Analysis of Foreign Military Anti-UAV Operations

Abstract In the future informationized and intelligent battlefield， both the combat concepts and the technologies of weaponry and equipment will move towards intelligence. High-tech intelligent weaponry and equipment will be widely applied in the military field. Unmanned systems serve as the main material foundation for intelligent combat. Intelligent unmanned equipment such as unmanned aerial vehicles（UAVs），unmanned surface vessels，and unmanned vehicles are profoundly changing the form of war and the patterns of combat. Therefore， it is of great significance to study the key technologies of anti-unmanned combat platforms in combination with existing combat means. This article looks ahead to the application prospects of new types of UAVs and UAV swarms in the modern battlefield. By integrating with the combat process of UAV clusters，it summarizes the key anti-UAV technologies from four aspects which are deception，soft kill，and hard destruction，which together constitute a complete set of tactics and strategies for anti-UAV cluster combat in the naval battlefield.

1 Introduction

With the recent integration and development of artificial intelligence technology and air combat gaming technology, weaponry and equipment are undergoing an intelligent revolution. UAVs integrated with advanced AI algorithms can better understand the battlefield, plan mission routes, and make tactical decisions. They play crucial roles not only in reconnaissance, surveillance, and intelligence gathering but also in precision strike missions against land and sea targets. In modern military conflicts, the application of intelligent UAV technology has become a major feature of modern warfare. In 2016, an air combat AI jointly developed by the University of Cincinnati and the US Air Force Research Laboratory defeated a fourth-generation fighter jet piloted by US Air Force Colonel Gene Lee, supported by an AWACS aircraft, using a third-generation fighter in a simulated air combat scenario. In January 2020, the US military deployed an MQ-9 UAV to launch three "Hellfire" missiles, assassinating the Iranian senior commander Major General Soleimani^[1]^. In the Nagorno-Karabakh conflict that erupted in September 2020, Azerbaijan used UAVs carrying destructive payloads to attack Armenian ground forces, destroying a large amount of Armenian equipment, including S-300 air defense systems, within 24 hours^[2]^.

In April 2021, during the "Unmanned Systems Integrated Battle Problem 21" exercise, the US Navy for the first time employed a UAV swarm to conduct a saturation attack, destroying a surface vessel^[3]^. In the Russia-Ukraine conflict that erupted in February 2022, Russia used reconnaissance-strike integrated UAVs such as the "Forpost-R" and "Orion" for surveillance, reconnaissance, and fire strikes, while Ukraine employed UAVs like the TB-2 and "Switchblade" to harass Russian second-line logistics support units^[4]^. Advanced UAV systems are typically equipped with high-performance sensors, navigation equipment, and communication systems, enabling more accurate perception, faster decision-making, and more efficient actions. They can autonomously or semi-autonomously execute complex tasks. Their application in the military field is increasingly widespread, gradually becoming a significant form of modern local warfare, and their role in modern warfare is becoming ever more prominent.

2 UAV Combat Application

Based on specific mission tasks, UAVs and UAV groups typically perform different functions according to their activity characteristics and organizational implementation requirements. They possess powerful penetration capabilities, diverse combat modes, high intelligence, and low cost, enabling them to provide intelligence information and communication relay support, fire strike support, and electronic interference support. In the Russia-Ukraine conflict, Ukrainian forces used the "Starlink" system to control UAVs and unmanned surface vessels to launch a joint attack on the Russian Sevastopol base. During the operation, Ukrainian UAVs conducted feint attacks to draw Russian air defense fire, thereby buying time for the unmanned vessels to attack. The US military's "RQ-4 Global Hawk" unmanned reconnaissance aircraft participated throughout the process in commanding and controlling Ukrainian UAVs, guiding strikes, and evaluating effectiveness, causing severe damage to the Russian Black Sea Fleet. This is a typical case of UAV clusters conducting joint combat strikes.

2.1 Intelligence Support and Communication Relay

Reconnaissance and surveillance UAV systems are typically equipped with electro-optical or infrared sensor systems, high-resolution synthetic aperture radar, data links, specialized software, and other systems. With characteristics such as small size, high speed, high concealment, large combat radius, long endurance, all-weather and high-precision intelligence-gathering effectiveness, high survivability, low cost, and mobility, they can form a comprehensive, all-time-space, three-dimensional intelligence acquisition network together with satellites and manned aircraft^[5]^.

When executing combat missions, UAVs of various types can be equipped on aircraft carriers and surface vessels, launched towards enemy maritime areas, and deployed in batches across different battle zones. Leveraging computer image recognition technology, they can acquire reliable intelligence and discover relatively concealed potential enemy threats^[6]^. Remaining airborne for extended periods, they capture images of the entire battlefield situation and transmit them in real-time to other combat platforms like aircraft carriers or AWACS aircraft. This compensates for the limitations in observation area and range of surface vessels, enabling commanders to comprehensively grasp the battlefield situation, enhancing the real-time detection capability of surface vessel formations, and providing precise, timely intelligence assurance for the combat command system. In emergency situations, they can serve as aerial communication relay stations, using low-power, long-range wireless communication technologies for data acquisition and transmission, assisting uplink communication, improving communication speed and quality, and ensuring the effectiveness, timeliness, and security of intelligence transmission.

2.2 Fire Strike

UAVs and their clusters can be armed with various types of ammunition, such as missiles and loitering munitions, based on the target. They participate in multi-service joint combat chains, becoming a crucial link in the kill chain. In future naval battlefields, due to the deterrence of nuclear weapons, large-scale fire engagements will be replaced by localized peripheral conflicts, and UAVs will become the mainstay of aerial contests in the naval battlefield. Small UAV swarms, characterized by low cost, simple functions, and high fault tolerance, have low optical and radar signatures and minimal infrared radiation, making them difficult to detect with existing technologies. They can execute attack missions from long distances. UAV swarms covering large areas, through intelligent

cooperative wireless networking, can accurately analyze battlefield situational awareness, coordinate with our long-range weapons and manned-unmanned teams, rationally plan and assign combat mission targets, disperse enemy air defense firepower, collaborate with each other, conduct saturation strikes against the enemy, and assess strike effectiveness.

2.3 Electronic Interference

Modern battlefield air defense systems are tight, and defensive measures are mature. UAVs can act as decoys, simulating the radar and infrared detection signatures of different types and numbers of combat aircraft. Coordinating with other electronic jamming equipment, they can implement deception jamming, creating false aerial situations to cover other high-value combat equipment and weapons. This lures the enemy's early warning and detection systems into operational responses, forces enemy air defense firepower to retaliate, consumes enemy air defense weapons, and simultaneously reveals enemy defensive force deployments and response patterns. Furthermore, UAV clusters can be loaded with GPS jamming payloads, electronic jamming equipment, cyber attack devices, etc. Based on mission requirements, they can be deployed in batches within the target operational airspace, flying covertly at ultra-low altitudes. This enables them to conduct signal interference against enemy air combat formations, naval vessel formations, and ground combat clusters, disrupting the operational coordination between enemy land, sea, air, and other multi-dimensional combat elements, sub-groups, and units, thereby degrading their multi-domain joint combat capability and cross-domain cooperative strike capability^[7]^.

3 Anti-UAV Tactics and Methods

In response to the multiple combat roles and mission requirements of UAVs and their swarm systems on the modern battlefield, it is necessary to study the combat characteristics of UAV swarms, including their flight behaviors, communication patterns, and task execution strategies. Building on this, and integrating existing domestic and international anti-UAV technologies, a comprehensive set of anti-UAV defense measures should be developed. These measures encompass detection technologies, such as using advanced radar/radio/infrared sensor networks to identify and monitor enemy UAV intrusions in real-time, providing intelligence support for subsequent combat operations; deception and jamming technologies, including camouflage decoy deception, radio jamming, navigation jamming, and link hijacking, to degrade UAV reconnaissance and targeting of mission objectives and disrupt the navigation and control links of UAVs[原文如此]; destruction and strike technologies, including using direct physical destruction means such as missiles, microwave, and laser weapons to degrade or paralyze enemy UAV combat capabilities, or capturing enemy UAVs via nets.

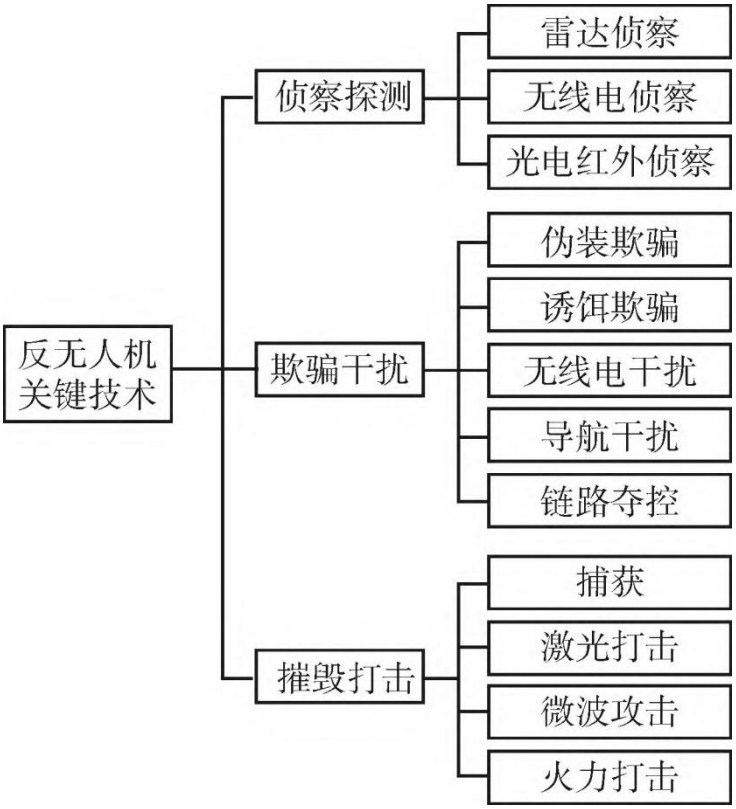

Figure 1 Key Anti-UAV Technologies

Based on specific combat scenarios and the characteristics of each stage of UAV operations, different countermeasures need to be selected to construct a multi-layered, all-around defense system. Taking a typical naval battlefield as an example, naval UAV clusters can cooperate with unmanned vessels, submarines, and aircraft through combat methods like long-endurance reconnaissance and surveillance, distributed relay communication, stealthy penetration, and cluster cooperative strikes. During this process, UAV combat mainly includes long-range launch, mid-range flight, short-range penetration, terminal operation, and return/recovery. Centering on the UAV combat process, anti-UAV operations can be divided into four phases: long-range detection and early warning, mid-range jamming and hijacking, short-range destruction and strike, and terminal comprehensive protection^[8]^

3.1 Long-Range Detection and Early Warning

Long-range detection and reconnaissance typically rely on technologies such as satellites, radar, electro-optics, and infrared detection. By identifying and analyzing characteristic signals of UAVs like signature images, electromagnetic wave signals, thermal imaging, and acoustic waves, early reconnaissance and warning are achieved. Details are as follows:

1) Radar Detection: Utilizes radar systems to transmit electromagnetic waves and detect/locate UAVs by receiving the reflected signals. Radar detection features long range, accurate positioning, and insensitivity to environmental effects. It targets the "low-slow-small" (LSS) characteristics of UAVs but suffers from close-range blind spots and shielding by special materials.

2) Laser Pulse Identification (LIDAR): Can be installed on various platforms like aircraft and vessels. It

emits laser pulses for remote sensing detection, creating high-precision 3D point cloud data by measuring the time it takes for the pulse to return after hitting an object. However, it is significantly affected by weather conditions^[9]^.

3) Electromagnetic Signal Identification: Includes visible light and infrared identification and tracking technologies, detecting and tracking UAVs by capturing their images via cameras. Visible light identification and tracking have lower costs but are limited by lighting conditions; infrared identification and tracking detect heat signatures, enabling all-weather use, but are easily affected by heat sources.

4) Acoustic Monitoring: Monitors and identifies UAV types by receiving and analyzing the noise generated during UAV flight and matching it against an acoustic signature database. This is a passive monitoring method with concealment and cost-effectiveness advantages. However, it can only detect UAV targets at close range and is significantly affected by ambient noise.

5) Radio Signal Detection: Used to detect communication signals between UAVs and their control stations, primarily in the 2.4 GHz and 5.8 GHz bands. This method can distinguish device models by measuring signal characteristics like carrier frequency, bandwidth, modulation type, preamble, etc., and create UAV whitelists/blacklists^[10]^, enabling precise identification of enemy UAVs. However, it can be affected by environmental factors and UAV silent flight modes, and decryption takes time, resulting in low real-time performance. Specific UAV models are small with weak electromagnetic signatures. A single detection method often cannot achieve comprehensive identification and monitoring of all types of UAV targets throughout their flight path. Therefore, an integrated land, sea, air, and space detection and early warning system should be established, forming a three-dimensional detection network covering high, medium, and low altitudes and long, medium, and short ranges. By integrating signal features collected from various sensors, information can be fused and shared to identify and track potential suspicious targets earlier.

3.2 Mid-Range Jamming and Hijacking

Jamming and hijacking of UAVs primarily rely on disrupting communications. When executing tasks, UAVs use sensors and automatic control systems for flight. They are typically equipped with navigation systems, attitude measurement systems, flight control systems, etc., transmitting their position, velocity, attitude, energy status, etc., in real-time to operators or other UAVs. This requires emitting radio signals for interaction and navigation/positioning. By cracking UAV communication links, transmitting spoofed navigation signals, emitting same-frequency radio communication signals, deploying high-power electromagnetic pulses, or launching cyber attacks, mid-range jamming and hijacking of UAVs can be achieved^[11]^.

1) Link Hijacking: Decrypts and deciphers the enemy's UAV swarm control signals. By illegally intruding and inputting false control commands, it achieves takeover control of the enemy UAV swarm. This method is commonly used against commercial UAVs, characterized by good concealment and high penetration capability. It requires sufficient preparation, prior knowledge of the enemy UAV communication link protocol, and the formulation of meticulous cracking strategies^[12]^.

2) Navigation Jamming and Spoofing: Navigation jamming can suppress a UAV's reception of navigation satellite signals, causing drift errors and deviation from the intended flight path. Spoofing techniques like no-fly-zone location spoofing, fixed-point spoofing, or flight path deviation can cause the UAV to obtain erroneous position information and fly according to a route set by us^[13]^. However, when multiple spoofing techniques are implemented simultaneously, or spoofing is combined with navigation jamming (suppression), the UAV is often in a state with no navigation information after suppression, making spoofing difficult to achieve the intended purpose.

3) Signal Jamming: Achieves electromagnetic spectrum suppression by emitting high-power, wide-area radio signals via directed energy weapons. This enables long-range electromagnetic interference, disrupting the UAV's remote sensing data link, damaging its electronic components, and paralyzing its electronic systems. This makes it difficult for the UAV to transmit data to other UAVs or the operator, leading to loss of control.

Drone systems possess unmanned characteristics; therefore, reliance on radio waves for networked communication is their inherent feature. Utilizing electromagnetic means to disrupt drone navigation systems, communication systems between drone swarms, and their command & control links with operators can effectively interfere with or even seize control of enemy drones. This method can effectively undermine the combat effectiveness of drones, possessing the advantages of pronounced operational effects and high cost-effectiveness ratio.

3.3 Short-range Destruction and Terminal Defense

Short-range destruction of drones includes kinetic strikes, net-based capture systems, microwave attacks, and laser strikes. This primarily involves using laser beams, microwave pulses, and artillery shells/munitions to destroy the electro-optical/infrared sensors, electronic components, or airframes of drones that have approached friendly positions, thereby neutralizing their attack capabilities.

Furthermore, comprehensive terminal defense against drones mainly encompasses active and passive defense measures. Active defense employs kinetic strikes. Passive defense is subdivided into camouflage techniques and protective hardening. Camouflage protection includes smoke screening, decoy deception, terrain masking, and net/cover protection. Examples include installing protective nets or covers on key targets, deploying decoys, releasing smoke screens, and reinforcing defensive structures to enhance resilience [14].

Kinetic Strikes: Kinetic strikes are primarily categorized as precision strikes and dense barrage fire. Traditional air defense weapons, such as rapid-fire cannons, anti-aircraft guns, and missiles, remain the most practical and effective measures currently used for terminal drone defense. By integrating artillery systems with pre-configured fragmentation munitions, a dense fire net can be established to effectively intercept drone swarm attacks. However, this interception method is relatively costly and may still fail to stop all targets when facing large-scale or saturation attacks. In maritime

operations, high-pressure water cannons or jets can also be used to short-circuit a drone's power supply system, though their effective range is limited.

Net-based Capture: Net-capture weapons mainly include net-deploying drones and net-projectile shells. Using net-capture weapons to intercept low-altitude, slow, and small drones (LSS drones) is highly cost-effective. These weapons utilize tube-launched devices carrying infrared proximity sensors to eject foam or nets, disrupting flight and forcing the drone to crash-land.

Directed Energy Weapon (DEW) Attacks: DEWs currently applied in actual combat are mainly laser weapons and high-power microwave (HPM) weapons. Their essence is to achieve electromagnetic spectrum suppression and hard kill effects on information systems through the directional radiation of high-intensity electromagnetic waves [15]. Lasers can thermally destroy small drones or damage their optical components, causing loss of detection capability and flight control. Against attack drones, lasers can be aimed at their carried munitions to induce detonation. HPM weapons can directly attack sensitive electronic components within the drone target, causing short circuits.

Traditional air defense weapons have long range and strong attack power. However, due to the high cost of their munitions and the high mobility, small size, and large numbers of drones, they suffer from a high cost-effectiveness ratio and are prone to letting targets slip through the net. Net-based weapons have shorter ranges and are limited to engaging slow-moving drones. With the advancement of fiber laser technology, solid-state laser technology, and solid-state high-power microwave devices, tactical DEWs characterized by miniaturization, light weight, and compactness are rapidly developing. These are gradually being deployed in actual combat, becoming effective means to counter unmanned systems. Integrating multiple systems to construct an interception system capable of engaging drones at different distances, altitudes, and types is an inevitable trend.

4 Conclusion

In the future, unmanned combat systems will continue to integrate more innovative technologies to attain higher levels of operational capability and accomplish complex combat missions. Their development will drive a new generation of transformation in military theory and practice. How to flexibly and ingeniously improve existing tactics and methods by combining the current air defense equipment system with new-domain and high-quality combat capabilities, and how to develop a counter-drone operational system, have become urgent and crucial problems requiring accelerated research and resolution. Starting from the operational employment of drones, this paper analyzed the combat characteristics of individual drones and drone swarms, further studied key counter-drone technologies, and on this basis, proposed a set of practical tactics and methods. With a long-term perspective, it aims to promote the construction of China's integrated joint defense system against unmanned systems.