systems: one ranks individuals by machine-learning scores, the other algorithms suggest structural targets (e.g. tunnel or command centers). Estimated effects are hotly disputed. Civilian casualty counts (reported by Gaza health ministry at ~44,000) surged as Israel bombarded buildings. Analysts note that AI "kill lists" likely contributed to very high collateral damage. Israeli officials insist humans review every target (quoting "*analysts verify against law*") but admit using these databases to inform targeting. On the Palestinian side, Hamas and allied groups experimented with drones (some Iranian "*Kaman-12*" UAVs struck Israel in Oct 2023).
- **The Israel–Iran "12-Day War" (2025):** The Israel–Iran "12-Day War" represented one of the first large-scale interstate conflicts defined by AI-enabled integrated warfare across the air, cyber, intelligence, and information domains. Unlike previous proxy confrontations, the conflict involved direct exchanges of ballistic missiles, loitering munitions, cyber-attacks, electronic warfare, and coordinated long-range strike operations between Iran, Israel, and allied regional systems. Analysts widely described the conflict as an early example of "*hyperwar*", in which AI-driven ISR fusion and machine-speed decision-making accelerated combat operations beyond traditional command cycles.

  A central feature of the conflict was the extensive use of AI-assisted air and missile defense systems. Israeli and allied command networks reportedly fused satellite imagery, drone feeds, SIGINT, radar telemetry, and interceptor tracking into real-time decision-support architectures capable of prioritizing threats within seconds. Systems such as *Iron Dome*, *David's Sling*, *Arrow*, and *Iron Beam* relied increasingly on automated target classification and interceptor allocation algorithms to counter simultaneous Iranian missile and drone salvos.

  Iran responded with large-scale saturation attacks designed specifically to overload AI-enabled defensive networks. Iranian forces launched combinations of ballistic missiles, cruise missiles, *Shahed*-series drones, decoys, and electronic warfare attacks intended to overwhelm interceptor coordination systems and create sensor confusion. Open-source reporting and strategic analyses indicated that Iranian doctrine increasingly emphasized

attacking the digital infrastructure underlying network-centric warfare rather than solely conventional battlefield targets.

Particularly significant were Iranian strikes and cyber operations targeting regional radar systems, ISR nodes, communications hubs, and military data centers associated with Israeli and U.S.-aligned operations. Analysts reported that Iran attempted to degrade the "sensor-to-shooter chain" supporting AI-assisted missile defense by targeting early-warning radars, satellite uplinks, cloud-processing facilities, and command-and-control networks across the Gulf and eastern Mediterranean. Some radar installations and regional data-processing facilities reportedly experienced temporary outages, degraded tracking capability, or communications disruption during peak phases of the conflict.

Cyber operations formed an integrated component of Iranian retaliation. Iranian-linked cyber actors reportedly targeted logistics databases, cloud infrastructure, military communications systems, and regional energy networks connected to Israeli and allied operations. Security researchers observed increasing use of AI-assisted malware adaptation, automated reconnaissance, and machine-speed vulnerability scanning during these campaigns. Electronic warfare and spoofing operations were also reportedly employed to confuse automated targeting systems and degrade ISR reliability.

The conflict additionally demonstrated the growing influence of OSINT and commercial AI analytics in warfare. Civilian analysts using AI-enhanced geolocation tools, synthetic-aperture radar imagery, and machine-learning-assisted object recognition tracked missile launches, strike damage, and air-defense activity in near real time. Social-media analysis systems employing natural-language processing monitored emerging narratives, disinformation campaigns, and escalation signals throughout the war.

Operationally, the "12-Day War" illustrated both the strengths and vulnerabilities of highly networked AI-enabled military systems. AI-assisted ISR fusion accelerated defensive coordination and targeting cycles, yet Iranian saturation attacks demonstrated that even advanced integrated defense architectures could be strained through simultaneous kinetic, cyber, and electronic attacks against their information infrastructure. Analysts concluded that future conflicts may increasingly focus not only on destroying military assets, but also on blinding or degrading the digital ecosystems that enable AI-supported warfare.

- **U.S. Intervention in Venezuela (2026):** The 2026 U.S. intervention in Venezuela illustrated the growing use of AI-enabled ISR, predictive analytics, and precision-targeting technologies in urban and regime-change operations. Unlike large-scale conventional invasions, the intervention relied on rapid, intelligence-driven operations supported by persistent surveillance and real-time data fusion.

  Open-source reporting indicates that U.S. forces employed AI-enhanced satellite analysis, drone reconnaissance, biometric databases, and communications interception tools to monitor Venezuelan military movements and leadership networks. Analysts described the operation as an example of "*surgical strike doctrine*", emphasizing precision raids, decapitation targeting, and minimal-force urban operations over broad battlefield maneuver.

Commercial satellite imagery combined with AI object-detection software enabled near real-time tracking of military facilities, airfields, and armored deployments. Some assessments suggested that machine-learning systems were used to identify anomalous movement patterns around suspected command locations and logistics hubs.

The operation also highlighted the role of AI-supported information operations. Social-media analysis platforms monitored public sentiment, tracked demonstrations, and identified viral narratives during the intervention. Automated translation and natural-language processing systems reportedly assisted intelligence analysts in processing large volumes of intercepted communications and online content.

Cyber operations accompanied physical deployments. Analysts reported attempts to disrupt Venezuelan communications infrastructure, financial systems, and military coordination networks. AI-assisted vulnerability scanning and automated penetration tools may have accelerated offensive cyber operations during the intervention.

Operationally, the intervention demonstrated how AI-supported ISR and precision targeting can reduce force requirements while increasing operational tempo. International observers also noted that the Venezuela operation may serve as a future model for technologically enabled limited interventions that combine cyber pressure, intelligence dominance, and rapid special operations deployments.

- **Operation "Epic Fury" (USA–Israel–Iran War, 2026):** Operation "Epic Fury" marked a major escalation in U.S.–Israeli military operations against Iran in early 2026 and represented one of the most technologically integrated precision-strike campaigns conducted to date. The operation combined large-scale cruise missile strikes, AI-assisted targeting systems, cyber operations, autonomous ISR platforms, and coalition intelligence-sharing architectures into a unified operational framework. Strategic analysts described the campaign as a defining example of "*AI-enabled coalition warfare*", in which interoperable algorithmic systems coordinated air, naval, cyber, and intelligence assets across multiple theaters simultaneously.

  According to U.S. and independent assessments, the campaign relied heavily on AI-assisted mission planning, predictive ISR analytics, and automated strike sequencing. Machine-learning systems reportedly prioritized missile launch sites, radar installations, underground facilities, drone infrastructure, and command-and-control nodes for simultaneous engagement. AI-driven route optimization tools were used to minimize radar exposure and synchronize strike timing across hundreds of targets.

  One of the most notable operational aspects of "Epic Fury" was the unprecedented scale of long-range precision strikes. CSIS analyses reported that approximately 850 *Tomahawk* cruise missiles were launched during the campaign, making it one of the largest concentrated cruise-missile operations in modern military history. ISR drones equipped with onboard computer-vision systems reportedly identified mobile launchers and relayed targeting information directly into strike-management systems. Autonomous maritime surveillance platforms and AI-assisted naval ISR systems monitored shipping lanes and regional force movements throughout the campaign.

Iran's response demonstrated an increasingly sophisticated doctrine of counter-network warfare. Rather than focusing exclusively on conventional retaliation, Iranian forces reportedly targeted the digital backbone supporting coalition military operations. Ballistic missiles, loitering munitions, cyber-attacks, and electronic warfare systems were directed against regional radar arrays, ISR coordination hubs, military communications facilities, and data centers linked to U.S. and Israeli command architectures.

Open-source reporting suggested that several regional radar systems and data-processing facilities suffered temporary disruption or degradation during Iranian retaliatory strikes. Analysts argued that these attacks were intended to weaken coalition situational awareness, slow AI-assisted target coordination, and disrupt integrated missile-defense synchronization. Iranian strategy appeared increasingly focused on degrading information dominance rather than simply inflicting kinetic battlefield damage.

Cyber warfare played a central role in this effort. Security researchers documented coordinated Iranian-linked cyber campaigns targeting cloud servers, logistics databases, energy infrastructure, military communications networks, and transportation systems associated with coalition operations. AI-assisted malware adaptation, automated vulnerability discovery, and rapid exploit generation accelerated offensive cyber operations during active strike windows.

Information warfare also intensified during the conflict. AI-assisted social-media campaigns, synthetic media, automated bot amplification, and real-time narrative shaping operations were employed by multiple actors. Meanwhile, OSINT communities used AI-enhanced satellite analysis, geolocation systems, and machine-learning-assisted battle-damage assessment tools to monitor strikes and military movements in near real time. These developments further reduced the traditional monopoly states once held over wartime intelligence dissemination.

Operationally, "Epic Fury" demonstrated the advantages of AI-supported targeting, ISR fusion, and coalition interoperability, while simultaneously exposing the vulnerabilities of highly networked command systems. Iranian attacks on radar networks, communications hubs, and data centers revealed that AI-enabled warfare depends heavily on resilient digital infrastructure. Military observers concluded that future interstate conflicts are likely to feature simultaneous attacks on both physical military assets and the data-processing ecosystems that sustain modern precision warfare.

The campaign also intensified international debates regarding escalation risks, accountability, and the legality of AI-assisted targeting systems. Critics warned that machine-speed decision cycles and increasingly autonomous battle-management architectures could compress political deliberation time and heighten the risk of uncontrolled escalation. As a result, Operation "Epic Fury" became a major reference point in the emerging global debate.

Technical capabilities, operational effects and outcomes

Modern battlefield AI systems rely on off-the-shelf and commercial technologies. Sensors include electro-optical cameras (day/night), thermal imaging, LIDAR, radar, and acoustic

arrays. For example, Russia's *V2U* uses TV/IR seekers plus a terrain LiDAR. Chipsets in these systems are often commercial: U.S. components (Intel/AMD CPUs, NVIDIA GPUs, Micron RAM) appear in Chinese and Russian drones despite sanctions. FPGA and ASIC boards from China (Leetop A603, Zhaoxin CPUs) also embed ML accelerators.

Common ML models used in weaponized AI are usually vision networks: YOLO (real-time object detection), ResNet/ConvNets for image classification, and some custom CNNs for missile signature recognition. Language models (BERT, GPT derivatives) see use in information ops (chatbots, data triage) but not yet directly in lethal systems. Notably, both Russia and Iran have tapped open-source large language models (LLaMA, Mistral, etc.) for internal.

Degrees of autonomy vary. Many UAVs have autopilots but require human authorization to fire. The Russian *V2U*, however, reportedly has no operator ("human-out-of-loop") and executes onboard target-recognition. Western militaries classify autonomy levels: "human-in-the-loop" (semi-autonomous with human firing decision) is still doctrine. A 2024 CSIS survey found no confirmed use of fully autonomous lethal robots in combat, but partial automation (e.g. auto-launching once locked on) is increasingly common [37].

AI-enhanced weapons have had clear tactical effects. In documented battles, drones and algorithms have multiplied strike rates. For example, *TIME* reports Israeli AI triaged hundreds of targets weekly vs. tens monthly pre-AI. In Ukraine, a succession of *Shahed* swarms (hundreds of drones) has forced changes in air defense tactics. Civilian casualties highlight ethical costs: AI-assisted targeting in Gaza correlates with unprecedented destruction of whole neighborhoods (as local and UN sources report).

Quantitatively, let's compare impacts (see Table 1 & 2): For instance, *Oryx* verified ~844 Armenian vehicles lost (Sept–Nov 2020), while *Dupuy* analysis suggests ~177 tanks on one side. In Ukraine, by late 2025 both sides lost thousands of ground vehicles (exact tallies vary). A *CSIS/Al-Jazeera* estimate states that Ukraine shot down ~820 Russian drones/missiles on Sept 7, 2025, alone, showing the sheer volume. On the other hand, not all AI experiments have paid off: some Russian *Lancet* drones mis-hit or crashed due to bad weather, and low-tech countermeasures (tarps, nets) occasionally saved targets.

Beyond destruction, these systems have intangible effects. The psychological impact of "unseen killer robots" changes morale. Propaganda videos of *TB2*'s striking tanks were widely shared by Azerbaijan. In Gaza, the perception that an algorithm "chose" targets has fueled global debate. Militaries recognize the "force-multiplier" advantage – one HQ analyst remarked that modern AI shortens operations from months to weeks – but they also note problems like over-reliance on faulty data.

Countermeasures and defenses

To neutralize AI-enabled attacks, forces employ both old and new methods. **Electronic warfare** is first line: jammers and spoofers target drones' navigation. In Artsakh, Armenian forces used Russian-made *Krasnukha-4*[19] jammers for a brief period, causing Azerbaijan to temporarily lose some *TB2* feeds. Modern EW suites can spoof GPS or blind camera sensors.

[19] The Krasnukha-4 (GRAU index 1RL257) is a Russian mobile, ground-based electronic warfare (EW) system. It is designed to neutralize airborne radars, reconnaissance satellites, and drone-guided weapon systems.

Kinetic defenses include anti-aircraft guns (e.g. Germany's *Gepard* 35mm in Ukraine) and short-range missiles. Ukraine has armed its *BMP-1*s with *ZU-23* autocannons and deployed quadcopter *Hunter* drones loaded with explosives to intercept Russian *Gerans*. **Directed-energy weapons** are emerging: Israel's *Iron Beam* laser battery became operational in 2025 to shoot down drones and rockets. Ukraine is investing in its own laser prototypes (e.g. the *90-kW* system by *Laser Innovation*) to cheaply zap drones rather than waste missiles.

Soft tactics also help: camouflage nets, decoy vehicles, and even inexpensive balloon reflectors have been used. Russia attempted *Parody* balloons to mislead *NASAMS* in Ukraine. Meanwhile, cyber-attacks target the networks of AI systems themselves – e.g. Ukraine's IT army launched phishing on Russia's drone controllers. In future, armies are researching AI defenses: neural networks trained to predict and preempt enemy drone attacks, though fielded systems remain rare.

Cyber and deception: Militaries attempt to hack or spoof AI systems. Ukraine's Defense Intelligence reportedly sent poisoned data to Russian AI scripts. Camouflage and decoys (rubber tanks, Tx antennas) mislead computer vision. Some propose "neural firewalls" – onboard AI that recognizes malicious ML patterns. In info warfare, platforms invest in AI filters to flag deepfakes, while analysts use reverse-ML methods to identify forgeries.

Human-in-the-loop & protocols: A simple but critical defense is policy: commanders now often require explicit human confirmation for AI-suggested targets. After the "*Lavender*" reports, IDF stated that multiple human analysts review every target [8]. NATO doctrines emphasize "*personnel usage of force cannot be abdicated to machines*". These operational constraints are as important as tech tools.

Legal, ethical, and policy issues

The rise of battlefield AI has rekindled debates on international law. Key worry: **distinction and proportionality**. International Humanitarian Law requires fighters to distinguish combatants from civilians. But AI systems (especially pattern-based ones like Lavender) often lack context, risking civilian misidentification. UN experts argue mass AI targeting in Gaza may breach the law of armed conflict. Human Rights Watch and Amnesty have demanded transparency and accountability, noting that civilians shouldn't be treated like algorithmic data points.

Meaningful human control is the buzzword. The UN Convention on Conventional Weapons held several 2023–24 talks on autonomous weapons (often called "*killer robots*"), but no treaty has emerged. Instead, dozens of nations issued voluntary statements. The U.S. DoD mandates a human in the loop for lethal decisions, and there are ethical guidelines (DoD's "Responsible AI Principles"). Academia and NGOs generally call for bans or strict limits; major powers call for caution.

On policy and exports: several governments now limit AI tech sales. From 2022, the U.S. blocked export of top-tier GPUs and chipmaking tools to China and its partners. Europe and Japan have similar controls. The intent is to slow adversaries' drone and missile programs (since advanced chips help autonomy). However, sanctions hinder but do not stop: CSIS notes that even under sanctions, over half of AI-related components in Russian drones were U.S.-made. This has sparked calls for tighter allied coordination on high-tech arms control. For instance, UNGA resolution urged states to ensure "*meaningful human control*" and consider new treaties on autonomous weapons.

There is no international ban specifically on AI arms, so discussions revolve around how existing laws cover them. The ICRC and UN human rights mechanisms have called for human

oversight and transparency. For example, the UN Special Rapporteur on Counter-Terrorism warned that remote automated targeting (without meaningful control) is unacceptable. Some countries (Norway, Austria) have advocated a treaty on autonomous weapons. Others (U.S., Russia, Israel) avoid new legal constraints, arguing current law suffices if humans remain in loop.

Ethically, critics liken indiscriminate AI targeting to "*targeting by formula*". They warn of black-box biases: if an algorithm's data is flawed (e.g., labeling teachers as militants), it could slaughter innocents under the guise of precision. The Israeli military's own reports suggest biases (family ties, device changes) might artificially flag people. If unchecked, these tools entrench suspicion and dehumanize warfare. Many ethicists stress that even if deployed, there must be post-hoc accountability – something absent in opaque AI tools.

Future trends

AI in warfare is accelerating. Experts predict drone swarms will expand – not just aviation but also ground & naval robots (e.g. four-legged 'robot dogs', or Chinese humanoid robots armed with machine guns have already been tested in limited roles). Swarm algorithms will improve with multi-agent RL (reinforcement learning) and 5G/6G communications. New sensors (quantum radar, metamaterials) combined with AI could detect stealth threats. Underwater drones (UGVs, UUVs) are under development for autonomous patrols and mine-clearing using ML sonar processing.

On the software side, integration of large language models and data analytics in C3 (command/control) centers will grow. Armies may deploy secure, military-tuned LLMs (closed-source or bespoke) to draft orders, translate intercepts, or simulate adversary responses. Open-source ML models (Meta's LLaMA, Google Gemini, etc.) are already being reverse-engineered for defense use. Ukraine, for example, is experimenting with GPT-based translation tools.

The 2025–2026 conflicts involving Israel, Iran, the United States, and Venezuela demonstrated the emergence of "*hyperwar*" environments characterized by machine-speed ISR processing, AI-assisted targeting, cyber-kinetic integration, and real-time OSINT ecosystems. Future wars are likely to feature increasingly autonomous sensor networks capable of coordinating strikes across air, maritime, cyber, and space domains simultaneously.

Another emerging trend is the increased availability of battlefield intelligence. During the 2026 Iran conflict, commercial satellite providers, independent OSINT analysts, and AI-enhanced geolocation communities produced near-real-time battlefield assessments comparable in some respects to state intelligence products. This erosion of information monopoly may fundamentally alter strategic communication and escalation management in future wars.

Cyber operations are also becoming increasingly integrated with kinetic campaigns. The synchronization of AI-assisted cyber-attacks with missile strikes during Operation Epic Fury suggests that future military doctrines will likely treat cyber disruption as an inseparable component of conventional warfare rather than a separate domain.

Finally, the conflicts underscored growing concerns regarding decision compression. AI-assisted targeting and predictive analytics may shorten human deliberation cycles to minutes or seconds, increasing escalation risks and reducing opportunities for diplomatic intervention. Strategic analysts increasingly warn that fully networked AI battle-management systems could create instability during high-intensity interstate crises if safeguards and human oversight remain inadequate.

Nevertheless, many uncertainties remain. Reliability of battlefield AI is not proven – models trained in one war may fail in another's chaos. Adversarial attacks (feeding false sensor data) are a threat. Also, increased autonomy could trigger unintended escalations or AI arms races. Policymakers are trying to anticipate these: some scientists have called for an "*AI in warfare summit*" to set norms.

Table 1: *The table below compare key systems and conflict uses. Sources are given where available. Contested figures (e.g. kill counts) are footnoted.*

System / Weapon	Type / Role	Manufacturer / Country	Conflicts Used	Key Features	Notes
Bayraktar TB2	MALE UAV (armed ISR/strike)	Turkey (Baykar)	Artsakh 2020, Libya 2019–20, Syria, Ukraine 2022–	Autopilot; precision bombs (MAM); HD camera feed	Effective vs armor/artillery; long loiter time
Harop ("*Harpy-2*")	Loitering munition (suicide drone)	Israel (IAI)	Artsakh 2020, Ukraine (2022-)	Radar/EO seeker; autonomous fire-and-forget	Used to ambush radars/air defenses
Lancet (*ZALA*)	Loitering munition	Russia (Kalashnikov)	Syria (2018-), Ukraine (2022-)	GPS/INS navigation; small warhead; possible ML node	Video guidance; updated variants in Ukraine
Shahed-136 / *Geran-2*	Loitering munition	Iran / Russia	Yemen (2019-), Ukraine (2022-), True Promise 1/2/3/4	GPS/INS; 2,000+ km range	Very cheap (~$20K), large salvo attacks
V2U UAV (Swarm)	Loitering munition (AI loiterer)	Russia (Volat / ZALA)	Ukraine (2025)	On-board NVIDIA Jetson AI; vision-based target ID; swarm tactics	Fully autonomous (no comm); new AI behavior
Switchblade 300	Man-portable loitering drone	USA (AV)	Ukraine (2022–)	Human-on-loop; deploy from ground; CG-guided	<10 kg bomblet; used for precision attack
Predator / *Reaper*	MALE UAV (manned-control)	USA (GA-ASI)	Afghanistan, Iraq, Syria (2010s), 12-Day War, Operation Epic Fury	Autopilot; long endurance; Hellfire missiles	non-AI
Israeli "*Robot Dog*" *	UGV (ground robot)	Ghost Robotics (USA / Israel)	Israel–Gaza 2023	Tele-operated weapon; 4-legged with visual sensors	Possibly fired at Gaza tunnels
"Iron Beam"	Directed-energy anti-drone system	Israel (Rafael)	Israel (deployed 2025)	High-power laser; auto-tracking; low cost-per-shot	Designed to counter rockets/drones
"*Lavender*" System	AI Targeting database/tool	Israel (IDF, undisclosed)	Gaza 2023–24	ML scoring of individuals; data-fusion	Dubious; claimed to flag 37k+ Gazans
Deepfake Generation	Info Ops (AI disinfo)	Various (open-source AI)	Global (Ukraine, Gaza, etc.)	GANs, LLMs; false imagery/text	Used by militias and state-affiliated propagandists

*Confidential Israeli programs like "Robot Dog" usage are reported in media but lack official confirmation.

In each conflict, AI's effect must be weighed against complexity and rules of engagement. The examples show military advantage (greater range, precision, volume of engagement) but also escalation of risks (high civilian casualties, rapid warfare tempos).

Policy responses and export controls

Governments have begun to address the AI arms race. The U.S. enacted broad export controls on advanced AI chips and equipment, specifically to deny adversaries (China, Russia, Iran) the means to build lethal AI systems. These rules cover GPUs, accelerators, and even chipmaking machines. U.S. allies (Japan, EU) have parallel regimes. However, analysts note that Russia, China and Iran are cooperating, both in sharing their own developments and in circumventing Western restrictions. The fact that most electronics (memory, processors) continue to be produced using American technology shows how difficult it is to completely prevent transfers.

Internationally, in December 2024 the UN General Assembly passed a (non-binding) resolution urging states to ensure human control over weapons and to negotiate potential new agreements. Regional bodies (EU, AU) are debating controls on AI weapons. Military alliances are also adapting rules-of-engagement; for example, NATO's Defense Ministerials in 2025 endorsed AI ethical guidelines.

However, actual prohibitions are limited. The U.S. DoD updated its innovation strategy to include "*safe, secure and trustworthy AI*", but explicitly rejected a moratorium on lethal autonomous systems, focusing instead on supervision and robust testing. Private companies (e.g., *DJI*, *Palantir*) have voluntarily pledged not to sell certain tech to conflict zones. NGO's have petitioned the ICC and ICC Prosecutor, urging scrutiny of AI kill-lists as war crimes. The legal debate continues, highlighting, that new cases (like "*Lavender*") will set precedents.

Table 2. *Major Systems and Conflicts*

Type	Examples	Users	Capabilities	Outcomes/Notes
Autonomous Loiterers	TB2 with bombs; Harop; Lancet; V2U swarms, Shahed/Geran	Azerbaijan, Yemen, Russia, Ukraine, Israel, Iran	Guided flight; auto target kill; some swarm AI	Enabled deep strikes; contested accuracy; high civilian risk reported (e.g. Gaza)
Recon/Strike UAVs	Orlan-10, Phoenix Ghost, Predators	Russia, Ukraine, USA	Long endurance; EO/IR sensors; human-in-loop	Extensive ISR; but require human target clearance; still lethal strikes
Ground Robots	Ghost Robotics "UV-UGV"; Wheelbots; Stationary AI turrets	USA, Israel, Russia	Can carry weapons; sensor payload; teleop/autonomy	Mostly experimental; Israel field-tested Spot robotic dogs in Gaza (limited reports)
Cyber-AI	APT "Malware-as-Byte": automated phishing, LLM codegen	Russia, Iran, USA	Automates code/prop creation; ML scanning	Ukraine reports AI-assisted hacking surges; offensive use of ChatGPT remains classified

Type	Examples	Users	Capabilities	Outcomes/Notes
Deepfake Tools	GAN-based image/video generators (Midjourney, StableDiffusion)	Global online actors	Creates realistic fakes at scale	Used in disinfo on all sides; hard to quantify military impact (influence operations).

Sources: Government and think tank analyses (CSIS, Dupuy Institute, SIPRI, RAND), NGO investigations (HRW, UNRWA), academic studies, and major media (Reuters, AP, TIME, Al Jazeera). Many specific platform details come from open-source arms catalogues and manufacturer info (e.g. missilethreat.csis.org). Where claims are disputed (e.g. counts of kills), we cite multiple viewpoints or note uncertainty.

Conclusion

The evolution of artificial intelligence in warfare between 2010 and 2026 has fundamentally transformed the character, speed, and structure of armed conflict. What began as limited experimentation with autonomous UAVs and machine-assisted reconnaissance evolved into highly integrated operational ecosystems combining AI-enabled ISR fusion, autonomous drones, cyber warfare, predictive analytics, algorithmic targeting, and machine-speed command architectures. Recent conflicts demonstrate that AI is no longer a supplementary military capability but an increasingly central component of modern military power.

The conflicts examined in this study, including Artsakh 2020 war, the Russia–Ukraine war, the Israel–Hamas conflict, the Israel–Iran "12-Day War", Operation "Epic Fury", and the 2026 U.S. intervention in Venezuela collectively illustrate the rapid acceleration of AI-enabled warfare. These conflicts revealed how relatively inexpensive autonomous systems and AI-assisted targeting platforms can produce disproportionate battlefield effects, challenge conventional force structures, and reshape operational doctrine. Drone swarms, loitering munitions, AI-assisted missile defense, and cyber-kinetic coordination increasingly define modern combat environments.

The 2025–2026 interstate conflicts further demonstrated the emergence of "*hyperwar*", characterized by compressed decision cycles, real-time sensor fusion, and simultaneous operations across physical, cyber, and informational domains. AI-enabled systems significantly accelerated target identification, strike coordination, and battlefield awareness. At the same time, adversaries increasingly shifted toward counter-network warfare strategies aimed at degrading radar systems, ISR infrastructure, communications hubs, and military data centers that support AI-driven command architectures. These developments indicate that future wars may focus as much on destroying digital infrastructure and information dominance as on traditional battlefield attrition.

Another major transformation highlighted in this article is the democratization of battlefield intelligence. Commercial satellite imagery, OSINT communities, AI-assisted geolocation, and publicly accessible analytical tools increasingly challenged the traditional state monopoly over wartime information. Real-time open-source analysis now influences strategic communication, public perception, escalation dynamics, and operational transparency in ways unprecedented in earlier conflicts.

However, the growing integration of AI into warfare also introduces profound legal, ethical, and strategic concerns. Algorithmic targeting systems, autonomous weapons, and machine-speed operational environments raise difficult questions regarding accountability,

proportionality, civilian protection, and meaningful human control over lethal force. The increasing reliance on opaque AI decision-support systems may reduce transparency in military operations while simultaneously compressing political and diplomatic decision-making timelines during crises.

Despite growing international concern, global governance mechanisms remain fragmented and insufficient to regulate rapidly advancing military AI technologies. Existing initiatives: primarily voluntary declarations, non-binding resolutions, and limited export controls, have not kept pace with the speed of technological and doctrinal change. Meanwhile, major military powers continue accelerating investments in autonomous systems, AI-enabled ISR, cyber capabilities, and integrated battle-management architectures, suggesting that strategic competition in AI warfare will intensify further in the coming decade.

Ultimately, the conflicts analyzed in this article demonstrate that AI is reshaping warfare at tactical, operational, and strategic levels simultaneously. The trajectory of military innovation points toward increasingly autonomous, networked, and data-driven forms of conflict in which cyber operations, information warfare, autonomous systems, and precision targeting become inseparable components of military power. Whether these technologies ultimately enhance deterrence and operational precision or increase instability and escalation risks will depend not only on technological development, but also on the establishment of effective legal norms, political safeguards, and international mechanisms capable of governing the future of AI-enabled warfare.

References

1. Sh. Shaikh, W. Rumbaugh, The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense.
   CSIS, 08.12.2020,
   https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense
2. J. Janovsky et al.,The Fight for Nagorno-Karabakh: Documenting Losses On The Sides Of Armenia And Azerbaijan. *Oryx*, 2020,
   https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html
3. K. Bondar, Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare.
   CSIS, 06.03.2025,
   https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare
4. K. Bondar, How Russia Is Building a Sovereign Drone Ecosystem for AI-Driven Autonomy. *CSIS*, 13.04.2026,
   https://www.csis.org/analysis/how-russia-building-sovereign-drone-ecosystem-ai-driven-autonomy
5. 'AI-assisted genocide': Israel reportedly used database for Gaza kill lists.
   Al Jazeera, 04.04.2024,
   https://www.aljazeera.com/news/2024/4/4/ai-assisted-genocide-israel-reportedly-used-database-for-gaza-kill-lists

6. Y. Serhan, How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare. *Time,* 18.12.2024, https://time.com/7202584/gaza-ukraine-ai-warfare/
7. Questions and Answers: Israeli Military's Use of Digital Tools in Gaza. *Human Rights Watch*, 10.09.2024, https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-of-digital-tools-in-gaza
8. Twelve Days Under Fire: A Comprehensive Report on the Iran-Israel War. *HRANA News Agency*, 28.06.2025, https://www.en-hrana.org/twelve-days-under-fire-a-comprehensive-report-on-the-iran-israel-war/
9. A. Chughtai, Visualising 12 days of the Israel-Iran conflict. *Al Jazeera*, 26.06.2025, https://www.aljazeera.com/news/2025/6/26/visualising-12-days-of-the-israel-iran-conflict
10. F. Alam, How AI shaped the Iran-Israel 12-day war. *The Daily Star*, 29.06.2025, https://www.thedailystar.net/opinion/views/news/how-ai-shaped-iran-israel-12-day-war-3927726
11. Y. J. Bob, IDF's AI unit transformed air force effectiveness in Iran war, commander tells 'Post' – exclusive. *The Jerusalem Post, 02.05.2026,* https://www.jpost.com/defense-and-tech/article-894775
12. O. Kabir, From drones to warnings: IDF expands use of AI in active combat against Iran. *CTECH, 30.03.2026,* https://www.calcalistech.com/ctechnews/article/hyguzhoo11l#google_vignette
13. Y. Bachar, Operational Integration of AI and Cyber: An Analysis of "Epic Fury / Roaring Lion". *ICT, 06.04.2026,* https://ict.org.il/operational-integration-of-ai-and-cyber-an-analysis-of-epic-fury-roaring-lion/
14. F. Lemieux, Algorithmic Warfare in the Iran Conflict: Operation Epic Fury and Dawn of the AI Battlefield. *Homeland Security Today*, 06.03.2026, https://www.hstoday.us/subject-matter-areas/ai-and-advanced-tech/algorithmic-warfare-in-the-iran-conflict-operation-epic-fury-and-dawn-of-the-ai-battlefield/
15. Ch. Fitchew, How AI is rewriting the rules of modern warfare. *Vision of Humanity*, 22.04.2026, https://www.visionofhumanity.org/how-ai-is-rewriting-the-rules-of-modern-warfare/
16. AI Integration in Operation Epic Fury and Cascading Effects. *The Soufan Center,* 03.03.2026, https://thesoufancenter.org/intelbrief-2026-march-3/
17. V. Brandi, US deploys 150-plus military aircraft, drones and other tech in raid to capture Venezuela's Maduro. *Defensescoop,* 03.01.2026,

https://defensescoop.com/2026/01/03/us-military-operation-venezuela-absolute-resolve-details-gen-caine/

18. Kh. Singh, Operations Absolute Resolve and Epic Fury: Role of Artificial Intelligence. *Manohar Parrikar Institute for Defence Studies and Analyses*, 30.03.2026, https://idsa.in/publisher/issuebrief/operations-absolute-resolve-and-epic-fury-role-of-artificial-intelligence
19. H. Ziemer, The Geopolitics of Maduro's Capture: What Does Operation Absolute Resolve Mean for Russia? *CSIS*, 20.01.2026, https://www.csis.org/analysis/geopolitics-maduros-capture-what-does-operation-absolute-resolve-mean-russia
20. F. Gadaleta, The New Intelligence: How AI is Changing the Battlefield Technologically and Ethically by Francesco Gadaleta. *Data Science Talent*, 23.01.2026, https://datasciencetalent.co.uk/the-new-intelligence-how-ai-is-changing-the-battlefield-technologically-and-ethically-by-francesco-gadaleta/
21. Next-Gen Multi-Domain Command and Control (MDC2/JADC2) Systems Revolutionizing Defense Operations. *Defence Industries*, 27.11.2025, https://www.defence-industries.com/articles/next-gen-multi-domain-command-and-control-mdc2jadc2
22. K. Oldřich, M. Chovančík, A. Ilavská, Open-Source Intelligence (OSINT) and the fog of war at the strategic level: Defence industrial production in Russia. *European Journal of International Security*, 16.02.2026, pp. 1-24, DOI: https://doi.org/10.1017/eis.2026.10046
23. M. K. Lucas, Open-Source Intelligence and the New Transparency of Global Conflict. *The Source*, 15.06.2025, https://www.thesourcenews.org/post/open-source-intelligence-and-the-new-transparency-of-global-conflict
24. R. K. Sharma, The 12-Day War: Cyber Frontlines between Israel and Iran. *Manohar Parrikar Institute for Defence Studies and Analyses*, 11.08.2025, https://idsa.in/publisher/comments/the-12-day-war-cyber-frontlines-between-israel-and-iran
25. P. Costanzo, Operation Epic Fury: What the Reports Missed - An Independent OSINT Analysis of the Iranian Cyber Campaign. *Independent Security Researcher*, 17.03.2026, https://www.researchgate.net/publication/403170108_Operation_Epic_Fury_What_the_Reports_Missed_An_Independent_OSINT_Analysis_of_the_Iranian_Cyber_Campaign_February_2026
26. M. F. L. Sddiqui, Artificial Intelligence in Future Warfare: Ethical Frameworks and the Regulation of Lethal Autonomous Weapons IEEE Transactions on Technology and Society, 2026. *IEEE Transactions on Technology and Society*, https://www.researchgate.net/publication/403643037_Artificial_Intelligence_in_Futu

re Warfare Ethical Frameworks and the Regulation of Lethal Autonomous Weapons IEEE Transactions on Technology and Society

27. F. A. Barnaby, Artificial Intelligence, Ethics and Armed Conflict. *Keynote Address, ICRC*, 05.09.2025, https://www.icrc.org/en/article/artificial-intelligence-ethics-and-armed-conflict
28. N. Goussac, V. Boulanin, Responsible Procurement of Military Artificial Intelligence. *SIPRI*, 2026, https://www.sipri.org/sites/default/files/2026-02/0226_milai_procurement.pdf
29. B. Perrin, Lethal Autonomous Weapons Systems & International Law: Growing Momentum Towards a New International Treaty. *American Society of International Law*, 24.01.2025, https://asil.org/insights/volume-29-issue-1/
30. K. H. Cho, Piercing the Algorithmic Fog of War: AI-Enabled Decision-Support Systems and the Responsibility Gap for War Crimes under the Rome Statute, 2026. *UC Law SF International Law Review*, Volume 49, N1, pp. 33-58, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1905&context=hastings_international_comparative_law_review
31. M. Ali, H. Duggal, Charting the past year of Russian drone and missile attacks on Ukraine. *Al Jazeera*, 09.09.2025, https://www.aljazeera.com/news/2025/9/9/charting-the-past-year-of-russian-drone-and-missile-attacks-on-ukraine
32. Ch. A. Lawrence, Casualty Counts from the 2020 Nagorno-Karabakh War. *The Dupuy Institute*, 10.12.2020, https://dupuyinstitute.org/2020/12/10/casualty-counts-from-the-2020-nagorno-karabakh-war/
33. Ch. A. Lawrence, Losses in latest Nagorno-Karabakh Conflict. *The Dupuy Institute*, 02.11.2020, https://dupuyinstitute.org/2020/11/02/losses-in-latest-nagorno-karabakh-conflict/
34. P. Paganini, Ukraine sees surge in AI-Powered cyberattacks by Russia-linked Threat Actors. *Security Affairs*, 10.10.2025, https://securityaffairs.com/183222/apt/ukraine-sees-surge-in-ai-powered-cyberattacks-by-russia-linked-threat-actors.html
35. D. Klepper, Fake babies, real horror: False AI-generated images of the war in Gaza spark alarm. *Los Angeles Times*, 29.11.2023, https://www.latimes.com/world-nation/story/2023-11-29/israel-hamas-war-artificial-intelligence-deepfakes-disinformation
36. A. Chapple, Magic Bullet? Sci-Fi Laser Weapons Are Now An Anti-Drone Reality. *Radio Free Europe, Radio Liberty*, 08.03.2026, https://www.rferl.org/a/iran-ukraine-russia-israel-laser-weapons-future-war/33696183.html
37. A. Blanchard, L. Bruun, Autonomous Weapon Systems and AI-enabled Decision Support Systems in Military Targeting: A Comparison and Recommended Policy Responses. *SIPRI*, 2025, https://www.sipri.org/sites/default/files/2025-06/laws_v_0.pdf