Journal of Electronic Research and Application, 2026, Volume 10, Issue 8
http://ojs.bbwpublisher.com/index.php/JERA
Online ISSN: 2208-3510
Print ISSN: 2208-3502

# Discussion on Challenges and Development of Electronic Warfare under Distributed Operations

**Bing Luo*, Tianwei Zhou, Yuanming Zhou, Guofeng Shao**

No.36 Research Institute, China Electronics Technology Group Corporation, Jiaxing, Zhejiang 314033, China

***Corresponding author:** Bing Luo, 416283286@qq.com



**Abstract:** Against the backdrop of intensifying global strategic competition, distributed operations have evolved into a dominant new warfare paradigm. Based on the latest operational concepts proposed by the U.S. military, this paper elaborates on the origin, evolution trajectory and operational characteristics of distributed maritime and air operations, and analyzes the technical development paths and implementation approaches for future distributed combat systems. Furthermore, it investigates the operational efficacy and inherent dilemmas of electronic warfare (EW) when countering distributed operations, and proposes a roadmap for key EW technological advancements, providing references for the future development of electronic warfare.

**Keywords:** Distributed operations; Electronic warfare (EW); Anti-access/area denial (A2/AD)

**Online publication:** Sept 8, 2026

## 1. Introduction

Previous U.S. military campaigns, including the Gulf War, Kosovo War, and Syria War, mainly targeted adversaries with relatively limited military strength, relying on concentrated combat platforms to achieve overwhelming operational superiority. However, when confronting peer great-power competitors, robust Anti-Access/Area Denial (A2/AD) capabilities of rival forces will severely constrain the effectiveness of traditional centralized combat architectures. To address this vulnerability, the United States has put forward the distributed operations concept, heavily invested in unmanned platforms, artificial intelligence (AI), and other emerging technologies, and integrated them into practical combat deployments [1]. The U.S. military has restructured its troop formation to build large-scale, low-cost unmanned forces, leveraging AI-assisted command-and-control (C2) decision-making to deliver enhanced combat performance at a lower overall cost. Notably, recent U.S.-Israeli joint operations such as Operation Epic Fury have validated highly intelligent distributed combat architectures. Dispersed reconnaissance and strike nodes are rapidly integrated into an intelligent kill web via ubiquitous wide-area communication networks.

Distributed operations are overwhelmingly dependent on electronic information systems, while electronic warfare serves as the core means to paralyze and disrupt such information infrastructure. This paper analyzes how EW disrupts three core pillars of distributed combat: sensor intelligence for operational decision-making, communication networks for coordinated command, and unified time-synchronization and friend-or-foe identification data required for multi-platform coordination. On this basis, it explores the developmental trends of EW against distributed operations to offer engineering and theoretical references.

## 2. Analysis of distributed maritime and air operations concepts

To adapt to great-power competition and meet the operational demands of high-contention maritime and air combat environments, the U.S. military has designed forward-looking warfare frameworks and proposed distributed maritime operations and distributed air operations, laying theoretical foundations for future peer-level conflicts [2].

### 2.1. Distributed maritime operations

Distributed maritime operations disperse naval combat assets across extensive maritime zones to sustain persistent sea control capability. This concept originated from Jeff Kares' "Distributed Networked Force" theory, with its evolutionary timeline summarized in **Table 1**.

**Table 1.** Evolution timeline of distributed maritime operations concept

| Year | Key development milestones |
|---|---|
| 2006 | Retired U.S. Navy officer Jeff Kares published *Distributed Networked Operations: The Foundation of Network-Centric Warfare*, proposing the "Distributed Networked Force" composed of manned warships, unmanned surface vessels (USVs), and ship-borne unmanned aerial vehicles (UAVs). |
| 2014 | U.S. Naval War College formalized the "Distributed Lethality" concept, which mandates every surface combatant to deliver credible offensive threats to hostile forces [3,4]. |
| 2020 | Senior U.S. Navy leaders, including former Chief of Naval Operations Gary Roughead, identified unmanned surface vessels, unmanned underwater vehicles (UUVs), and drone carriers as top priorities for future naval force structure, designating distributed maritime operations as the primary naval combat paradigm. |
| 2026 | The U.S. Navy announced annualization of the Pacific Distributed Operations Experiment; distributed maritime operations have become the standard framework for naval routine training and force generation, with unmanned systems accounting for over 20% of total naval assets. |

The core winning mechanism of distributed maritime operations lies in covert, dispersed, and flexible deployment of large numbers of surface combatants armed with heavy offensive ordnance [4]. This forces adversaries to allocate excessive detection and firepower resources. (**Figure 1**)

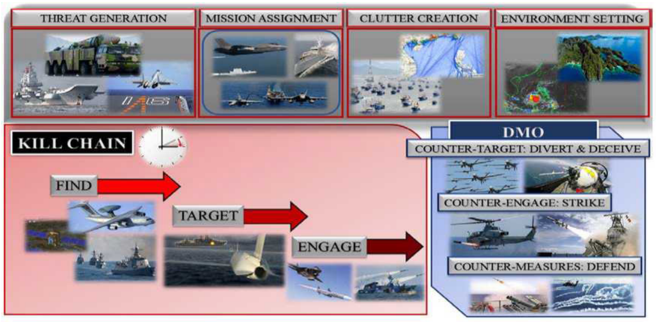


**Figure 1.** Concept diagram of distributed maritime operations.

(1) Core characteristics of distributed maritime operations

Multi-Domain Integration: Dynamic reorganization of combat platforms, weapons, and sensors fuses traditional fire-and-strike with intelligence warfare and electronic warfare across surface, subsurface, air, and cyber domains, maximizing integrated multi-domain combat performance.

(2) Deep informatization

Communication networking, automatic control, and intelligent signal processing form the technical foundation of distributed maritime combat. Guided by the distributed operations concept, the U.S. military has accelerated core information technology development, enabling manned/unmanned, surface/subsurface, and support platforms to support distributed information processing and networked cross-domain coordinated combat.

(3) System-centric integration

Individual combat platforms suffer catastrophic performance degradation once decoupled from the overall combat system. Inter-platform communication networks are the backbone of distributed architectures. The U.S. military maintains unique network integration advantages via high-speed, low-latency broadband satellite communication constellations represented by Starlink.

## 2.2. Distributed maritime operations

Distributed air operations were pioneered by the U.S. Defense Advanced Research Projects Agency (DARPA) to innovate aerial combat paradigms [5,6]. The concept integrates manned fighters and autonomous UAVs, supported by AI-assisted command-and-control, to realize low-cost, high-lethality combat via flexible dynamic reconfiguration of aerial assets. Its evolutionary timeline is shown in **Table 2**.

**Table 2.** Evolution timeline of distributed maritime operations concept

| Year | Key development milestones |
| --- | --- |
| 2014 | DARPA launched the System of Systems Integration Technology and Experimentation (SoSITE) program and formally proposed distributed air operations. The project developed innovative system architectures for heterogeneous aircraft, weapons, sensors and mission systems, distributing aerial combat capabilities across interoperable manned and unmanned aerial platforms. |
| 2017 | DARPA introduced the novel “Mosaic Warfare” operational framework. |

| | |
|---|---|
| 2020 | The U.S. military published *Mosaic Warfare: Decision-Centric Warfare Powered by Artificial Intelligence and Autonomous Systems*. Mosaic Warfare was framed as a concrete implementation pathway for the overarching decision-centric warfare framework, enabling commanders to generate faster, more effective decisions while paralyzing adversary decision cycles. |
| Post-2026 | Next-Generation Air Dominance (NGAD) manned fighters (e.g., F-47) and Collaborative Combat Aircraft (CCA, e.g., YFQ-42A/YFQ-44A, XQ-58A) will achieve full operational deployment, ushering in an era of large-scale manned-unmanned swarm coordination via system-of-systems clusters. |

After 2017, distributed air operations were gradually subsumed under the Mosaic Warfare framework, which shares identical core logic: dynamically assembling low-cost, single-function modular assets into scalable combat systems. The two concepts are inherently consistent [7]. Future distributed air operations will decompose high-end aerial combat capabilities (detection, EW, strike) onto low-cost autonomous UAVs, with a small number of high-performance manned fighters serving as coordination hubs to field scalable, cost-effective modular combat clusters with rapid technology iteration cycles. (**Figure 2**)

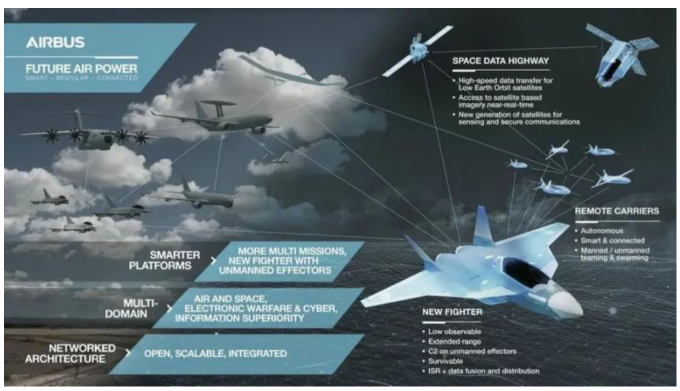


**Figure 2.** Concept diagram of distributed air operations.

Core characteristics of distributed air operations:

(1) Scalable force generation

Functional decomposition is the core of distributed air combat. High-end fighters offload detection, EW, and strike functions to unmanned platforms, forming disruptive manned-unmanned swarm combat led by a small number of manned command aircraft.

(2) Broad environmental adaptability

UAVs can carry diversified ordnance. Supported by AI, they generate real-time multi-dimensional mission solutions and dynamically reconfigure payloads to adapt to high-intensity and low-intensity combat environments.

(3) Diversified offensive tactics

Mass deployment of heterogeneous aerial assets creates severe battlefield fog, obscuring real strike axes and feint decoys for adversaries. Diversified weapon payloads further complicate enemy threat identification and response planning.

## 2.3. Core implementation paths for distributed operations

Distributed combat capabilities will be realized through breakthroughs and large-scale deployment of four core technologies: manned-unmanned collaborative coordination, modular combat element dynamic reconfiguration, AI-assisted decision-making, and self-organizing anti-jamming communication links.

(1) Advancement of unmanned platforms

Since the 21st century, U.S. unmanned system R&D priorities have shifted toward systematic integration and autonomous intelligence. The U.S. Department of Defense has released five successive editions of the Unmanned Systems Integrated Roadmap to advance swarm networking and autonomous combat capabilities. The 2017–2042 Unmanned Systems Integrated Roadmap, published in August 2018, serves as the U.S. military's overarching strategic guide for unmanned assets [8]. Centered on four core themes—interoperability, autonomy, secure networking, and human-machine coordination—the roadmap.

(2) Advancement of artificial intelligence

AI functions as the primary enabler of distributed operations. Current machine learning algorithms process massive multi-source sensor datasets to accelerate commander situational awareness and decision-making. Future AI will transfer most cognitive overhead associated with closed kill-chain operations to autonomous intelligent systems, allowing human commanders to focus on high-level strategic judgment and rapid tactical response. DARPA's Project MAVEN, an AI-enabled battlefield analytics program, has evolved into the core technical foundation of the U.S. Joint All-Domain Command and Control (JADC2) architecture by 2026.

(3) Advancement of self-organizing communication networks

Self-organizing networks constitute the technical backbone of distributed combat systems. Future distributed architectures will feature exponentially expanding network nodes and combat assets, driving surging demand for network bandwidth and transmission latency performance. Military IoT and advanced combat cloud networks will witness rapid development, transmitting not only raw sensor data but also shared machine-to-machine autonomous decision information to form a wireless combat cloud for real-time inter-node collaborative judgment [9].

# 3. Analysis of EW challenges and developmental directions

## 3.1. Core operational value of electronic warfare

As analyzed above, unmanned surface, subsurface, and aerial vehicles represent the foundational nodes of future distributed combat systems, carrying integrated sensors, strike weapons, and EW payloads [10]. Via self-organizing networks and AI, they form integrated manned-unmanned combat clusters to enhance battlefield lethality and survivability. Electronic warfare delivers decisive capability degradation by blinding sensors and severing communication links, emerging as the primary countermeasure against distributed combat architectures.

(1) Sensor neutralization tool

EW jams radar, electro-optical, infrared, and navigation sensors, depriving distributed combat clusters of real-time, accurate target metadata, including position, velocity, range, and target classification, completely breaking their situational awareness foundation.

(2) Communication link disruption tool

Inter-platform communication networks form the prerequisite for coordinated distributed combat. EW interference severs data exchange between dispersed nodes, dismantling system-level coordinated combat capacity.

(3) Command-and-control disruption tool

Accurate decision-making relies on credible sensor intelligence, low-latency communication links, and stable autonomous decision algorithms. EW distorts sensor data via deception jamming, delays or infiltrates communication channels, and fundamentally corrupts adversary command and tactical judgment cycles.

### 3.2. Inherent dilemmas confronting EW countermeasures

While EW can degrade distributed sensor and communication performance, advances in anti-jamming sensing, communication, and signal processing technologies have significantly mitigated traditional jamming effectiveness. Distributed combat architectures adopt multi-modal heterogeneous sensors and redundant communication backbones, diluting single-source EW suppression; in addition, distributed platforms may carry dedicated counter-EW hard-kill weapons targeting EW assets.

(1) Limitations of sensor jamming

Distributed platforms deploy heterogeneous multi-modal sensors with diversified waveform modulation and omnidirectional detection apertures, supported by high-precision multi-source data fusion algorithms. This creates critical EW challenges, including adaptive multi-modal jamming coverage, regional jammer deployment optimization, and real-time jamming effectiveness assessment. Advanced fusion filters can suppress external jamming signals, rendering conventional blanket jamming ineffective or marginally impactful.

(2) Limitations of communication network jamming

Distributed combat relies on self-organizing IP-based mesh networks interconnected via multi-layer routing protocols, complemented by directional datalink systems such as the Integrated Flight Data Link (IFDL) to enhance anti-jamming resilience. EW assets cannot simultaneously blanket all heterogeneous communication links, failing to fully sever inter-platform coordination and collapse distributed combat clusters.

### 3.3. Future development directions of electronic warfare

Analysis of EW operational utility and inherent limitations confirms that conventional standalone EW systems lack decisive, system-level suppression effects against distributed combat architectures, mandating comprehensive technical iteration and capability upgrades along four core pathways:

(1) Distributed EW system architecture technology

To counter heterogeneous multi-modal sensors and IP mesh communication networks of adversary distributed combat systems, EW must adopt a system-of-systems countermeasure paradigm to deliver equivalent distributed suppression capacity. A modular distributed EW framework paired with agile EW command-and-control algorithms enables multi-domain, multi-modal integrated jamming to dismantle enemy inter-platform coordination.

(2) Cooperative deception jamming technology

Deception jamming represents the dominant evolutionary trend for modern sensor countermeasures and the optimal pathway for communication network infiltration and disruption. Tailored to multi-platform distributed coordination architectures, deception jamming generates false target tracks and phantom contacts to exhaust adversary intercept ordnance and decision-making resources. Multi-source cooperative deception injects inconsistent radar echo data into separate enemy nodes, corrupting multi-sensor data fusion consistency.

(3) Integrated cyber-electronic attack technology

Conventional standalone EW is limited by line-of-sight range constraints and cannot engage remote distributed assets. Integrated cyber-electronic attack technology leverages wireless communication access and sensor terminal vulnerabilities to implant malware and gain remote control over large-scale unmanned swarms, realizing "single-point penetration, wide-area paralysis" and extending EW operational range to deliver decisive system-level disruption of distributed combat architectures.

(4) Cooperative EW-fire strike integration technology

A core objective of counter-distributed operations is disrupting adversary command-and-control and slowing their OODA (Observe-Orient-Decide-Act) decision cycles. Integrated EW-fire strike technology combines active/passive cooperative detection, multi-source heterogeneous data fusion, and communication node geolocation to rapidly identify high-value core command nodes within distributed combat clusters. EW suppression opens penetration corridors for kinetic strike assets, enabling hard-kill elimination of adversary system hubs to deliver fatal collapse of distributed combat superiority.

## 4. Conclusion

Driven by advances in electronic information technology and large-scale deployment of unmanned platforms, distributed operations will evolve into a mainstream warfare paradigm characterized by modular multi-weapon, multi-platform integrated combat systems, imposing severe response challenges for opposing forces. Electronic warfare serves as the decisive countermeasure against distributed combat architectures. Accelerated development of distributed EW systems, cooperative deception jamming, integrated cyber-electronic attack, and EW-kinetic joint strike technologies will effectively neutralize distributed combat advantages and drastically improve overall combat cost-effectiveness ratios.

## Disclosure statement

The authors declare no conflict of interest.

## References


[1] U.S. Department of Defense, 2016, Remarks by Deputy Secretary Work on Third Offset Strategy. U.S. Department of Defense: 5–8.

[2] Zhou X, Xu Q, He Z, 2020, Preliminary Research on Future Maritime and Air Distributed Combat Concepts and Force Employment. 2020(15): 856–860.

[3] Clark B, Cropsey S, Walton T, 2020, Sustaining the Undersea Advantage: Disrupting Anti-Submarine Warfare Using Autonomous Systems. Hudson Institute.

[4] Qin R, 2022, Research on Future Naval Distributed Combat Equipment Development. Journal of Naval Electronic Engineering, 42(07): 14–19.

[5] Yuan C, Mu Z, 2020, Analysis of U.S. Distributed Air Combat Concepts. Aeronautical Weapons, 2020(27): 11–16.

[6] Tang F, 2023, Analysis of U.S. Air Force Distributed Combat Progress Based on SoSITE Program. Avionics Technology, 54(04): 9–15.

[7] DARPA, 2023, DARPA Budget, https://www.darpa.mil/about-us/budget

[8] Li C, Sun Y, Fan Z, et al., 2023, Development Status and Trend of Unmanned Combat Platforms. Journal of China Academy of Electronics and Information Technology, 18(03): 274–279.

[9] Liu G, Zhao T, Mao Y, 2025, Enlightenment from U.S. Communication Network Development for Distributed Air Combat. Telecommunication Engineering, 65(12): 1957–1964.

[10] Yang K, Wang C, Wang B, 2025, Distributed Operations: Concepts, Development and Future Trends. China Military to Civilian Conversion, 2025(10): 23–24.