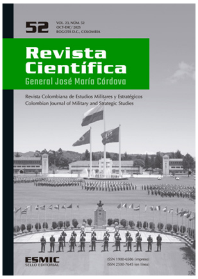

Revista Científica General José María Córdova
Colombian Journal of Military and Strategic Studies

Bogotá D.C., Colombia
ISSN 1900-6586 (print), 2500-7645 (on line)
https://doi.org/10.21830/19006586.1565

RESEARCH ARTICLE

Application of Emerging Defence Technologies in Contemporary Warfare: Lessons Learnt and Prospects

Aplicación de las tecnologías de defensa emergentes en la guerra contemporánea: lecciones aprendidas y perspectivas

Shishir Upadhyaya
Rabdan Academy, Abu Dhabi, United Arab Emirates
supadhyaya@ra.ac.ae

How to cite in APA: Upadhyaya, S. (2025). Application of Emerging Defence Technologies in Contemporary Warfare: Lessons Learnt and Prospects. *Revista Científica General José María Córdova, 23*(52), 843-858.
https://doi.org/10.21830/19006586.1565

Published online: November 13, 2025

Revista Científica General José María Córdova
Colombian Journal of Military and Strategic Studies

Bogotá D.C., Colombia
Volume 23, Issue 52, October-December 2025, pp. 843-858
https://doi.org/10.21830/19006586.1565

RESEARCH ARTICLE

Application of Emerging Defence Technologies in Contemporary Warfare: Lessons Learnt and Prospects

Aplicación de las tecnologías de defensa emergentes en la guerra contemporánea: lecciones aprendidas y perspectivas

Shishir Upadhyaya
Rabdan Academy, Abu Dhabi, United Arab Emirates

ABSTRACT. This paper explores the ongoing revolution in military affairs and looks at the emerging de-fence technologies. It examines the application of technologies such as drones, precision munitions and artificial intelligence in recent and ongoing conflicts to identify their impact on contemporary military doctrine and strategy. The paper argues that because the new de-fence technologies have increased strike effectiveness leading to reduced collateral damage in short-duration conflicts, they seem to have lowered the threshold for warfare, driven by illusions of control. Here, the paper highlights significant ethical, legal, and strategic chal-lenges. The article concludes by calling for doctrinal reform and international cooperation to ensure military innovation serves collective security and respects international law.

Keywords: Artificial Intelligence, defence technology, drones, OODA loop, precision strikes

RESUMEN. Este artículo examina las tecnologías de defensa emergentes, argumentando que crean una fuerza híbrida donde los nuevos sistemas inteligentes coexisten con equipos heredados mo-dernizados. Tecnologías como los drones y las municiones de precisión han aumentado la efectividad de los ataques y reducido las bajas en conflictos de corta duración. La inteli-gencia artificial acelera la toma de decisiones (superciclo OODA), proporcionando una ven-taja temporal e inestable. Sin embargo, esta proliferación parece haber disminuido el umbral para la guerra, impulsada por ilusiones de control. El artículo destaca importantes desafíos éticos, legales y estratégicos. Los riesgos clave incluyen errores de automatización, menor supervisión humana y escalada incontrolada, todo lo cual amenaza la estabilidad regional. El artículo concluye haciendo un llamado a la reforma doctrinal y la cooperación internacional para garantizar que la innovación militar sirva a la seguridad colectiva y respete el derecho internacional.

Palabras clave: ataques de precisión, drones, ciclo OODA, inteligencia artificial, tecnología de defensa

Received: September 9, 2025 • **Accepted:** November 11, 2025

Contact: Shishir Upadhyaya ✉ supadhyaya@ra.ac.ae

Introduction

The emerging defence technologies and innovations of the twenty-first century, which are rapidly proliferating, are reshaping modern warfare across all domains: air, land, sea, and cyberspace. The Indian Chief of Defence Staff, General Anil Chauhan, recently described this phenomenon as the third ongoing revolution in military affairs (RMA), led by the convergence of multiple technologies "combining first and second-generation warfare with the third (Singh, 2025)." This statement essentially implies that the introduction of newer technologies has not only created new challenges but also rather than leading to the obsolescence of older systems; the ongoing RMA has, instead, spawned a series of hybrid systems that are more complex and lethal. Some key emerging technologies already in use or in various stages of adoption by leading militaries include artificial intelligence, lethal autonomous weapons, hypersonic/precision-guided weapons, directed energy weapons, biotechnology, and quantum technology (Congressional Research Service, 2024, p. 2). Many of these technologies are the result of major scientific advances that extend military capabilities, creating new opportunities for military applications but also huge challenges for national and global security.

A study of recent conflicts worldwide provides valuable insights into the impact of emerging defence technologies. Evidently, the new military technologies have demonstrated revolutionary capabilities that seem to be fundamentally altering the nature of conflict, calling for a review of the extant military doctrines and strategies. While the fundamental nature of war *per se,* as defined by Clausewitz — "an extension of politics by other means" — remains unchanged, the introduction of these emerging military technologies could have wider geostrategic ramifications. This paper seeks to examine the overall impact of the ongoing development of various innovative defence technologies based on case studies of the Armenia-Azerbaijan conflict, the ongoing Russia-Ukraine war, and the recent India-Pakistan clashes following a terrorist attack in Kashmir, India. The paper proceeds as follows. Firstly, it provides an overview of the emerging defence technologies. Next, it examines the three recent conflicts to identify and analyse key emerging defence technologies and innovations that were used and their operational impact on the battlefield. Subsequently, the paper discusses the overall impact of these technologies, explaining how rapid innovation and adaptation cycles influence military effectiveness in contemporary conflicts and outlining key lessons learnt. Finally, the paper concludes with likely future trends that could redefine modern conflicts.

Emerging Defence Technologies

Artificial Intelligence (AI)

As is widely known, there are three types of AI: narrow AI, general AI, and artificial superintelligence. While the latter two types of AI are not yet ready, narrow AI capable of performing specific tasks has been adopted by several leading militaries. Narrow AI has been demonstrated across multiple military applications, including intelligence, surveillance, and reconnaissance (ISR); logistics; cyber operations; command and control; and semiautonomous and autonomous vehicles (Congressional Research Service, 2024, p. 2).

The limitations of narrow AI, largely due to algorithmic biases, are well known, but its use in the military is expected to increase widely, as it has the potential to speed up and improve the precision of military operations. These capabilities and the inherent potential for innovation have already been demonstrated in multiple military operations across ongoing conflicts. In addition to military operations, a related area where AI technology holds immense potential is Information Warfare (IW), where AI has been used to generate deepfakes and forged photo, audio/ video content that could be used to maliciously influence and shape public discourse.

Lethal Autonomous Weapon Systems (LAWS)

The United States Department of Defence defines LAWS as follows: A class of weapon systems capable of both independently identifying a target and employing an onboard weapon to engage and destroy the target without manual human control. This concept of autonomy is also known as "human out of the loop" or "full autonomy (Congressional Research Service, 2024, p. 9)." In addition to fully autonomous LAWS, there are other types of weapon systems that allow human monitoring and supervision for target engagement — "autonomous weapons systems" — and others that require human intervention in selecting targets —" semi-autonomous weapon systems."

Obviously, humans are prone to errors just as automated systems are liable to vulnerable to failure however with a fully autonomous weapon system the risks are much higher with potential risks of "mass fratricide, with large numbers of weapons turning on friendly forces," due to "hacking, enemy behavioural manipulation, unexpected interactions with the environment, or simple malfunctions or software error (Scharre, 2016, p. 9)." While such risks can be minimised and no such cases have been observed in the extensive use of such weapon systems so far, the possibility of such disasters can never be eliminated.

Hypersonic Missiles

Are weapons that can fly at more than five times the speed of sound, or Mach 5. Some of the leading military powers, including the United States, Russia, China, and India, are known to be developing hypersonic weapons. Hypersonic weapons, compared to ballistic missiles, which also travel at hypersonic speeds, do not follow a predictable parabolic ballistic trajectory but can manoeuvre en route to their destination. This makes hypersonic missiles immune to extant missile defence system.

There are two types of Hypersonic missiles: glide vehicles launched from a rocket before gliding to the target, and cruise missiles powered by high-speed engines throughout their flight. Hypersonic missiles were used for the first time ever in combat in November 2024 when Russia's Strategic Missile Forces fired the *Oreshnik* hypersonic missiles at an industrial site in Dnipro, Ukraine. The Ukrainian military officials said the missile reached a speed of Mach 11 and reportedly President Putin compared the missile strike to a "meteorite" striking the target (AP News, 2024).

Directed Energy (DE) Weapons

Directed energy weapons (DEWs) use highly focused electromagnetic energy, rather than kinetic energy, to damage or destroy enemy equipment by heating, melting, or disrupting electronic systems. DEWs can be used to counter drones, missiles, and other airborne threats, as well as land- and sea-based targets. DEWs offer advantages such as high speed, or rather the speed of light, precise targeting as compared to other kinetic ordinance, since light is practically immune to the effect of gravity or atmospheric conditions (though light dispersion/ scattering affects its range), and much lower cost per shot with almost limitless firing capability as long as the weapon's power supply is available.

Furthermore, another key tactical advantage is that DEWs are discreet and silent, as radiation does not produce sound and is almost invisible. However, DEWs are also limited in range by atmospheric absorption and scattering, as well as by adverse weather conditions such as fog, rain, and dust storms, which can affect the laser beam's intensity and reduce their effectiveness. DEWs have been in use for a few years and were first used by the US military during the Iraq War to disrupt and destroy Iraqi electronic systems.

Precision Guided Munitions (PGMs)

Also known as Smart Bombs, are guided munitions intended to hit a target, whether stationary or moving, with extreme precision and minimise secondary and collateral damage. PGMs incorporate a guidance system, a payload, and steering fins. The guidance system will usually communicate with the fins to steer the PGM towards the intended target, effectively turning an unguided or "dumb" bomb into a smart bomb. Well-known precision-guided munitions are:

- Radio-controlled bombs
- Electro-optical bombs
- Infrared-guided bombs
- Laser-guided bombs
- Radar-guided bombs
- Satellite-guided bombs (EDGE, 2023)

Although the use of guided weapons can be traced back to World War I, technological developments, such as lasers and semiconductors, have led to major advancements in missile guidance, resulting in far greater accuracy. Today, the term "precision" is used to not just describe a particular guidance technology or some military standard in accuracy, but rather as a generic term that implies the ability to strike targets with near pinpoint accuracy based on superior "intelligence, planning and decision making" that underpin the use of such weapons in modern conflicts.

Others

In addition to the above technologies, biotechnology and quantum technology hold significant promise for military applications. Biotechnology is essentially based on leveraging life sciences for various technological applications, including use in the military, in areas such as "biological weapons, genome editing, or more invasive forms of human performance modification (Congressional Research Service, 2024, p. 21)." Quantum technology, based on the principles of quantum physics, could create game-changing military technologies, such as encrypted communication, submarine detection, and satellite-free navigation systems (Rana, 2025). However, these applications are mostly futuristic, as developments in quantum technologies are still in their nascent stages.

The Application of Emerging Military Technologies in Recent Conflicts

This section examines the use of emerging military technologies in contemporary conflicts to understand how such developments are shaping the modern battlespace and military doctrine and strategy.

The Nagorno-Karabakh War

The Second Karabakh War between Azerbaijan and Armenia, which has officially just ended with the signing of a Peace Treaty in August 2025 at the White House, involved a forty-year-old dispute over the region of Nagorno-Karabakh and surrounding territories. The war that lasted just six weeks will go down in history as the first major conflict involving an effective use of drone technology to achieve a swift and decisive victory. The war commenced following Azerbaijan"s lightning offensive on 27 September 2023 and ended on 10 November 2023 in a cease-fire brokered by Russia with the occupation of Nagorno-Karabakh by Azerbaijan. By January 2024, the ethnic Armenian enclave was officially dissolved, and over 100,000 people, almost all of Nagorno-Karabakh's ethnic Armenian population (Center for Preventive Action, 2025), fled to Armenia.

Azerbaijan's decisive victory over Armenian forces showcased the power of unmanned aerial vehicles (UAVs) for precision strikes and tactical dominance. Prior to the war, both sides had modernised their armed forces, with Armenia largely investing in an inventory of Russian-origin missiles/ rockets, such as the vintage *Tochka* and *Scud* missiles received from the former Soviet Union and the *Iskander* missiles from Russia in 2016. In contrast, Azerbaijan, flush with funds from oil and gas sales over the past decade, built an impressive arsenal of drones such as the Turkish *Bayraktar* TB2 drones and Israeli-made *Harop* loitering munitions, also known as “suicide” or “kamikaze” drones. During the war, in a remarkably effective tactic, Azerbaijan also used modified Soviet-era AN-2 Colt biplanes fitted with remote-control systems, as unmanned “bait drones” or decoys, flying them to the front lines to draw out Armenian air defences. This is an example of convergence between emerging military technologies and legacy platforms to produce a new, highly effective, or “smart” type of weapon system.

By all accounts, the Azeri drones inflicted huge losses on the Armenian side. Although the exact numbers of military equipment losses and soldiers killed on both sides vary widely, according to one report:

> Azerbaijan’s UAVs obliterated Armenia’s formidable array of ground-based air defences, after which they systematically decimated Armenia’s ground force matériel, including tanks, artillery pieces, and supply trucks. This onslaught forced Armenia to accept a humiliating ceasefire imposed by Russia…It can be said that this was the first postmodern conflict, in that it was the first in which unmanned-aircraft overwhelmed a conventional ground force, grinding it down to the point of impotence and paving the way for the Azeri ground forces to roll in and take possession of a strategic chokepoint (Rubin, 2020, pp. 4-5).

Based on the above account, it may seem that the Azeri drones alone swung the war in Azerbaijan’s favour; however, it is important to note that the same results could also have been achieved by a superior air force. Clearly, Armenia’s weak air defence was the cause of this outcome. According to one report, the Azeri forces faced stiff resistance in the initial days but soon wore down Armenian air defence through sheer perseverance despite heavy drone losses, as Azerbaijan had many more in its inventory. In the end, the Azeri drones achieved destruction of enemy air defence (DEAD) within the initial period of the war with relatively fewer soldiers lost.

Thus, an important lesson from this war was that UAVs can potentially play the traditional roles carried out by manned aircraft, such as intelligence gathering, surveillance, reconnaissance, target identification, and direct strikes, at a fraction of the overall cost and perhaps, more importantly, far lower risk - thus offering asymmetric airpower advantage to a military without a powerful air force. However, it is crucial to have UAVs in large numbers as the Azeri forces did. Evidently, manned aircraft are designed with far more robust countermeasures than unmanned drones, which are generally seen as disposable in war and, as a result, require a large inventory.

The Russia-Ukraine War

The ongoing Russia-Ukraine conflict that began with a full-scale attack by Russian forces in February 2022 has demonstrated many “cutting-edge” military technologies, as well as the use of legacy equipment, including heavy armour and artillery, in the various military operations that have been conducted by both sides. The veracity of these technologies, particularly

AI, unmanned aerial vehicles (UAVs)/drones, and precision-guided munitions, and their impact on military strategy, are being keenly watched – notwithstanding the political condemnation of Russia for starting the war - by not just all militaries around the world but also the defence industry, and offer many important lessons to be learnt. In many ways, the war has become a test bed for emerging military technologies being employed in ongoing operations.

The war began with Russian forces advancing on multiple axes into Ukraine in a "blitzkrieg campaign," led by heavy armoured vehicles and artillery, which advanced quickly to cover up to 250 kilometres along an axis towards Kyiv. However, thereafter, Russia seems to have resorted to a strategy of attrition warfare to strike at the Ukrainian military and consolidate territory. During this period, Russia relied on "dismounted infantry that resorted to killing and wounding Ukrainian soldiers (Jones & McCabe, 2025)" amid reports of war crimes committed by Russian troops in several towns and cities. Russia also employed glide bombs, drones, cruise and ballistic missiles, and artillery fire to carry out stand-off attacks mainly on multiple military and industrial targets inside Ukraine.

Three years later, while Russia continues to retain the initiative and has made significant land gains, it has paid a heavy price in terms of losses, and the subsequent pace of advance has been slow (Watling et al., 2024). According to estimates, Russian forces have advanced at speeds as slow as 50 to 135 metres per day in several locations, much slower than many pitched campaigns of the WW II. Furthermore, since January 2024, "Russia has lost roughly 1,149 armoured fighting vehicles, 3,098 infantry fighting vehicles, 300 self-propelled artillery, and 1,865 tanks," with about one million killed or wounded (Jones & McCabe, 2025).

A study by CSIS indicates that this number of Russian fatalities is "15 times larger than the Soviet Union's decade-long war in Afghanistan and 10 times larger than Russia's 13 years of war in Chechnya (Jones & McCabe, 2025)." The inordinately large number of casualties could be attributed to the Russian tactics of using dismounted infantry troops, in small squads, including poorly/ hurriedly trained recruits. Significantly, Ukraine has also lost about 400,000 personnel (including killed and wounded).

While Russia's offensive attacks progressed slowly, Ukraine's response was slow but later picked up pace, with some success. Significantly, based on Western technology platforms such as Palantir and Project Maven, Ukraine has actively integrated AI in military operations. This capability was demonstrated by effectively integrating real-time data from satellites, UAVs, and open sources to generate targeting data for precision strikes on Russian units (Bendett, 2025). A major success achieved by Ukraine in the initial months of the conflict was the sinking of the Russian naval ship *Moskva* on 13 April 2022. Ukrainian forces launched a swarming attack on the Moskva with drones that seemed to have confused the crew while scoring a direct hit on the ship with two R-360 Neptune anti-ship cruise missiles. Evidently, the ship's robust multi-layered air defence systems failed to stop the attacks as the crew was distracted and overwhelmed by the speed of the attack. Significantly, the Moskva was the largest naval ship to be sunk since WWII, a morale booster for Ukrainian forces.

Another attack by Ukraine was Operation *Spiderweb,* wherein a surprise simultaneous drone attack launched from trucks cleverly designed as civilian cargo vehicles on five major Russian air bases destroyed/ damaged 41 aircraft, including strategic bombers, amounting to an estimated $7 billion in losses (Institute for the Study of War, 2025). Reportedly, the attack – called Russia's "Pearl Harbour"– was conducted in utmost secrecy, overseen by President Zelensky personally, and has been the most audacious unconventional strike so far in the war. Pertinently, while this attack is reported to have destroyed virtually one-third of Russia's extant long-range bomber inventory, that too at locations deep inside Russia and over 2000 kilometres from Ukraine, there was no loss of lives in the operation *per se* (Jensen, 2025).

On balance, the war so far has clearly resulted in an inordinately large number of casualties and massive losses of military equipment not seen since WWII. It is also the first major war to involve both legacy military hardware, such as heavy armoured vehicles and artillery, and the latest technologies, such as drones and hypersonic missiles. Evidently, the huge losses reported are the result of employing legacy military doctrine and tactics in the face of emerging technologies such as AI, autonomous platforms, and precision-guided missiles. This calls for an urgent revision of the extant military doctrine and tactics.

The India-Pakistan Conflict

Following a terrorist attack on 22 April 2025 that killed 26 tourists in Pahalgam, in the North Indian state of Kashmir, India, in an operation codenamed Operation *Sindoor, the Indian government* launched punitive strikes on Pakistan on 7 May 2025. In the initial strike, the Indian Air Force hit nine major terrorist camps known to be linked to terrorist outfits such as the Jaish-e-Mohammed *(JeM), Lashkar-e-Taiba (LeT),* and *Hizbul Mujahideen* located in civilian-populated regions of the disputed parts of Kashmir in Pakistan.

The strikes were carried out with precision munitions based on accurate targeting intelligence and reportedly resulted in minimal collateral damage (Public Information Bureau, 2025). With this began a four-day conflict between the two rival nuclear states from 7 – 10 May, setting a new precedent in India's military response to cross-border terrorism. Significantly, the brief clashes saw the use of precision-guided cruise missiles such as the *Brahmos* missiles (jointly developed via Indo-Russian military collaboration) and French-made SCALP-EG smart bombs by India, and short-range ballistic missiles such as *Fatah* 1 and II, by Pakistan; in addition to extensive drone attacks by both sides (Clary, 2025).

In the end, the two sides declared victory amid considerable fake news about what occurred with the social media streaming deep fakes depicting fabricated images of airplanes downed. The conflict ended when, according to the Indian side, the Pakistan Army requested a ceasefire following precision strikes at a probable nuclear site at the Nur Khan air base located near Islamabad.

While there have been several varying accounts of what really happened during the four-day war, certain conclusions can be made. Firstly, the conflict demonstrated India's capability to carry out standoff attacks on a wide swath of territory inside Pakistan using Smart Bombs that could be launched from Indian airspace to glide onto targets hundreds of kilometres inside Pakistan. This is an important capability that did not exist until recently, thanks to the acquisition of new military technologies such as precision-guided missiles and smart bombs. In the past, India responded to similar terror attacks from Pakistan by conducting "surgical strikes" by special forces.

While such strikes had been successful in achieving limited tactical objectives, they were highly risky. Several potential scenarios by security analysts included situations wherein a repeat surgical strike by Indian special forces is ambushed by a group of a terrorist group that brutally eliminates the Indian soldiers, leading to a huge public outcry for revenge. And with domestic pressure building, the government is forced to declare war against Pakistan, which quickly escalates to a nuclear conflict. Such scenarios appear very realistic given the region's overall security environment. However, the successful demonstration of drone and precision strike operations from stand-off ranges during Operation *Sindoor* clearly indicates that the potential risk from at least such scenarios is greatly reduced.

Secondly, while there is no evidence that the air force planes from either side crossed over into each other's airspace, both sides have claimed shooting down several planes, particularly on social media, using what appear to be fake images and videos. For instance, the Indian air force announced that five Pakistan air force jets, including one possible AWA&C, were shot down, while the Pakistan side maintains that five Indian air force jets, including three Rafale jets, were downed. Thirdly, India's integrated air and missile defence system appears to have defeated several waves of Pakistani air attacks by drones and ballistic missiles with little damage reported on the ground in India. Thus, a key lesson from this conflict is that a sophisticated, fully integrated air defence system is the best countermeasure against relatively cheap drone attacks. Another lesson that emerges is that the clever use of deepfakes to spread misinformation can be an effective strategy for shaping a false narrative that seems to have a lasting impact.

Impact of Emerging Military Technologies

Based on the above case studies, this section examines the overall impact of emerging defence technologies to explain how rapid innovation and adaptation cycles, as witnessed in leading militaries, are influencing future military force structures, doctrines, and strategy.

Hybrid Approach

A few clear trends can be discerned. Firstly, most militaries seem to have adopted a hybrid approach to various new acquisitions. Thus, while most militaries continue to induct and upgrade their extant inventory of platforms, weapons, and sensors — such as fighter planes, ships, and missiles —they are also investing in newer systems based on emerging technologies, such as autonomous systems and drones for use in air, land, and sea. Evidently, this approach helps balance costs and maintain operational continuity and flexibility, leveraging previous investments, including training and repair/maintenance facilities.

Clearly, replacing the existing inventories of most large platforms — such as tanks, armoured vehicles, fighter planes, and ships, including minor craft/boats — is not only expensive but also poses significant logistical challenges. Thus, upgrading/ outfitting various legacy systems – with some exceptions of certain platforms and equipment that may have become truly obsolete or ineffective - with newer technologies such as advanced weapons and sensors and AI software makes legacy platforms "smarter" while retaining their core capabilities. In the long term, this is very cost-effective and allows militaries to extend the usefulness of existing equipment.

As a result of these developments, militaries are now employing several "smart" or upgraded platforms alongside legacy equipment in a hybrid mode. For instance, as noted earlier in the paper, during the second Nagorno-Karabakh War, the Azeri forces employed modified Soviet-era AN-2 Colt biplanes with remote-control systems, as unmanned "bait drones" or decoys to locate Armenian air defences. Similarly, there are reports that the Indian Air Force is planning to convert its retired Soviet origin MiG-21 *Bison* fighters – once the backbone of India's air defence - into UAVs for employment in various roles such as targets, decoys, communication relays, and Kamikaze missions (IDRW, 2025). Furthermore, some of the latest military operations in the ongoing Russia-Ukraine War, such as the use of high-speed boats modified for use as unmanned sea drones by Russia to sink Ukraine navy's largest ship, the *Simferopol,* on 28 August 2025, are examples of the new form of hybrid operations.

Significantly, the use of sea drones had been demonstrated by Ukraine on several occasions during the war to target Russia's Black Sea Fleet, including the flagship *Moskva*, the largest naval ship sunk since WWII. These are examples of successful hybrid operations that use legacy platforms integrated with advanced software deployed in digitally managed battlefield networks—a new normal in military warfare. As a result of these technological improvements, the evolving battlespace is now characterised as a "hybrid" space, featuring a synergetic mix of legacy equipment and "smart" or customised platforms that leverage autonomous control systems, advanced sensors, and artificial intelligence.

Enhanced Decision Making – The Super OODA Loop

In addition to the hybridisation of the battlefield, the advent of AI-enabled systems is also reshaping military operations and decision-making in profound ways. Evidently, the technological advancements of the twenty-first century, particularly rapid progress in intelligence, surveillance, and reconnaissance (ISR) systems, have led to an information overload. This has made modern warfare, already a complex business, far more intense, fast-paced, and difficult for human decision-making to keep up with the tempo of operations.

As a result, military commanders, who must often make split-second decisions in the prevailing "fog of war" to outmanoeuvre their adversaries in increasingly complex situations on saturated battlefields, may find themselves swamped with information. For instance, real-time footage from drones and space-based systems continuously streaming into an operations room could be humanly impossible to interpret or analyse. However, AI systems could sift through enormous amounts of data to generate actionable intelligence and guide unmanned drones or missiles to enemy targets, as demonstrated, for instance, by Ukraine during Operation *Spiderweb*.

These functions are also the basic elements of the OODA Loop – a four-step decision-making model (developed by military strategist John Boyd) to "Observe, Orient, Decide, Act." Essentially, the OODA Loop is a continuous cycle for making quick decisions in a dynamic environment: processing information, deciding, acting on it, and then observing the results to start the process over again. The goal is to outpace the enemy through the loop to dominate the battlefield. Thus, AI has the capability to enhance "the pace, accuracy, and adaptability of military operations in ways previously unimaginable (Raska, 2025)," transforming the traditional "OODA Loop" cycles into an automated, high-speed decision-making process, enabling near-instant responses through machine-to-machine interface or the Super OODA Loop (Raska, 2025).

The future "Super OODA" Loops will be increasingly AI-driven, highly autonomous, and operate on near-instantaneous timelines that far exceed human response speeds. While it is likely that automated decision-making processes in fast-paced military operations will raise ethical and legal challenges, posing questions of accountability and human control, it is also highly probable that solutions to these issues will evolve organically over time. Likely ongoing developments – demonstrated in military operations such as *Spiderweb* - could include real-time integration of ISR data using AI, machine learning based decision-making, adapting to enemy tactics in near real-time, and autonomous decision-making and targeting/ interceptions – based on preset protocols bypassing human oversight (Raska, 2025).

Low Collateral/ Secondary Damage Through Precision Strikes

Another major development in the ongoing RMA has been the advent of precision-guided munitions from standoff ranges with minimal collateral/ secondary damage. This capability was most recently demonstrated by the Indian Air Force during Operations *Sindoor*. Such precision strikes enable achieving military objectives with minimal force and low risk, as engagements are conducted from stand-off ranges. Furthermore, such strikes delivered with lightning speed help to achieve surprise – a key principle of war. Evidently, such swift strikes achieve "shock and awe" by dominating the battlefield and paralyzing the adversary's decision-making in the initial stages of the conflict. In the end, this greatly reduces the likelihood of long, drawn-out wars, as observed in the India-Pakistan conflict, which ended with a ceasefire within four days of its start. Although there is no guarantee that all such conflicts will not escalate.

A key military advantage of precision munitions is that such attacks can be carried out by small teams of networked missile battery units equipped with advanced sensors, including drone feeds, and managed by digital command and control systems, without the need for mass mobilisation of forces. Crucially, these technologies enable militaries to project power over long ranges, deep into enemy territory, as demonstrated by the strikes carried out by the Indian Air Force in May 2025. This capability allows limited-area operations, confining the conflict to specific areas, though the prospect of the conflict escalating into a wider war can't really be ruled out. Overall, these capabilities enable short wars in limited geographic areas, as seen in the recent India-Pakistan conflict, and could therefore lead to an increased frequency of such conflicts.

Newer Types of Military Equipment

In addition to the changes discussed above, emerging technological developments are also driving the development of entirely new systems and ushering in a new generation of platforms, weapons, and sensors that could eventually replace several legacy systems. For instance, recently, the Royal Navy unveiled its first uncrewed submarine, a 12m experimental vessel, displacing 19 tonnes named *Excalibur* (Royal Navy, 2025). Reportedly, the vessel will undergo extensive sea trials, aimed at helping the navy develop a deeper understanding of operating uncrewed vessels of this size and prepare for future operations alongside legacy submarines and ships. Similar acquisitions are known to be underway in other navies around the world.

Another example of a new generation of platform is the Drone Carrier that could potentially replace the traditional Aircraft Carrier. These Drone Carriers are being acquired by leading world navies, including the Türkiye Navy, the Italian Navy, and the Japanese Navy, which are currently modifying aircraft carriers and large amphibious ships to operate a mix of fixed-wing aircraft, helicopters, and drones. The use of such modified platforms capable of operating a mix of fighter planes and drones is a recent development and adds a new dimension to hybrid strike capability at sea.

In addition to the above platforms, a new generation of diverse weapons is being trialled and introduced into leading militaries. Some examples are the Russian intercontinental, nuclear-armed, nuclear-powered, autonomous torpedo *Kanyon*; the 3M22 *Zircon* hypersonic cruise missile; laser-directed energy weapons (LDEWs) undergoing sea trials in the UK and the United States; and the shipborne rail gun now being fitted to modern warships in several leading world navies. The history of warfare shows that every weapon system eventually has a countermeasure. Thus, it is likely that each new emerging weapon system will eventually be countered by superior technology.

For instance, the answer to hypersonic anti-ship missiles and drones probably lies in LDEWs, and the nuclear-powered autonomous torpedo, like the Kanyon, could be countered by equally smart autonomous underwater drones acting as decoys. However, the jury is still out on the veracity of such technologies, which remain to be convincingly proven in war, particularly against significant advances in ship self-defence measures. Modern militaries must adapt their extant doctrines, training, and force structures to integrate these technologies for speed and flexibility. Overall, while the militaries of the world are currently undergoing a period of transition with the introduction of new technologies, it is likely that in the long term, the successful induction of such technologies may lead to their complete transformation with an entirely new generation of unmanned technologies that may replace the traditional platforms, weapons, and sensors.

Strategic Implications of Emerging Defence Technologies

Based on the above analysis of the impact of emerging defence technologies, it is likely that states may be tempted to initiate short, limited conflicts or wars to resolve outstanding issues. Collectively, the various emerging defence technologies discussed above seem to create a strategic perception that wars can now be fought with greater precision and greater control over escalation, with commensurately less human risk and economic cost. Thus, states may now believe that military action can be confined to short, sharp interventions rather than protracted campaigns.

The recent India-Pakistan conflict discussed above and the latest attacks by the Israel Defence Forces (IDF) on September 9, 2025, in the Leqtaifiya district of Qatar's capital Doha, aimed at eliminating key Hamas operatives, are clear examples of how states may wish to conduct strategic operations to resolve issues. According to the ACLED Conflict Index, the number of Global Conflicts has doubled over the past five years (ACLED, 2025). Another dataset shows that the number of interstate conflicts, largely over territory, land, and border integrity, which had reduced since 1980, has risen sharply since 2010.

Despite the promise of the latest defence technologies for localised or controlled violence demonstrated in multiple conflicts, the reality remains fraught with danger. Evidently, while it is true that attacks by unmanned drones and precision strikes by missiles can limit secondary or collateral damage in each engagement, there is no guarantee that such attacks, in large numbers or spread over multiple targets, could not lead to indiscriminate or mistaken targeting, raising difficult questions of legal and moral responsibility. Furthermore, it is likely that AI-accelerated decision cycles leading to the Super OODA loop to control military operations could trigger rapid escalation due to the resulting loss of human oversight, which should ideally guide all military operations.

Conclusion

The above analysis of emerging defence technologies and their application in contemporary conflicts unambiguously demonstrates that these technologies are redefining military strategy and operational doctrines globally. Given the case studies of recent conflicts —such as the

Nagorno-Karabakh War, the ongoing Russia-Ukraine War, and the recent Indo-Pakistani conflict —where the use of such technologies, including autonomous systems, precision-guided weapons, and hybrid platforms, has been amply demonstrated, the following lessons emerge. First, the gradual integration of drones, smart munitions, and autonomous systems enhances operational efficiency while reducing risks to combatants and civilians. This capability of modern militaries to conduct long-range precision strikes, supported by real-time data and AI-accelerated OODA loops, has been demonstrated, though the veracity of such systems in the face of evolving countermeasures remains to be seen. However, the success of the systems seems to have created an illusion of control and speed for decision-makers, fostering a temptation by states to use force to resolve disputes, driven by the belief that conflict can be contained, short, and low-cost.

Second, the fusion of old systems and new technologies in a hybrid approach pushes the boundaries of traditional military doctrines, as armies adapt structures and operations to incorporate "intelligent" heterogeneous platforms, blurring the lines between conventional and asymmetric warfare. This hybridity becomes a major asset for flexible and reactive responses to the growing complexity of modern battlefields. Third, while new technologies offer clear opportunities for resource saving, precision, and loss minimization, they also raise significant ethical, legal, and strategic challenges.

It is likely that accelerated decision-making and increasing automation could increase the risk of uncontrollable escalation, and importantly, misidentification errors – however rare - can have major consequences for legitimacy and compliance with international laws of armed conflict that require human oversight. Furthermore, the proliferation of these technologies to non-state actors and mid-sized and even small powers threatens a cascade of localized but frequent conflicts, fuelling regional and international instability.

In summary, the emergence and rapid integration of next-generation defence technologies necessitate a redefinition of doctrines and an adaptation of national and international strategies. The modernity of the battlefield, dominated by speed, connectivity, and precision, demands not only technological responses but also deep reflection on ethical principles, political responsibility, and international cooperation to regulate the use and proliferation of such weapons. This doctrinal renewal will be crucial to ensure that military innovation translates not only into increased power but also into long-term collective international stability and security.

Disclaimer

The author declares no potential conflict of interest related to the article. No artificial intelligence content generation tools were used in its preparation.

Funding

The author does not declare any source of funding for this article.

About the author

Shishir Upadhyaya is a Commander (Retired) of the Indian Navy. Ph. D. in International Relations and Security Studies, University of Wollongong, Australia. M.A. in Defence and Strategic Studies, Madras University. M.A. in Telecommunication, Cochin University of Science & Technology, Kerala. Associate Professor at Rabdan Academy, Abu Dhabi, United Arab Emirates

https://orcid.org/0000-0001-6255-7531 - supadhyaya@ra.ac.ae

References

ACLED - Armed Conflict Location & Event Data Project. (2025). *ACLED Conflict Index*. https://acleddata.com/series/acled-conflict-index

Bendett, S. (2025). *Roles and implications of AI in the Russian-Ukrainian conflict*. Center for a New American Security. https://tinyurl.com/ycdy2ywk

Center for Preventive Action. (2025). *Tensions between Armenia and Azerbaijan*. https://tinyurl.com/52pu793r

Rubin, U. (2020). *The Second Nagorno-Karabakh War: A Milestone in Military Affairs*. Center for Strategic Studies. https://tinyurl.com/7v6pyh8c

Clary, C. (2025). *Four days in May: The India-Pakistan crisis of 2025*. Stimson. https://tinyurl.com/4kytwwc9

Congressional Research Service. (2024). *Emerging military technologies: Background and issues for Congress*. https://tinyurl.com/2hb5pfm2

EDGE Group. (2023). *Precision guided munitions: Behind the technology that made bombs go from "dumb" to smart*. https://tinyurl.com/bawa8sct

Jones, S. G., & McCabe, R. (2025). *Russia's battlefield woes in Ukraine*. CSIS Brief. https://tinyurl.com/s5j5npp

Raska, M. (2025). *Will AI-driven "Super-OODA Loops" revolutionise military strategy and operations?* RSIS. https://tinyurl.com/5njfbst6

Rubin, U. (2020). *The second Nagorno-Karabakh war: A milestone in military affairs*. The Begin-Sadat Center for Strategic Studies. https://tinyurl.com/4hfxkfk2

Scharre, P. (2016). *Autonomous weapons and operational risk*. Center for a New American Security. https://tinyurl.com/yd8asw82

Jones, S. & McCabe, R. (2025). Russia's Battlefield Woes in Ukraine. CSIS Brief. https://tinyurl.com/s5j5npp

Jensen, B. (2025). *Ukraine's Operation Spider Web destroyed more than aircraft – it tore apart the old idea that bases far behind the front lines are safe*. https://tinyurl.com/yevu9rsu

Singh, M. (2025). Operation Sindoor continues, military preparedness has to be very high: CDS Anil Chauhan. https://tinyurl.com/4zmssnnw

Rana, J. (2025). *Quantum startup QuBeats wins Rs 25 crore govt grant to build GPS-free navigation for Indian Navy*. https://tinyurl.com/5n9by23u

Watling, J., Danyluk, O. & Reynolds, N. (2024). *Preliminary Lessons from Ukraine's Offensive Operations, 2022-2023*. Royal United Services Institute. https://tinyurl.com/4vuetrjw

AP News. (2024, December 9). *Russia has used its hypersonic Oreshnik missile for the first time. What are its capabilities?* https://tinyurl.com/2p8xvupx

Royal Navy. (2025, May 15). *Royal Navy unveils 12 metre uncrewed submarine named after Excalibur*. https://tinyurl.com/2xffbh45

Public Information Bureau (PIB) (2025, May 18). *Operation SINDOOR*. https://tinyurl.com/v2ryxjs6

IDRW. (2025, August 18). *Should the IAF convert retired Mig 21 Bison fighters into UAVs?* https://tinyurl.com/5eykhvaa