EXPLAINERS

How Do Counter-Drone Systems Work? Jammers, Interceptors and Air Defence Explained

Author: CNAWS Research Team • **Published:** October 24, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

The evolution of air defence has historically been driven by the need to counter increasingly sophisticated aerial threats. From anti-aircraft artillery during the First World War to radar-guided missiles and integrated air defence networks during the Cold War, defensive technologies largely evolved to intercept expensive, high-performance aircraft and missiles. The proliferation of inexpensive unmanned aerial systems has challenged this established architecture. Small drones, loitering munitions and long-range one-way attack drones have introduced threats that are difficult to detect, increasingly capable of operating autonomously and economical to employ in large numbers. Consequently, modern air defence faces not merely a technological challenge, but an increasingly significant problem of operational and economic sustainability.Counter-drone systems have emerged as a critical component of contemporary air defence, combining radar, electro-optical sensors, radio-frequency detection, electronic warfare, kinetic interceptors and directed-energy weapons. However, no single technology offers comprehensive protection. Radio-frequency jammers can disrupt drone communications, but autonomous and fibre-optic-controlled systems can reduce their effectiveness. Conventional surface-to-air missiles remain capable of intercepting suitable drone threats, although their cost and limited inventories constrain their employment against inexpensive targets. Interceptor drones, radar-guided guns, high-energy lasers and high-power microwave weapons offer alternative defensive options, each with distinct operational limitations.The Russia–Ukraine war has demonstrated how rapidly offensive drones and defensive countermeasures are evolving, particularly through improvements in navigation, propulsion, autonomy and interception technologies. India's experience during Operation Sindoor in May 2025 similarly underscored the importance of integrating specialised counter-UAS

> *capabilities with conventional air defence networks. The central strategic assessment is that the future of counter-drone warfare will depend less on the superiority of any individual weapon and more on the effectiveness of layered, interoperable and economically sustainable defensive architectures. As unmanned systems become more autonomous, numerous and technologically adaptable, the ability to detect, classify and neutralise threats at scale, while continuously adapting to emerging technologies, will increasingly determine the effectiveness of modern air defence.*

The emergence of drones as a major instrument of modern warfare has exposed a fundamental weakness in the architecture of air defence. For nearly a century, air defence systems evolved around the assumption that airborne threats would be relatively expensive, technically sophisticated and limited in number. Whether the threat came from strategic bombers, fighter aircraft, cruise missiles or ballistic missiles, the underlying objective remained broadly consistent. Detect the incoming threat, establish its identity, track its trajectory and destroy it before it reaches its target.

Unmanned aerial systems have complicated this calculation. A relatively inexpensive drone can threaten an aircraft worth millions of dollars, disrupt operations at a military installation or damage strategically important infrastructure. Large numbers of drones can also force defenders to expend costly interceptor missiles, creating an economic imbalance even when most incoming aircraft are successfully destroyed. The problem is no longer simply whether an air defence system can intercept an aerial threat. It is whether it can continue intercepting threats at the scale, frequency and cost imposed by the attacker.[1]

The Russia–Ukraine war has brought this challenge into sharp focus. Russia's employment of Iranian-designed Shahed drones, subsequently adapted and manufactured domestically as the Geran family, has forced Ukraine to develop defensive arrangements involving conventional surface-to-air missiles, electronic warfare, mobile gun teams, acoustic sensors and increasingly specialised interceptor drones. The struggle has become a continuous technological competition in which every improvement in detection or interception encourages corresponding changes in drone guidance, propulsion and employment.[2]

Understanding counter-drone technology, therefore, requires more than examining jammers, anti-drone guns or laser weapons in isolation. It requires tracing the historical development of air defence, understanding why conventional systems face difficulties against modern drones and examining how emerging counter-unmanned aerial systems are being integrated into broader defensive networks.

From Anti-Aircraft Guns to Integrated Air Defence

The origins of modern air defence lie in the First World War, when military aircraft began moving beyond reconnaissance into artillery observation and bombing. Armies responded by adapting artillery weapons to engage airborne targets. These early anti-aircraft systems were constrained by the difficulty of predicting an aircraft's future position. Gunners had to account for altitude, speed, direction and the time required for a projectile to reach its target. Because aircraft could change course during this interval, effective interception required considerable estimation and coordination. During the interwar period, improvements in mechanical fire-control computers, acoustic detection, searchlights and anti-aircraft artillery strengthened defensive capabilities. Nevertheless, aircraft were becoming faster, flying higher and carrying increasingly destructive payloads. By the Second World War, it was evident that individual anti-aircraft batteries could not provide an adequate national defence without a coordinated system for detecting and responding to approaching formations. Britain's experience during the Battle of Britain in 1940 marked a decisive transformation. The Chain Home radar network, integrated with Royal Observer Corps reporting, command centres and Royal Air Force fighter squadrons through the Dowding System, allowed British commanders to identify approaching German aircraft and direct available fighters towards them. The significance of this development extended beyond radar

itself. Britain had connected detection, information processing, command decisions and interception into a functioning defensive network. Air defence was becoming an integrated system rather than a collection of independent weapons.[3]

The arrival of jet aircraft and guided missiles after the Second World War brought another transformation. Conventional artillery became progressively less suitable for intercepting increasingly fast and high-altitude aircraft. Surface-to-air missiles offered a means of extending interception range, altitude and accuracy. The American Nike-Ajax system, operational from December 1953, represented an early example of radar-guided surface-to-air missile defence. The Soviet Union subsequently developed systems such as the S-75 Dvina, known to NATO as the SA-2 Guideline. Its ability to threaten aircraft operating at exceptionally high altitudes was demonstrated when a Soviet SA-2 brought down an American U-2 reconnaissance aircraft on 1 May 1960.?

By the 1960s and 1970s, air defence increasingly combined surveillance radars, tracking radars, surface-to-air missiles, interceptor aircraft, anti-aircraft artillery and centralised command-and-control networks. Rather than depending on a single interception method, militaries began employing weapons with different engagement ranges and altitude envelopes. The 1973 Arab–Israeli War demonstrated the effectiveness of dense surface-to-air missile and anti-aircraft networks against conventional airpower. Egyptian and Syrian missile systems significantly constrained Israeli aircraft, particularly during the opening stages of the conflict. Israel's subsequent operations against Syrian air defences in Lebanon's Bekaa Valley in June 1982 demonstrated the other side of the equation. Electronic warfare, intelligence, unmanned decoys and coordinated strikes could suppress or dismantle an integrated defensive network.?

These experiences reinforced two principles that remain central to air warfare. An air defence system must operate as an integrated network, and the effectiveness of that network depends on its ability to adapt to the techniques used to penetrate or neutralise it.

How Drones Disrupted the Conventional Air Defence Model

The first generation of modern military drones did not immediately overturn established air defence doctrine. Large surveillance and strike platforms, including the American MQ-1 Predator and MQ-9 Reaper, generally operated within a technological environment familiar to conventional air defence planners. Although unmanned, these aircraft could still be detected and engaged by suitable radar and missile systems.

The more consequential transformation emerged with the proliferation of smaller commercial drones, first-person-view (FPV) systems, loitering munitions and comparatively inexpensive one-way attack drones. These platforms differed considerably in size, propulsion, range, payload and operational employment. A small quadcopter conducting reconnaissance over a battlefield presents a different problem from a Shahed-type drone flying hundreds of kilometres towards an infrastructure target. A tactical FPV drone may require a defensive response within seconds, while a long-range one-way attack drone may be tracked through several layers of a national air defence network. Larger military drones may resemble conventional aircraft in their detectable characteristics. Yet these different categories collectively challenged several assumptions embedded in traditional air defence doctrine.

The first challenge concerns detectability. Small drones generally have comparatively low radar cross-sections because of their dimensions and construction materials. Their slow speeds and low-altitude flight can also complicate detection and classification in an environment containing buildings, vegetation, birds and ground reflections. Conventional surveillance radars optimised to identify aircraft moving at substantial speeds and altitudes may not provide sufficiently reliable coverage against every small drone.

The second challenge concerns numbers. Conventional military aircraft are expensive assets whose losses carry considerable financial, operational and political consequences. Small unmanned systems can be manufactured in much

larger quantities and, depending on their design, employed in missions where their destruction is anticipated.

The third challenge is economic. A defender may successfully destroy an incoming drone while spending substantially more on the interceptor than the attacker spent on the drone. Repeating this exchange over hundreds or thousands of engagements creates a problem extending beyond the immediate battlefield.

The fourth challenge concerns the drone's role within the wider targeting system. Even an unarmed drone may be dangerous if it provides targeting information to artillery, missiles or other weapons. Consequently, the threat cannot always be assessed by the size of its explosive payload. A reconnaissance drone that locates a valuable military asset may create greater subsequent damage than an individual armed drone.

Two conflicts illustrated the emerging problem before the large-scale invasion of Ukraine. The September 2019 attacks on Saudi Arabia's Abqaiq and Khurais oil facilities demonstrated how low-flying precision weapons could penetrate an apparently well-equipped defensive environment and cause strategic economic disruption. In the 2020 Nagorno-Karabakh War, Azerbaijan's combination of reconnaissance drones, armed unmanned aircraft and loitering munitions contributed to the destruction of Armenian military equipment, including air defence assets. The conflict exposed the shortcomings of defensive formations relying on ageing systems without sufficiently effective counter-drone coverage.? These developments did not render conventional air defence obsolete. Rather, they exposed gaps between the types of threats existing defensive systems were designed to counter and the increasingly diverse systems being introduced into modern warfare.

How Counter-Drone Systems Actually Work

Counter-unmanned aerial systems, commonly abbreviated as C-UAS, represent a collection of technologies designed to detect, identify, track and, when necessary, neutralise potentially hostile drones. A counter-drone system is not necessarily a weapon. A military radar capable of detecting a small quadcopter, a passive radio-frequency sensor identifying drone communications, a jammer disrupting a control link and an interceptor physically destroying the aircraft may all be components of the same defensive architecture. The fundamental principle is that detecting a drone and defeating it are separate technical problems. An effective counter-drone system must solve both, while ensuring that the response is appropriate to the threat.?

Detection and Tracking

Radar remains one of the most important detection technologies. It transmits electromagnetic energy and analyses signals reflected from objects to estimate their position, distance and movement. Specialised counter-drone radars use processing techniques adapted to smaller aerial targets. Some can exploit characteristics associated with rotating propellers to help distinguish drones from other objects. However, radar detection alone does not establish hostile intent. A small radar contact may represent a drone, bird or another airborne object. Even when a drone is positively identified, the radar cannot necessarily determine whether it is carrying an explosive payload, conducting authorised surveillance or performing an innocuous civilian activity.

Electro-optical and infrared sensors complement radar by providing visual and thermal information. High-resolution cameras can assist operators in identifying the aircraft's shape and configuration, while thermal imagers can provide useful information in low-light conditions. Their effectiveness nevertheless depends on visibility, weather, line of sight and the target's thermal characteristics. Radio-frequency detection systems operate differently. Instead of transmitting radar energy, passive RF sensors monitor relevant electromagnetic emissions associated with drone communications. Where an aircraft and its controller exchange detectable radio signals, such systems may assist in identifying the drone

type and estimating the direction of the transmission. Their principal limitation is that they depend on the presence of emissions that their sensors can recognise. Acoustic detection offers another approach. By analysing the characteristic sounds of drone motors and propellers, microphones and signal-processing software can provide warning of nearby aircraft. This is particularly useful as a supplementary sensor in environments where conventional radar coverage is difficult, although acoustic performance is strongly influenced by distance, environmental noise and weather.?

An effective counter-drone architecture therefore combines information from different sensor types rather than depending exclusively on one.

Identification, Command and the Engagement Decision

After detecting a possible drone, the defensive system must establish whether it represents an actual threat. This involves correlating sensor reports, assessing the object's movement and checking available information about authorised aircraft operating in the area. The resulting information is processed by a command-and-control system, which creates a common operational picture for the personnel responsible for air defence. Once a target is identified as hostile, the system must determine which defensive measure is appropriate. A jammer may be sufficient against a radio-controlled commercial drone, while a larger autonomous attack drone may require physical interception. The availability of different systems, the proximity of friendly aircraft, the consequences of falling debris and the importance of the protected asset all influence the response.

This is where modern counter-drone systems are increasingly using automated tracking, sensor fusion and decision-support software. Rather than requiring separate operators to interpret several disconnected radar displays and camera feeds, an integrated system can correlate available information and present a coherent assessment of the threat. The US Army's Mobile-Low, Slow, Small Unmanned Aircraft Integrated Defeat System, known as M-LIDS, illustrates this approach. During the September 2026 Yudh Abhyas exercise, the system was employed as an integrated combination of radar, electro-optical and infrared sensors, command-and-control equipment and kinetic and non-kinetic defeat capabilities.? A successful defensive engagement, therefore, is not simply a matter of destroying the drone. The system must detect it early enough, classify it correctly, assign an appropriate response and verify whether the threat has actually been neutralised.

How Drone Jammers Work

Electronic warfare systems are among the most widely used counter-drone technologies because many drones depend on electromagnetic signals for navigation, control or communication. Broadly, electronic countermeasures seek to deny or manipulate the signals necessary for a drone to perform its intended mission. A radio-frequency jammer generates electromagnetic interference intended to disrupt a drone's communication link with its operator. If the interference prevents the receiver from reliably recovering the intended control signals, the operator may lose the ability to command the aircraft. The drone's subsequent behaviour depends on its internal programming. Some commercial systems may hover, initiate an automated landing or attempt to return to a previously designated location. Others may continue operating according to a pre-programmed mission. The loss of a control link does not automatically mean that the aircraft will fall from the sky.

Satellite-navigation jamming addresses a different dependency. Drones using Global Navigation Satellite Systems, including GPS, obtain positioning and timing information from satellite signals. If these signals become unavailable or unreliable, the aircraft may experience degraded navigation performance. A more sophisticated technique is spoofing, in which misleading navigation information is introduced to cause a receiver to calculate an incorrect position or trajectory. Successful spoofing can potentially cause an aircraft to deviate from its intended route, although effectiveness depends

on the drone's receiver, navigation architecture and defensive safeguards.[1]? Modern electronic warfare systems may employ directional or broader-area interference according to their intended role. The choice involves practical trade-offs between coverage, power requirements and the risk of disrupting friendly systems.

Why Jamming Cannot Stop Every Drone

The increasing use of autonomy has weakened the assumption that disrupting a radio-control link will reliably neutralise an unmanned aircraft. An autonomous drone may follow a previously programmed route without continuous instructions from an operator. Systems equipped with inertial navigation, visual navigation or other onboard guidance capabilities may also retain some ability to navigate when satellite signals are degraded. The electronic warfare competition in Ukraine illustrates this development. Russia has repeatedly modified the navigation and communication architecture of its Geran drones, including the incorporation of more sophisticated anti-jamming satellite-navigation antennas. The September 2026 CSIS assessment of the Geran programme documented an evolving cycle in which Russia adjusted onboard technologies to counter Ukrainian electronic warfare measures.[11]

Another development is the use of fibre-optic-controlled drones. These systems transmit control information through a physical optical cable rather than depending on a conventional radio link. As a result, ordinary radio-frequency command-link jamming does not interrupt communication through the fibre. Such systems have their own operational limitations, including dependence on the integrity of the physical connection, but demonstrate how quickly attackers can adapt to established defensive techniques.

The broader implication is that electronic warfare is highly valuable but cannot be treated as a universal solution. Its effectiveness depends on the electronic and navigational dependencies of the particular drone being engaged.

Kinetic Interception and the Return of Anti-Aircraft Guns

Where electronic countermeasures attempt to interrupt the operation of a drone, kinetic countermeasures seek to physically damage, capture or destroy it. Kinetic interception encompasses conventional anti-aircraft artillery, specialised ammunition, surface-to-air missiles and increasingly, drones designed specifically to intercept other drones.

An important consequence of the drone threat has been renewed interest in short-range anti-aircraft guns. These weapons had gradually lost prominence as guided missiles became increasingly capable, but their relatively inexpensive ammunition and ability to engage targets at short range have restored their relevance. Modern anti-aircraft systems are considerably more sophisticated than their predecessors. Radar-directed guns can receive target information from external sensors and employ automated fire-control systems. Some use programmable airburst ammunition, which disperses fragments near an aerial target rather than requiring a direct projectile impact. These capabilities can be useful against small drones, although effective engagement remains dependent on target acquisition, tracking quality and the weapon's firing envelope. Ammunition expenditure, collateral damage and the danger posed by projectiles or falling wreckage also have to be considered.

Surface-to-air missiles constitute another layer. Systems originally designed to engage conventional aircraft can be effective against larger drones and certain loitering munitions, provided the target falls within their engagement capabilities. Their limitation is not necessarily an inability to destroy drones, but the efficiency of doing so. Expensive guided missiles may be justified when protecting particularly valuable assets against dangerous incoming threats. They are less economically attractive when routinely expended against very inexpensive unmanned aircraft.

Modern counter-drone doctrine therefore increasingly seeks to match the cost and sophistication of the defensive weapon with the threat it is intended to defeat.[12]

The Emergence of Interceptor Drones

One of the most significant recent developments is the employment of interceptor drones, often described as drone-on-drone air defence. These aircraft are designed to locate and physically intercept hostile drones, either through direct collision or a dedicated interception mechanism. They may receive target information from ground-based sensors and then employ onboard cameras, guidance systems or human operators to complete the engagement. The attraction of interceptor drones lies partly in their potential for relatively low-cost production. An unmanned interceptor does not necessarily require the complex propulsion, guidance architecture or warhead technology associated with a conventional surface-to-air missile.

Ukraine has demonstrated the operational significance of this approach, employing relatively inexpensive interceptor drones against Russian one-way attack aircraft. However, the emergence of faster, jet-powered Russian drones has exposed the limitations of existing interceptors. Reuters reported in September 2026 that Ukrainian interceptor drones, typically costing less than $2,000, had proved effective against many conventional Shahed-type targets but were struggling to cope with substantially faster jet-powered variants.[13]

This illustrates an important limitation. Interceptor drones should not be understood as universally cheaper replacements for missiles. They occupy a growing segment of the defensive spectrum, but their effectiveness depends on speed, guidance accuracy, reaction time, environmental conditions and the characteristics of the incoming threat. As drone propulsion and autonomy improve, interceptor technology must evolve correspondingly. The resulting competition is increasingly resembling the historical struggle between manned interceptors and increasingly capable offensive aircraft, but at substantially lower unit costs and potentially much larger scales.

Directed-Energy Weapons and the Search for Economical Air Defence

The continuing economic imbalance between low-cost drones and conventional interceptor missiles has accelerated interest in directed-energy weapons. Unlike conventional missiles or artillery projectiles, directed-energy systems use concentrated electromagnetic energy to interfere with or physically damage a target. Two technologies have attracted particular attention in counter-drone applications. These are high-energy lasers and high-power microwave systems.

High-Energy Lasers

A high-energy laser concentrates electromagnetic energy onto a small area of an aerial target. If sufficient energy is deposited for an adequate period, the resulting heating can damage structural components, sensors or other critical parts of the aircraft. Laser weapons offer several theoretical advantages. They do not require a conventional projectile to travel towards the target, and their per-engagement electrical energy consumption can be much less expensive than firing a missile. Provided sufficient power, cooling and system availability are maintained, they can also reduce dependence on finite missile inventories. Britain's DragonFire programme illustrates the progress being made. In November 2025, the UK Ministry of Defence announced that the system had successfully engaged high-speed drones during trials and awarded a contract intended to introduce DragonFire systems into Royal Navy service from 2027. The ministry estimated a firing cost of approximately £10 per shot.[1?]

However, the commonly advertised low cost per laser engagement needs careful interpretation. Electrical energy is only one component of the overall operating cost. Acquisition, maintenance, cooling, power generation and personnel remain significant considerations. Laser performance also depends on conditions that missiles may be better equipped to tolerate. Rain, fog, smoke, atmospheric turbulence and other factors can degrade the propagation or concentration of energy. A target's movement, construction and exposure time influence how effectively the energy can damage it.

Consequently, a laser system should not be regarded as an unlimited-ammunition replacement for conventional air defence. It offers a potentially economical additional defensive layer, particularly against suitable targets under favourable operating conditions.

High-Power Microwave Systems

High-power microwave weapons operate through a different physical mechanism. Instead of concentrating energy onto a very small point to cause thermal damage, microwave systems emit electromagnetic energy intended to disrupt or damage electronic components within an aerial target. Their principal attraction lies in the possibility of affecting several electronic systems within a comparatively broad engagement area, potentially making them useful against multiple drones. The US Air Force Research Laboratory demonstrated this concept in April 2023 when its Tactical High-power Operational Responder, or THOR, successfully engaged multiple drones during a simulated swarm attack.[1]?

Unlike laser weapons, which generally require precise concentration of energy on individual targets, microwave systems can potentially affect multiple susceptible electronic devices within their beam. However, effectiveness is influenced by factors including distance, target design, electromagnetic shielding and the characteristics of the emitted energy. The distinction between electronic jamming and high-power microwave weapons is particularly important. A conventional jammer seeks to interfere with communication or navigation signals. A high-power microwave weapon seeks to disrupt or damage electronics through electromagnetic energy itself. Therefore, an autonomous drone that does not require an active radio-control link may still be susceptible to a sufficiently effective microwave weapon.

The difficulty lies in converting promising demonstrations into reliable operational capabilities. In August 2026, the US Army acknowledged the technical effectiveness of both laser and microwave systems while emphasising the need to understand their performance, sustainment requirements and practical use on operational installations.[1]?

Why Modern Air Defence Must Be Layered

The historical development of air defence demonstrates that no single weapon has ever remained consistently effective against every airborne threat. Anti-aircraft artillery was supplemented by radar-directed fire. Guided missiles subsequently extended the engagement envelope. Electronic warfare became essential for both attacking and protecting radar networks. Today, counter-drone technology adds another set of sensors and defensive weapons to this existing architecture. The resulting concept is commonly described as layered air defence.

Long-range surveillance and interception systems remain important for detecting and engaging high-altitude aircraft and long-range missile threats. Medium-range systems provide additional coverage against aircraft and other suitable aerial targets. Short-range missiles, radar-directed guns, electronic warfare equipment, interceptor drones and specialised counter-UAS systems protect formations and installations against threats within their respective engagement capabilities.

These layers are not isolated geographical rings. They are overlapping capabilities intended to provide alternative engagement options, redundancy and resilience. A drone that is not effectively countered by electronic warfare may still be engaged kinetically. A target unsuitable for a short-range interceptor may require a conventional missile. A threat that cannot be destroyed in time may still have its effects reduced through warning, dispersion or physical protection. The integration of these capabilities is at least as important as the capabilities themselves. NATO's February 2025 Integrated Air and Missile Defence Policy specifically emphasised complementary defensive systems operating at different ranges and altitudes, alongside passive measures including hardening, camouflage, deception, dispersion and redundancy.[1]? This represents a return to the central lesson of the Dowding System in 1940. The decisive advantage

lies not merely in possessing advanced sensors or weapons, but in coordinating them into a defensive structure capable of responding intelligently to different types of threats.

What Recent Conflicts Reveal About Counter-Drone Warfare

Ukraine and the Problem of Industrial-Scale Attrition

Ukraine offers perhaps the clearest contemporary demonstration of the counter-drone challenge. Russian long-range drone attacks have forced Ukrainian forces to develop a distributed defensive system that combines conventional military capabilities with relatively inexpensive and rapidly developed technologies. CSIS documented Ukraine's employment of extensive acoustic sensor networks, shared digital operational systems and other approaches intended to improve the efficiency of detecting and intercepting incoming drones.[1]?

The requirement extends beyond achieving a high interception rate. It includes protecting critical infrastructure, maintaining sufficient defensive ammunition, distinguishing decoys from genuine threats and preserving more expensive missiles for targets that cannot be intercepted economically by other means. Russian adaptation has complicated this task further. The introduction of faster jet-powered drones, improved navigation equipment and more sophisticated communications architecture demonstrates how countermeasures can become less effective as attackers change their designs. In September 2026, Reuters reported the growing deployment of Russian jet-powered attack drones capable of operating at considerably higher speeds than earlier propeller-driven Shahed variants. Ukraine's initial generation of inexpensive interceptor drones was consequently facing a threat for which it had not originally been optimised.[1]?

The central lesson is that counter-drone warfare increasingly depends on the rate of adaptation. A defensive capability that performs exceptionally well against one generation of drones may deliver diminishing results against subsequent variants unless sensors, interceptors and operational systems evolve.

India's Experience During Operation Sindoor

The May 2025 India–Pakistan military confrontation provided an important demonstration of the relevance of integrated counter-drone and conventional air defence in South Asia. According to the Indian Ministry of Defence's statement of 8 May 2025, Pakistan attempted to engage military targets across northern and western India using drones and missiles during the night of 7–8 May. The ministry stated that the incoming threats were neutralised by India's Integrated Counter-UAS Grid and air defence systems. Subsequent government reporting highlighted the employment of a combination of counter-UAS systems, electronic warfare assets, low-level air defence guns, legacy surface-to-air missile systems and modern weapons such as Akash.[2]? These statements establish the officially reported employment of a layered defensive architecture, although they should not be interpreted as independently verified performance data for every system involved.

The significance of Operation Sindoor extends beyond the reported destruction of incoming threats. It demonstrated the operational requirement to integrate conventional air defence with specialised counter-drone capabilities in an environment where unmanned aircraft, missiles and electronic warfare measures may be employed during the same confrontation. For India, the challenge also extends across very different operating environments. Protection of military airbases, border deployments, ammunition facilities, naval installations and strategically important infrastructure cannot depend on identical counter-drone configurations. The threat characteristics and defensive requirements vary considerably. The implication is that India requires an interoperable counter-drone architecture rather than merely the procurement of individual anti-drone weapons. Detection, identification, electronic warfare, short-range interception and conventional air defence need to operate within a coordinated command structure.

The Future of Counter-Drone Warfare

The next phase of counter-drone warfare is likely to be shaped by developments in autonomy, sensor fusion, directed-energy weapons and the industrial production of inexpensive interceptors. Artificial intelligence and machine learning are already becoming relevant to the classification of radar contacts, interpretation of electro-optical imagery, correlation of sensor reports and prioritisation of potential threats. As the volume of airborne activity increases, such capabilities may help reduce the burden on operators who would otherwise have to assess large numbers of contacts manually.

Nevertheless, automated classification does not eliminate uncertainty. Mistaken identification, poor sensor data and incomplete situational awareness can produce incorrect conclusions. Human oversight, particularly where engagement could endanger civilians or friendly aircraft, will remain a critical consideration.

A second trajectory involves the development of increasingly autonomous defensive interceptors. Systems capable of operating with reduced operator intervention may improve response times and help manage larger numbers of targets. Their effectiveness will still depend on reliable detection, appropriate target discrimination and safeguards against unintended engagements.

Third, the competition between electronic warfare and navigation technology will intensify. Improved interference-resistant satellite navigation, onboard visual navigation, inertial systems and alternative communications arrangements are likely to reduce the effectiveness of some existing jamming methods. Defensive systems will increasingly require several means of detecting and defeating the same target.

Fourth, future defensive architectures are likely to become more distributed. Rather than depending entirely on a small number of expensive radar installations and missile batteries, militaries may deploy networks of specialised sensors and relatively inexpensive defensive systems connected through common command-and-control software. NATO's Layered Counter-UAS Initiative, including interoperability trials conducted in Latvia during August 2026, reflects the increasing institutional emphasis on integrating different technologies and operational systems.[21]

A fifth development concerns the growing importance of production capacity. Defending against sustained drone attacks requires not only technically effective interceptors, but sufficient quantities of them. Defence manufacturers and militaries will have to balance sophisticated high-performance systems against cheaper weapons that can be produced and replenished rapidly. Directed-energy weapons could eventually improve this balance, but their practical contribution will depend on reliability, deployability and favourable engagement conditions. Traditional guns, missiles and interceptor drones are therefore likely to remain relevant alongside emerging technologies.

Finally, counter-drone warfare is moving beyond the exclusively military domain. Airports, energy installations, transport infrastructure, ports and other civilian facilities face a growing requirement for drone detection and protection. Yet employing jammers or physically destroying aircraft can interfere with legitimate communications and aviation activity, while falling debris may create additional hazards.

The legal and institutional challenges are substantial. European governments were still considering changes to the authority of critical infrastructure operators to employ counter-drone technologies in October 2026, demonstrating that regulation has not kept pace with technical development.[22]

Strategic Assessment

The evolution of air defence has reached another important transition. During the twentieth century, technological progress increasingly favoured sophisticated sensors, expensive guided weapons and centralised defensive

architectures. These systems remain essential against conventional aircraft and advanced missile threats, but their economic and operational assumptions are being challenged by the proliferation of inexpensive unmanned systems.

Drones have not invalidated the principle of integrated air defence. They have substantially expanded the range of threats that such a system must defeat. The distinction is consequential. A conventional missile battery may be technically capable of destroying many incoming drones, but repeated reliance on expensive interceptors against comparatively cheap targets can become unsustainable. Conversely, a low-cost jammer may neutralise certain commercial aircraft but provide little protection against drones with autonomous guidance or communications architectures that do not depend on vulnerable radio links. The decisive issue is therefore not the superiority of jammers over missiles, or interceptor drones over conventional air defence. It is the ability to assemble complementary technologies into a system that can identify different threats and respond without unnecessarily exhausting scarce defensive resources.

The future of counter-drone warfare will be determined by three interdependent factors, namely the effectiveness of detection and interception, the economics of sustained defensive operations and the speed at which defensive organisations can adapt to evolving threats. The Russia–Ukraine war demonstrates that tactical solutions can be overtaken rapidly by new offensive technologies. Operation Sindoor underscores the relevance of integrating conventional and specialised defensive systems in India's security environment. Emerging directed-energy weapons and autonomous interceptors indicate possible future solutions, but none removes the requirement for coordinated sensors, command systems, trained personnel and resilient infrastructure.

Counter-drone defence is consequently becoming a permanent component of modern air defence rather than a specialised capability reserved for unusual threats. Its strategic importance will continue to grow as unmanned systems become more numerous, more autonomous and more deeply integrated into reconnaissance and strike operations.The states best positioned to manage this transition will not necessarily be those possessing the most expensive defensive platforms. They will be those capable of combining technological sophistication with operational flexibility, economical interception and the industrial capacity to sustain defence against large numbers of continuously evolving aerial threats.

Endnotes

1. Benjamin Jensen and Yasir Atalan, “Drone Saturation: Russia’s Shahed Campaign,” Center for Strategic and International Studies (CSIS), May 13, 2025.

2. Kateryna Bondar and Nicole Errera, “From Shahed to Geran: How Russia Continues to Reinvent the One-Way Attack Drone,” CSIS, September 4, 2026.

3. Royal Air Force Museum, “How Radar Works,” History of the Battle of Britain, accessed October 21, 2026.

4. Smithsonian National Air and Space Museum, “Nike-Ajax Antiaircraft Missile System Technical Manuals,” and “ SA-2 Guideline Missile,” museum collections, accessed October 21, 2026.

5. “The Bekaa Valley War,” Air & Space Forces Magazine, June 2002.

6. Ian Williams, “Don't Waste This Lesson: How Drone Attacks Reveal Fixable Flaws with American Air Defenses,” CSIS, September 24, 2019. Shaan Shaikh and Wes Rumbaugh, “The Air and Missile War in Nagorno-Karabakh:

Lessons for the Future of Strike and Defense," CSIS, December 8, 2020.

7. Andre Haider, "A Comprehensive Approach to Countering Unmanned Aircraft Systems," Journal of the Joint Air Power Competence Centre, January 2020.

8. U.S. Government Accountability Office, "Science & Tech Spotlight: Counter-Drone Technologies," GAO-22-105705, March 15, 2022.

9. Kalina Hyche, "M-LIDS Strengthens Counter-UAS Interoperability during Yudh Abhyas 2026," U.S. Army, September 25, 2026.

10. Haider, "A Comprehensive Approach to Countering Unmanned Aircraft Systems."

11. Bondar and Errera, "From Shahed to Geran."

12. U.S. Army Acquisition Support Center, "Innovation Draws International Interest," and U.S. Government Accountability Office, "Science & Tech Spotlight: Counter-Drone Technologies."

13. Max Hunder and Tom Balmforth, "Ukraine Races to Counter Russia's Jet-Powered Drone Attacks," Reuters, September 15, 2026.

14. UK Ministry of Defence, "Boost for Armed Forces as New Laser Weapon Takes Down High-Speed Drones," November 20, 2025.

15. Nina Rogers, "AFRL Conducts Swarm Technology Demonstration," U.S. Air Force Research Laboratory, May 16, 2023.

16. Vonnie Wright, "JIATF-401 Counter-UAS and Critical Infrastructure Protection Media Roundtable," U.S. Army, August 24, 2026.

17. North Atlantic Treaty Organization, "NATO Integrated Air and Missile Defence Policy," February 13, 2025.

18. Jensen and Atalan, "Drone Saturation: Russia's Shahed Campaign."

19. Hunder and Balmforth, "Ukraine Races to Counter Russia's Jet-Powered Drone Attacks."

20. Ministry of Defence, Government of India, "Pakistan's Bid to Escalate Negated: Proportionate Response by India ," Press Information Bureau, May 8, 2025. Government of India, "Operation Sindoor: The Rise of Aatmanirbhar Innovation in National Security," Press Information Bureau, May 14, 2025.

21. NATO Allied Command Transformation, "Military and Industry Unite to Advance NATO Counter Drone Capability through LCI-X 3-26," August 13, 2026.

22. Reuters, “Europe Weighs Giving Utilities, Infrastructure Companies More Powers to Bring Down Drones,” October 21, 2026.