Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 6, June, 2026
Website: usajournals.org

ATTACKS ON AIR DEFENSE SYSTEMS IN MODERN MILITARY CONFLICTS AND METHODS OF COUNTERACTION

Ermetov Axrar Anarbekovich
Senior Lecturer at the Department of the Institute of Information and Communication Technologies and Military Communications of the University of Military Security and Defense of the Republic of Uzbekistan

Abstract
The article examines modern methods of attacks against air defense systems in the context of 21st century armed conflicts, as well as the main approaches to improving the survivability and effectiveness of air defense systems. The study analyzes the characteristics of Suppression and Destruction of Enemy Air Defenses operations, the role of unmanned aerial vehicles, precision-guided weapons, electronic warfare, and cyberattacks in contemporary military conflicts.
Keywords: Air defense, unmanned aerial vehicles, electronic warfare, cyberattacks, precision-guided weapons, loitering munitions, modern military conflicts, air defense systems, network-centric warfare, air operations, artificial intelligence, missile defense.

Modern armed conflicts demonstrate a rapid transformation in the nature of air warfare and the role of air defense systems. While in the past the primary mission of air defense was to repel enemy aircraft attacks, today the spectrum of threats has expanded significantly and includes cruise missiles, ballistic weapons, hypersonic systems, unmanned aerial vehicles, loitering munitions, and electronic warfare assets. Under contemporary conditions, adversaries seek not only to penetrate air defense systems but also to completely disable them through specialized Suppression and Destruction of Enemy Air Defenses operations. Analysis of recent military campaigns indicates that the effectiveness of air operations directly depends on the ability of the opposing sides either to suppress enemy air defense systems or to preserve the survivability of their own air defense networks [1].

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 6, June, 2026
Website: usajournals.org

This tendency has become especially evident in the conflicts in the Middle East, Nagorno-Karabakh, Syria, and Ukraine. The mass employment of inexpensive drones and precision-guided munitions has forced military planners to reconsider classical principles of air defense organization. Modern attacks against air defense systems are characterized by a comprehensive approach that combines reconnaissance activities, electronic warfare, decoys, cyberattacks, and precision strikes simultaneously. Under such conditions, the survivability of air defense systems depends not only on technical capabilities but also on rapid maneuverability, integration into a unified information network, and adaptability to emerging threats [2].

Suppression of Enemy Air Defenses represents a complex set of measures aimed at temporarily or permanently disabling enemy detection, command, and fire-control systems. The primary objective of such operations is to create favorable conditions for the safe employment of aircraft, cruise missiles, and unmanned systems. In modern conflicts, SEAD and DEAD operations have become an indispensable element of every major air campaign. The principal targets include radar stations, command posts, surface-to-air missile systems, communication assets, and elements of automated command-and-control systems [1].

Modern SEAD operations are characterized by a high degree of automation and the employment of reconnaissance-strike complexes. Prior to an attack, detailed reconnaissance of enemy radar activity is conducted, including analysis of radar frequencies and identification of maneuver routes used by mobile systems. Anti-radiation missiles, unmanned aerial vehicles, electronic warfare systems, and decoys are subsequently employed. As a result, air defense systems are forced either to shut down their radars or face destruction. Such tactics were widely used during NATO operations against Yugoslavia and continue to be employed in contemporary conflicts in Ukraine and the Middle East [1; 3].

One of the key factors transforming modern air warfare has been the widespread use of unmanned aerial vehicles. Contemporary UAVs are capable of conducting reconnaissance of air defense positions, overloading detection systems, and delivering precision strikes against radar stations and missile launchers. Particularly dangerous are loitering munitions that combine reconnaissance and strike capabilities within a single platform. During the 2020 Nagorno-Karabakh

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 6, June, 2026
Website: usajournals.org

conflict, Azerbaijani armed forces actively employed Turkish Bayraktar TB2 drones and Israeli-made Harop loitering munitions to destroy Armenian air defense assets [3].

The conflict in Ukraine has also demonstrated the increasing importance of inexpensive strike drones and tactics involving mass attacks. Russian and Ukrainian forces actively use UAVs to overload air defense systems, distract operators, and reveal radar positions. The widespread use of drones creates a situation in which expensive interceptor missiles are expended against relatively cheap aerial targets. As a result, the problem of economic exhaustion of air defense systems emerges. Contemporary analysts emphasize that in the future, the primary threat to traditional air defense systems will stem from the mass scale and combined nature of aerial attacks [4].

Electronic warfare plays a critical role in the suppression of air defense systems in modern conflicts. EW systems are capable of jamming radar stations, disrupting communication channels, distorting navigation data, and reducing the effectiveness of fire-control systems. Modern air defense systems heavily depend on the stability of information channels and automated data exchange networks, making them vulnerable to electronic interference. During the conflict in Ukraine, electronic warfare systems capable of temporarily reducing radar detection effectiveness and complicating missile guidance have been extensively employed [5].

An additional threat is posed by cyberattacks targeting automated air defense command-and-control systems. Modern air defense complexes are integrated into digital communication networks and increasingly employ artificial intelligence elements for airspace analysis. This creates opportunities for interference with software systems, the insertion of false targets, and disruption of information exchange between system components. Military experts increasingly regard cyberspace as a fully-fledged theater of military operations where the struggle for information superiority has become as important as the use of traditional kinetic weapons [6].

Modern military conflicts demonstrate that combined attacks against air defense systems are among the most effective operational methods. Such attacks involve the simultaneous employment of drones, cruise missiles, ballistic weapons,

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 6, June, 2026
Website: usajournals.org

decoys, and electronic warfare assets. The principal objective of these attacks is to overload the air defense system and create conditions in which operators are unable to distribute targets effectively or utilize a limited number of interceptor missiles in a timely manner. Similar tactics are actively employed in the Russian-Ukrainian conflict, where both sides use mixed waves of attacks to exhaust enemy air defense capabilities [4].

Particularly dangerous are long-range precision-guided missiles and low-observable strike systems. Modern cruise missiles are capable of flying at extremely low altitudes while following terrain contours, which significantly complicates their detection. Hypersonic weapons further reduce the reaction time available to air defense systems. Consequently, modern air defense complexes are forced to operate under conditions of constant information overload and severe time constraints. Analysts emphasize that the continued development of precision-guided weapons will further increase the vulnerability of traditional air defense systems [2; 3].

One of the principal approaches to improving air defense survivability is the creation of deeply layered and integrated defense architectures. Modern air defense must include systems of various operational ranges, mobile radar stations, automated command centers, and electronic warfare assets. High mobility of missile systems and the ability to rapidly change positions after engagement have become critically important. The experience of recent conflicts demonstrates that stationary air defense systems quickly become vulnerable targets for precision-guided weapons and drones [2].

Another important direction involves the implementation of artificial intelligence and advanced automated command systems. Modern algorithms can significantly accelerate target classification, task allocation, and decision-making processes during mass attacks. Particular attention is devoted to the development of low-cost anti-drone solutions, including laser systems, electronic warfare systems, and rapid-fire artillery platforms. Experts argue that only the combination of traditional missile systems with innovative counter-UAV technologies will ensure the survivability of air defense systems in future conflicts [4; 6].

The effectiveness of modern air defense directly depends on reconnaissance and information exchange capabilities. In highly maneuverable warfare, satellite

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 6, June, 2026
Website: usajournals.org

surveillance systems, airborne early warning aircraft, reconnaissance drones, and automated data-processing centers play an increasingly important role. The modern concept of network-centric warfare assumes the integration of all air defense elements into a unified information network. Such integration enables rapid target allocation, coordination among various defense systems, and enhanced survivability during massive attacks [2].

Particular importance is attached to cooperation among air defense systems, aviation assets, and electronic warfare units. Modern systems must function as a unified complex capable of rapidly adapting to changes in the air situation. An important development trend involves distributed command-and-control systems, where the destruction of a single command post does not result in the collapse of the entire network. Such approaches are actively implemented by leading military powers and are considered essential for the survival of air defense systems under conditions of high-technology warfare [5].

Modern military conflicts demonstrate a fundamental transformation in the nature of attacks against air defense systems. The principal threats now include unmanned aerial vehicles, precision-guided weapons, electronic warfare assets, and cyberattacks. Adversaries seek not only to destroy individual components of air defense systems but also to disrupt the operation of the entire command-and-control network. The experience of recent conflicts shows that even the most advanced air defense systems remain vulnerable to massive combined attacks and information-channel overloads.

Under such conditions, the future development of air defense must focus on increasing mobility, automation, and integration of all defensive elements into unified information networks. Particular significance is attached to low-cost counter-drone systems, laser weapons, artificial intelligence technologies, and distributed command structures. Future air defense systems must be capable of operating effectively under conditions of constant electronic and informational confrontation while maintaining survivability even when individual components are partially destroyed.

The experience of modern armed conflicts demonstrates that the success of air operations increasingly depends not on the number of aircraft available but on the ability of military forces to suppress enemy air defense systems or effectively

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 6, June, 2026
Website: usajournals.org

protect their own. For this reason, the modernization of air defense has become one of the key priorities in the development of the armed forces of leading military powers. Contemporary air defense is evolving into a sophisticated multilayered system in which information technologies, automation, and adaptability to new forms of threats play a decisive role.

References:

[1] Bronk J. Getting Serious About SEAD: European Air Forces Must Learn from the Failure of the Russian Air Force over Ukraine // Royal United Services Institute (RUSI). URL: https://www.rusi.org/explore-our-research/publications/rusi-defence-systems/getting-serious-about-sead-european-air-forces-must-learn-failure-russian-air-force-over-ukraine.
[2] Bronk J. Modern Russian and Chinese Integrated Air Defence Systems: The Nature of the Threat, Growth Trajectory and Western Options // Royal United Services Institute (RUSI). URL: https://www.rusi.org/explore-our-research/publications/occasional-papers/modern-russian-and-chinese-integrated-air-defence-systems-nature-threat-growth-trajectory.
[3] Understanding the SEAD/DEAD Missions of Modern Fighter Jets // War Wings Daily. URL: https://warwingsdaily.com/understanding-the-sead-dead-missions-of-modern-fighter-jets.
[4] Jensen B., Atalan Y., Tiersten-Nyman E. The New Salvo War: Russia's Evolving Punishment Campaign // Center for Strategic and International Studies (CSIS). URL: https://www.csis.org/analysis/new-salvo-war.
[5] Sdrakas A. Beyond the Hype: Assessing Russian Airborne EW Shortcomings in the Ukraine Conflict // Joint Air Power Competence Centre (JAPCC). URL: https://www.japcc.org/articles/beyond-the-hype.
[6] Wang J., Liu Y., Song H. Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends // arXiv. URL: https://arxiv.org/abs/2008.12461.