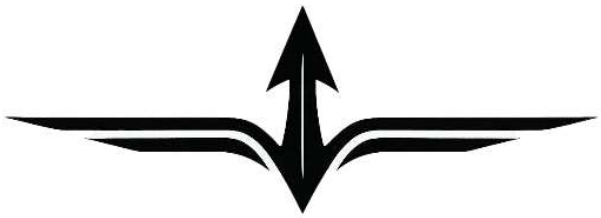
Chapter 9



Multi-Domain Operations in System-Centric Warfare

Lami Kim

"Victory in future combat will depend less on individual capabilities and more on integrated strengths of a connected network available for coalition leaders to employ."[2]

— General David L. Goldfein
U.S. Air Force Chief of Staff (2016–2020)

The Emerging Multi-Domain Battlespace

The strategic environment shaping the United States' defense posture is undergoing its most significant transformation since the end of the Cold War. For the first time in decades, the U.S. military faces adversaries capable of contesting its power across every

doi.org/10.71236/d9h03gyw

domain—land, sea, air, space, cyberspace, and the electromagnetic spectrum. These competitors, most notably the People's Republic of China, are leveraging advanced technologies, integrated operational concepts, and widening spheres of influence to challenge American military freedom of action in ways that place unprecedented pressure on traditional U.S. advantages.

This shift is most acute in the Indo-Pacific—the world's most consequential theater and the central arena of today's contested strategic environment. Geography, technology, and regional security dynamics converge here to create conditions in which rapid, coordinated, cross-domain operations are becoming the defining feature of modern conflict. As Admiral Samuel J. Paparo Jr., Commander of U.S. Indo-Pacific Command, emphasized in his April 2025 Posture Statement, the People's Liberation Army (PLA) is now conducting "persistent multi-domain pressurization activities" around Taiwan and throughout the region.[3] These operations integrate air, maritime, cyber, and space assets to impose continuous pressure, normalize coercive behavior, and rehearse the very joint operations the PLA would employ in crisis or conflict.

Against this backdrop, the U.S. Joint Force faces a profound challenge: it must not only maintain capability superiority but evolve in ways that allow it to outpace and out-adapt adversaries whose operational models are specifically designed to exploit seams between U.S. domains and services. The United States can no longer rely on dominance within individual domains; it must instead generate advantage through the synchronized employment of effects across all domains—creating dilemmas that overload adversary decision cycles and enabling U.S. forces to operate at a tempo and scale that competitors cannot match.

This new logic of warfare is captured in the doctrine of Multi-Domain Operations (MDO). MDO is not simply an update to joint operations, nor is it driven solely by new technologies. Rather, it represents a fundamental rethinking of how the Joint Force conceives of combat power. It demands integrating capabilities across domains through shared data architectures, resilient communications, distributed sensors, autonomous and semi-autonomous systems, and human-machine teaming. At its core, MDO seeks to achieve *convergence*—the ability to combine cross-domain effects simultaneously and precisely to penetrate, disintegrate, and exploit adversary defenses while maintaining the initiative.[4]

To enable this approach, the Department of War is developing a digital backbone known as the Combined Joint All-Domain Command and Control (CJADC2), an architecture designed to connect U.S. and allied sensors, decision-makers, and shooters across all domains. CJADC2 aims to give commanders the ability to sense, make sense, and act at the speed required for modern warfare.[5] By accelerating decision cycles and enabling distributed operations, CJADC2 enables MDO to become operationally achievable.

Yet this growing reliance on integrated networks also presents new vulnerabilities. China's emerging doctrine of *Systems Destruction Warfare* seeks to paralyze the U.S. military by targeting the very connective tissue—data flows, networks, communications, and sensing architecture—that enables the Joint Force to operate as an integrated system. In response, the United States must ensure that its integrated systems are resilient, redundant, and capable of

maintaining operational cohesion even when degraded by cyber, electronic, or kinetic attacks.

This chapter examines the defining military challenge of our era: China's system-centric approach to warfare and the United States' response through MDO and CJADC2. It analyzes the evolution of PLA doctrine, the capabilities supporting China's multi-domain strategy, the U.S. military's adoption of MDO, the architecture of CJADC2, and the institutional and technological challenges that remain. Ultimately, it argues that America's strategic edge in the era of competitive multipolarity will depend on its ability to integrate forces across all domains—coherently, rapidly, and in close partnership with allies—while safeguarding the networks and systems that enable such integration.

China's System-Centric Theory of Warfare

China's challenge to the United States does not stem from any single breakthrough capability but from a fundamental reengineering of how the PLA conceptualizes, organizes, and conducts modern warfare. At the core of this transformation is a doctrinal conviction that future conflicts will be decided by the side capable of maintaining the integrity of its own operational system while degrading or collapsing that of its opponent. In this framework, warfare is no longer a contest of platforms or even domains—it is a contest between competing systems of systems.

This shift can be traced to the early 1990s, when PLA strategists studying the U.S. victory in the Gulf War concluded that America's advantage lay not simply in superior aircraft or precision weapons, but in its ability to link forces through integrated command and

control, satellite-enabled sensing, joint fires, and real-time data fusion.[6] These assessments marked the PLA's recognition that the coherence and responsiveness of a military's operational architecture mattered more than the performance of individual platforms.

Guided by this insight, Beijing embarked on a decades-long effort to "informatize" the PLA.[7] This modernization replaced legacy analog systems with digital networks, expanded satellite communications, strengthened cyber and electronic warfare capabilities, and invested in long-range precision strike. Early milestones—including the fielding of the CSS-6 and CSS-7 ballistic missiles, the development of advanced air-defense systems, and the successful 2007 anti-satellite test—signaled China's willingness to contest domains underpinning U.S. global operations.[8]

As these capabilities matured, they converged into a broader strategic logic known as *Systems Destruction Warfare*.[9] This doctrine asserts that technologically advanced adversaries such as the United States rely on tightly integrated C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. If those networks can be disrupted—through cyber intrusion, electronic warfare, anti-satellite operations, precision strikes, or attacks on data flows—the U.S. Joint Force can be rendered disoriented, fragmented, and unable to coordinate operations at scale. China's aim is therefore not to destroy every ship or aircraft, but to paralyze the systems that enable U.S. forces to function coherently.[10]

To transform this vision into a warfighting reality, China undertook major organizational reforms. The creation of the

Strategic Support Force (SSF) in 2015 unified space, cyber, and electronic warfare under a single entity responsible for enabling joint operations.[11] In 2024, Beijing dissolved the SSF and established the Information Support Force (ISF), elevating information dominance as the central organizing principle of China's future force. The ISF is tasked with building, defending, and integrating the PLA's information architecture—reinforcing the notion that victory hinges on speed, resilience, and survivability of a force's networks, not on platform inventories alone.[12]

China gave operational form to this system-centric worldview in 2021 with the articulation of *Multi-Domain Precision Warfare* (MDPW).[13] MDPW is designed to execute *Systems Destruction Warfare* at scale.[14] It seeks to fuse multi-domain data through artificial intelligence and machine learning to produce targeting information faster than an adversary can respond. In PLA doctrine, precision extends beyond striking targets accurately; it involves orchestrating cyberattacks, electronic warfare, space control, unmanned systems, and long-range fires in coordinated sequences that disable the critical nodes of an adversary's operational system.[15] Key vulnerabilities include satellite uplinks, logistics hubs, data centers, command nodes, naval radars, and the gateways that connect U.S. service networks.[16]

By the early 2020s, China's modernization had entered the era of intelligentization—a shift that expands beyond informatization by emphasizing autonomous systems, machine-to-machine communication, human-machine teaming, and AI as core drivers of operational advantage. PLA publications increasingly describe future warfare as operating at "machine speed,"[17] where decision advantage accrues to the military capable of processing data rapidly,

generating real-time targeting solutions, and executing synchronized cross-domain effects before an opponent can respond. China's Military-Civil Fusion strategy accelerates this trajectory by enabling the rapid transfer of commercial innovations—in telecommunications, quantum research, robotics, and big data analytics—into practical applications.[18]

Together, these developments depict a military designed not to mirror the U.S. Joint Force but to undermine the architecture that enables it. China's system-centric approach seeks to complicate U.S. power projection, disrupt the data flows that sustain American lethality, and fracture the operational coherence of U.S. and allied forces in the Indo-Pacific. It is this architectural, integrated, cross-domain challenge that has compelled the Department of War to adopt MDO and build a resilient, allied-integrated command and control system through CJADC2.[19]

The U.S. Response: MDO and CJADC2

The United States' response to China's system-centric approach to warfare represents the most consequential transformation in American warfighting since the end of the Cold War. After two decades focused on counterinsurgency and stability operations, the Department of War has reoriented toward adversaries capable of contesting U.S. operations across every domain. The imperative is clear: if Beijing aims to fracture the U.S. operational system, then the United States must build one that is faster, more resilient, more distributed, and more coherently integrated than any it has fielded before.

This logic underpins Multi-Domain Operations (MDO), the Joint Force's doctrinal framework for synchronizing land, maritime, air, space, cyber, and electromagnetic capabilities into a unified operational construct.[20] MDO is not simply a modernization program or a technological update. It reflects a fundamental shift in the American conception of combat power—from massing forces to massing effects; from deconflicted domain operations to cross-domain convergence; and from linear kill chains to distributed kill webs that preserve operational tempo even when disrupted.[21]

The intellectual lineage of MDO traces to the mid-2010s, when U.S. defense leaders began confronting the operational consequences of China's maturing precision-strike, cyber, electronic warfare, and counter-space capabilities. In 2017, General David Perkins introduced the early concept of "Multi-Domain Battle,"[22] which evolved the following year into *The U.S. Army in Multi-Domain Operations 2028*.[23] This framework anticipated a battlefield in which adversaries could jam communications, degrade satellites, target logistics nodes, and attack C4ISR networks across the theater. It argued that future U.S. forces would need to penetrate adversary defenses, disintegrate their operational systems, and exploit the resulting gaps through converged, cross-domain effects.[24]

Today, the multi-domain fight is no longer theoretical. As noted in Admiral Paparo's 2025 Posture Statement, the PLA's persistent multi-domain pressurization activities around Taiwan illustrate that China is already rehearsing integrated operations designed to compress decision timelines and test U.S. and allied coherence.[25] These patterns underscore why the Joint Force must operate as an integrated network rather than a set of parallel components. U.S. and

allied exercises now reflect this shift. Valiant Shield and Pacific Steller fuse naval, air, and space forces with cyber and electronic warfare elements, stressing the ability to share targeting data and maintain a common operating picture under contested conditions.[26] The deployment of Autonomous Multi-Domain Launchers (AML) to Palau illustrates the emerging reality: unmanned launchers cued by distributed sensors can generate long-range fires from austere locations, presenting adversaries with dilemmas while enhancing the survivability and flexibility of U.S. forces.[27]

To operationalize MDO at scale, the Department of War is building Combined Joint All-Domain Command and Control (CJADC2), the digital architecture that enables multi-domain convergence across the Joint Force.[28] By linking sensors, command elements, and shooters across services, domains, and allied forces, CJADC2 underpins the ability to sense, make sense, and act under contested conditions.

Sensing involves a wide constellation of ISR and open-source assets that discover, collect, correlate, and aggregate data from friendly, neutral, and adversary sources across all domains. *Making sense* is the process of transforming that data into knowledge using AI-enabled analytics to understand and predict adversary intentions. Finally, *acting* is the ability to rapidly disseminate decisions to the Joint Force, underpinned by the tenets of mission command, which allows commanders to preserve the initiative even in C2-degraded environments.[29]

CJADC2 is therefore not a single system but a distributed architecture—a resilient, data-driven ecosystem designed to maintain coherence in contested environments. As Vice Chairman

of the Joint Chiefs of Staff, Admiral Christopher Grady explained, CJADC2 integrates the Joint Force along three axes: horizontally across all domains, vertically from strategic leaders to tactical operators, and internationally by linking allies and partners into a shared operating environment.[30]

This allied dimension is indispensable. Congress designated the Indo-Pacific as the priority theater for CJADC2 implementation,[31] and U.S. Indo-Pacific Command has since established the Joint Fires Network—a battle-management system designed to share real-time targeting information among U.S. and allied forces.[32] For the first time, the United States, Japan, Australia, and other partners are beginning to experiment inside a common architecture designed to synchronize cross-domain fires at the multinational level.

Yet the very integration that strengthens the Joint Force also creates vulnerabilities. China's doctrine of *Systems Destruction Warfare* is explicitly designed to paralyze the networks, data flows, and decision-support systems upon which CJADC2 depends. Recognizing this, the Department of War is shifting from linear kill chains—optimized for permissive environments—to resilient kill webs—distributed networks that degrade gracefully rather than catastrophically. In a kill web, the loss of a single node must be automatically offset by alternative nodes, ensuring that the Joint Force can continue sensing, deciding, and acting while under attack.[33]

In this sense, MDO and CJADC2 are not merely modernization initiatives; they are the structural and conceptual foundations required to preserve the integrity of America's operational system against adversaries who seek to dismantle it. This transformation is

both urgent and unavoidable. In an Indo-Pacific theater defined by long distances, contested domains, and rapid technological change, the future of American deterrence—and the United States' ability to project power—will depend on how effectively it can integrate forces, fuse information, and converge effects at a speed, scale, and level of resilience that China cannot match.

Operationalizing Multi-Domain Operations

The shift toward MDO is not confined to doctrine or digital architecture; it is taking tangible form in the operational concepts now reshaping the Joint Force. These concepts reflect a shared recognition across the services that the United States must be able to sense, decide, and act in a highly contested environment where China aims to degrade communications, disrupt logistics, and fracture operational coherence. Rather than relying on large, centralized formations, the emerging model emphasizes dispersion, mobility, and the ability to generate cross-domain effects from networks of smaller, harder-to-target nodes.

The Army's Multi-Domain Task Forces (MDTF) embody this evolution most directly. Designed initially to counter anti-access and area denial (A2/AD) challenges in the Indo-Pacific, MDTFs integrate long-range fires, electronic warfare, space support, cyber capabilities, unmanned systems, and deep-sensing platforms under a single headquarters. This convergence enables MDTFs to penetrate adversary systems, degrade critical nodes, and create windows of opportunity that facilitate joint force maneuver.[34] Recent exercises across the Western Pacific have demonstrated their ability to synchronize sensing, targeting, and precision fires over

long distances—an essential requirement in a theater defined by vast geography and contested communications.

A parallel transformation is underway within the Air Force through Agile Combat Employment (ACE). ACE departs from the traditional reliance on large, centralized air bases, which are highly vulnerable to precision missile attacks. Instead, it disperses aircraft across networks of smaller, austere airfields, complicating adversary targeting while sustaining operations through flexible refueling, pre-positioned materiel, and a more agile logistics footprint. ACE also demands resilient communications and tighter integration with cyber and space assets, as dispersed air operations must be continuously informed by distributed sensing and real-time threat updates.[35]

The Marine Corps' Expeditionary Advanced Base Operations (EABO) concept applies similar logic to the maritime domain. EABO envisions small, highly mobile units operating across island chains, coastal zones, and key chokepoints throughout the Indo-Pacific. From these positions, Marines can contribute to long-range fires, sensing and reconnaissance, dispersed logistics, and kill-web architectures that hold adversary forces at risk. Designed specifically for contested littorals, EABO leverages maritime terrain to complicate adversary targeting while enabling persistent joint presence in strategically decisive spaces.[36]

The Navy's evolving operational construct—Distributed Maritime Operations (DMO)—reinforces this broader shift toward a more dispersed and networked approach to warfighting. DMO reorganizes naval forces into smaller, distributed elements that coordinate through resilient networks to deliver effects across wider

distances. Integrated fires, unmanned surface and undersea vehicles, and autonomous ISR platforms expand the fleet's sensing and striking capacity while reducing risk to crewed ships. These innovations reflect the Navy's recognition that persistent multi-domain pressure from the PLA requires a flexible, adaptive, and survivable force posture.[37]

Together, these operational concepts demonstrate how the Department of War is institutionalizing multi-domain integration across the Joint Force. Each service contributes differently, yet all move toward a common operational logic: dispersion rather than concentration, integration rather than isolation; resilience rather than fragility; and tempo rather than reaction. As these approaches mature, they increasingly anchor U.S. deterrence in the Indo-Pacific not simply by projecting power from afar, but by operating persistently, jointly, and in concert with allies inside the contested spaces where strategic outcomes will be decided.

Challenges to Implementing MDO and CJADC2

Even as the United States embraces MDO and builds the CJADC2 architecture, the transformation remains uneven and incomplete. A paradox sits at the center of this modernization effort: the same integration that enables multi-domain convergence also magnifies the system's complexity, fragility, and overall attack surface—essentially, the number of points an adversary can target. As the Joint Force becomes more interconnected, it becomes simultaneously more vulnerable. Whether MDO becomes a decisive advantage or an unfulfilled ambition will hinge on how effectively this tension is managed.

One of the more persistent obstacles is integrating technology. The Department of War is attempting to connect an extraordinary range of sensors, shooters, networks, and data repositories—many of which are legacy systems never designed to interact with one another. Another challenge is connectivity and interoperability. Proprietary data formats, incompatible waveforms, closed communication protocols, and divergent software architecture complicate even basic interoperability. Within a single service, continuous connectivity among platforms cannot always be guaranteed. Extending connectivity across the entire Joint Force—each service with distinct cultures, requirements, and acquisition pathways—multiplies the challenge.[38]

These difficulties intersect with a structural gap between technological ambition and acquisition reality. MDO and CJADC2 rely on the rapid deployment of digital architectures, AI-enabled applications, autonomous platforms, and resilient communication networks. Yet the Department continues to struggle with software modernization,[39] lengthy procurement cycles, and the transition from promising prototypes to sustainable fielded capabilities. The commercial industry, by contrast, iterates at a pace shaped by agile development, market incentives, and rapid user feedback. The Department increasingly relies on dual-use commercial technologies for sensing, networking, and data analytics, even as it seeks to protect military functions from vulnerabilities embedded in global supply chains—not an easy balance to maintain.[40]

Interoperability with allies adds another layer of complexity. MDO in the Indo-Pacific cannot be executed by the United States alone. Effective deterrence requires synchronized operations with Japan, Australia, South Korea, the Philippines, and others. Yet each

ally maintains its own C2 architecture, classification rules, cybersecurity standards, data formats, and communications infrastructure. In the absence of shared data models, seamless information sharing remains elusive. Even among the closest intelligence partners, such as the Five Eyes, real-time, continuous data exchange cannot be assumed.[41] These seams create vulnerabilities that adversaries can exploit, complicating efforts to form a shared operating picture during periods of crisis or coercion.

Information security further constrains integration. The Joint Force must assume that adversaries will attempt to infiltrate or degrade the networks that enable MDO. But cybersecurity maturity varies across allied militaries, creating a weakest-link problem: a breach in one nation's network can compromise the integrity of shared data. Stricter security protocols reduce risk but restrict information sharing, while more permissive arrangements enhance operational fluidity but introduce potential vulnerabilities. Resolving this tension will likely remain one of the most significant challenges in implementing CJADC2.

The cognitive dimension of multi-domain integration presents another critical hurdle. MDO compresses timelines, accelerates decision cycles, and requires commanders at every echelon to interpret complex data sets while coordinating cross-domain actions under conditions of uncertainty. As AI systems automate sensing and speed data fusion, the burden of human decision-making increases. Leaders must not only understand the outputs of advanced analytics—they must determine when to trust them, when to override them, and how to integrate them into joint and multinational operations. Without major shifts in training, doctrine, and human-machine teaming, the risk increases that technological

capabilities will outpace the Joint Force's ability to employ them effectively.[42]

Meanwhile, the inherent vulnerability of connected systems remains a defining concern. China's doctrine of *Systems Destruction Warfare* is tailored to target the connective tissue of U.S. operations—satellite constellations, communication links, logistics nodes, command centers, and data repositories. As Beijing fields more advanced cyber, electronic warfare, counter-space, and precision-strike capabilities, the Joint Force must assume that its networks will be degraded early in any conflict. This reality drives the transition from linear *kill chains* to distributed *kill webs.* Designed from the outset with redundancy, dispersion, and graceful degradation in mind, kill webs ensure that the loss of a single node does not collapse the system but triggers rapid reconstitution and rerouting through alternative pathways, enabling continued sensing, making sense, and acting under fire.

Beneath these technical and operational challenges lies a deeper institutional one: culture and organizational inertia. Implementing MDO and CJADC2 requires reforms that extend beyond technology to doctrine, planning, acquisitions, and inter-service cooperation. For decades, service-centric approaches to budgeting, requirements, and operational planning have shaped the U.S. military's institutional behaviors. Multi-domain integration demands the opposite—horizontal coordination and shared priorities across services, domains, and theaters. Overcoming inertia will require sustained senior-leader direction, clear prioritization, and political support commensurate with the scale of the challenge.[43]

Taken together, these constraints underscore that MDO and CJADC2 are not merely modernization initiatives; they represent a profound redefinition of how the United States fights. The Joint Force must build an operational system capable of converging effects across domains faster than adversaries can disrupt it—while ensuring it remains resilient under sustained attack. Achieving this balance will shape the credibility of U.S. deterrence and the effectiveness of American warfighting in an Indo-Pacific theater where speed, integration, and adaptability increasingly define strategic advantage. Whether the United States can meet this challenge will determine its ability to maintain an operational edge in an era defined by multi-domain threats and system-centric competition.

Conclusion: Preserving Advantage in System-Centric Conflict

The contest between the United States and China is not defined by platform inventories or superiority in any single domain. It is a struggle between competing theories of modern warfare: one that seeks to dismantle the adversary's operational architecture, and one that seeks to integrate and harden it. China's decades-long modernization—through informatization, intelligentization, *Systems Destruction Warfare*, and *Multi-Domain Precision Warfare*—has produced a force designed to probe, degrade, and potentially paralyze the networks that enable U.S. joint warfighting. The PLA's objective is clear: collapse the decision-making, sensing, and command-and-control structures that bind the Joint Force into a coherent whole.

The United States has responded with a transformation of its own, centered on MDO and facilitated by the architecture of CJADC2. These concepts reconceive how the Department of War generates and applies combat power in an era defined by contested information environments, long-range precision threats, and adversaries capable of synchronizing actions across domains. MDO rests on the recognition that operational advantage no longer derives from dominance in any single domain, but from the ability to converge effects across all domains, compress decision cycles, and create dilemmas an adversary cannot manage. CJADC2 provides the connective tissue that turns this theory into practice: a distributed, resilient network designed to enable U.S. and allied forces to sense, make sense, and act faster than adversaries attempting to fracture the system.

Realizing this vision, however, remains an unfinished task. Interoperability shortfalls, fragile software systems, disjointed acquisition paths, and uneven progress in networking technologies continue to slow implementation. Bureaucratic inertia and divergent service cultures complicate the transition from legacy concepts to integrated warfighting. These challenges are magnified when viewed through an allied lens: Indo-Pacific partners operate with distinct systems, data standards, and security protocols, even as they remain central to U.S. strategy. At the same time, the very connectivity required for multi-domain integration introduces vulnerabilities that China seeks to exploit. The PLA's emphasis on targeting U.S. communications, logistics, satellites, and decision-support tools underscores the strategic risk inherent in a force dependent on rapid information flows.

The United States is not standing still. Emerging operational concepts across the services—MDTF, ACE, EABO, and DMO—reflect a broader shift toward dispersion, agility, and cross-domain integration. These approaches demonstrate how MDO is being translated into practice, enabling U.S. forces to operate effectively within contested environments, generate precision effects from distributed nodes, sustain tempo despite degraded communications, and demonstrate an ability to survive and adapt under pressure. They also anchor a more persistent and integrated posture in the Indo-Pacific, reinforcing deterrence by signaling that the Joint Force cannot be easily fractured or isolated.

The decisive question, therefore, is whether the United States can integrate technology, doctrine, and allied cooperation into a coherent, resilient warfighting system—one capable of withstanding the pressure of system-centric conflict. In an era defined by multi-domain threats, the operational advantage will belong not to the actor with the most advanced platforms, but to the actor with the most adaptive architecture: the force that can maintain coherence when challenged, restore function when disrupted, and act at speed in an environment designed to induce paralysis.

The stakes are significant. The Indo-Pacific remains the center of gravity for global economics, security, and technological innovation. The credibility of U.S. commitments, the confidence of regional partners, and the stability of the broader international system depend on the United States' ability to preserve its operational edge. MDO and CJADC2 form the foundation of that effort. They offer not only a pathway to prevailing in conflict but also a framework for sustaining peace by ensuring that potential adversaries understand that the United States and its allies can

respond quickly, coherently, and decisively across every domain of warfare.

Endnotes

[1] The author is solely responsible for the views expressed in this publication, which do not necessarily represent the official policy or position of the Daniel K. Inouye Asia-Pacific Center for Security Studies, the U.S. Department of War, or the U.S. government.

[2] Charles Pope, "Goldfein Details Air Force's Move Toward a 'Fully Networked,' Multi-Domain Future," U.S. Air Force, September 17, 2019, https://www.af.mil/News/Article-Display/Article/1963310/goldfein-details-air-forces-move-toward-a-fully-networked-multi-domain-future/.

[3] Samuel J. Paparo Jr., "Statement of Admiral Samuel J. Paparo Commander, U.S. Indo-Pacific Command, U.S. Indo-Pacific Command Posture" (April 2025), 3, https://armedservices.house.gov/uploadedfiles/indopacom_posture_statement_2025.pdf.

[4] Department of the Army, *TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations, 2028*, (Fort Eustis, VA: U.S. Army Training and Doctrine Command, December 6, 2018) 20, https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

[5] Chief Digital and Artificial Intelligence Office, "Combined Joint All-Domain Command and Control (CJADC2)", accessed December 12, 2025, https://www.ai.mil/Initiatives/CJADC2/.

[6] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), 10, https://www.rand.org/pubs/research_reports/RR1708.html.

[7] Engstrom, Systems Confrontation and System Destruction Warfare, 11.

[8] Council on Foreign Relations, "China's Anti-Satellite Test," February 22, 2007, https://www.cfr.org/backgrounders/chinas-anti-satellite-test.

[9] Engstrom, *Systems Confrontation and System Destruction Warfare*, 15–18; Edmund J. Burke et al., *People's Liberation Army Operational Concepts*, (Sana Monica, CA: RAND Corporation, 2024) 22, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf.

[10] Engstrom, Systems Confrontation and System Destruction Warfare, 17; Burke et al., People's Liberation Army Operational Concepts, 8.

[11] John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, China Strategic Perspectives, no. 13 (Washington, DC: National Defense University Press, 2018), 1, 5, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

[12] Tye Graham and Peter W. Singer, "The Future of China's New Information Support Force," *Defense One*, February 2, 2025, https://www.defenseone.com/ideas/2025/02/future-chinas-new-information-support-force/402677/.

[13] U.S. Department of Defense (DOD), *Military and Security Developments Involving the People's Republic of China 2022*, Annual Report to Congress (Washington, DC: DOD, 2022), 39, https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF

[14] Joel Wuthnow, "System Destruction Warfare and the PLA," briefing for Keystone, National Defense University, Institute for National Strategic Studies, updated June 2025, 3, https://keystone.ndu.edu/Portals/86/PLA%20Systems%20Attack%20-%20Keystone%20-%20JW%20update%20Jun%2025.pdf.

[15] Wuthnow, "System Destruction Warfare and the PLA," 4.

[16] U.S. DOD, *Military and Security Developments Involving the People's Republic of China 2024*, Annual Report to Congress (Washington, DC: DOD, 2024), 35–36, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

[17] U.S. DOD, *Military and Security Developments Involving the People's Republic of China 2023*, Annual Report to Congress, (Washington, DC: DOD, 2023), 97, https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[18] U.S. Department of State, "Military-Civil Fusion and the People's Republic of China," May 2020, https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf; U.S. DOD, *Military and Security Developments Involving the People's Republic of China 2024,* 24–30.

[19] U.S. DOD, "DoD Announces Release of JADC2 Implementation Plan," March 17, 2022, https://www.war.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/.

[20] Department of the Army, *TRADOC Pamphlet 525-3-1*, vi–xii, 17–20.

[21] DARPA, "Creating Cross-Domain Kill Webs in Real Time," September 18, 2020, https://www.darpa.mil/news/2020/cross-domain-kill-webs; Katrine Lund-Hansen and Jeff Reilly, "The Multi-Domain Operations Approach to Intermediate PME," *War Room* (U.S. Army War College), November 1, 2024, https://warroom.armywarcollege.edu/articles/competencies-6/.

[22] David G. Perkins, "Multi-Domain Battle: Driving Change to Win in the Future," *Military Review* (July-August 2017), https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2017/Perkins-Multi-Domain-Battle/.

[23] Department of the Army, *TRADOC Pamphlet 525-3-1*

[24] Department of the Army, *TRADOC Pamphlet 525-3-1*.

[25] Paparo, "Statement of Admiral Samuel J. Paparo Commander," 3.

[26] Jack Scypinski, "France, Japan, U.S. Partner in Multi-Large Deck Event in Philippine Sea," February 6, 2025, https://www.cpf.navy.mil/Newsroom/News/Article/4056329/france-japan-us-partner-in-multi-large-deck-event-in-philippine-sea/; U.S. Pacific Fleet, "Allies Come Together in the Indo-Pacific: Valiant Shield 24," June 4, 2024, https://www.cpf.navy.mil/Newsroom/News/Article/3796554/allies-come-together-in-the-indo-pacific-valiant-shield-24/.

[27] John Carter, "U.S. Joint Forces Strengthen Capabilities and Partnerships in Palau During Valiant Shield 24," July 20, 2024, *USINDOPACOM Stories*, https://www.pacom.mil/Media/NEWS/Article/3827711/us-joint-forces-strengthen-capabilities-and-partnerships-in-palau-during-valian/.

[28] U.S. DOD, "DoD Announces Release of JADC2 Implementation Plan."

[29] U.S. DOD *Summary of the Joint All-Domain Command and Control (JADC2) Strategy* (Washington, DC: DOD, 2022): 4–5, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.

[30] Christopher W. Grady, "Sharpening Our Competitive Edge," *Joint Force Quarterly*, 2023, 20, https://ndupress.ndu.edu/Joint-Force-Quarterly/Joint-

Force-Quarterly-111/Article/Article/3569518/sharpening-our-competitive-edge-honing-our-warfighting-capabilities-through-the/.

[31] National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, § 1504 (2023), https://www.congress.gov/bill/118th-congress/house-bill/2670.

[32] John C. Aquilino, "*Statement of Admiral John C. Aquilino, U.S. Navy, Commander, U.S. Indo-Pacific Command, on U.S. Indo-Pacific Command Posture*," March 18, 2024, 4, 24–27, https://www.armed-services.senate.gov/imo/media/doc/aquilino_statement.pdf.

[33] Heather Penney, *Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition*, Mitchell Institute Policy Paper no. 40 (Arlington, VA: Mitchell Institute for Aerospace Studies, May 2023), https://www.mitchellaerospacepower.org/app/uploads/2023/05/Scale_Scope_Speed_Survivability_-KillChain_-Policy_Paper_40-New.pdf; U.S. DOD *Summary of the JADC2 Strategy*, 3–4, 8.

[34] Andrew Feickert, *The Army's Multi-Domain Task Force (MDTF)*, CRS In Focus 11797 (Washington, DC: Congressional Research Service, updated December 17, 2025), https://www.congress.gov/crs-product/IF11797; Charles McEnany, "Multi-Domain Task Forces: A Glimpse at the Army of 2035," *AUSA Spotlight* 22-2 (March 2, 2022), https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035.

[35] Luke A. Nicastro, *Defense Primer: Agile Combat Employment (ACE) Concept*, CRS In Focus, IF12964 (Washington, DC: Congressional Research Service, June 24, 2024), https://www.congress.gov/crs-product/IF12694.

[36] Jim Lacey, "The 'Dumbest Concept Ever' Just Might Win Wars," *War on the Rocks*, July 29, 2019, https://warontherocks.com/2019/07/the-dumbest-concept-ever-just-might-win-wars.

[37] Ronald O'Rourke, *Defense Primer: Navy Distributed Maritime Operations (DMO) Concept*, CRS In Focus IF 12599 (Washington, DC: Congressional Research Service, December 4, 2025), https://www.congress.gov/crs-product/IF12599.

[38] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020); U.S. Government Accountability Office, *Defense Command and Control: Further Progress Hinges on Establishing a Comprehensive Framework*, Report to Congressional Committees, GAO-25-106454, (Washington, DC: GAO, April 2025, https://files.gao.gov/reports/GAO-25-106454/index.html.

[39] U.S. GAO, *Defense Command and Control* GAO-25-106454, 12–15.

[40] Sam Moyer, "Encouraging Private Investment in Defense Takes Strong Toolkits," *National Defense*, August 6, 2025, https://www.nationaldefensemagazine.org/articles/2025/8/6/emerging-technology-horizons-encouraging-private-investment-in-defense-takes-strong-toolkits.

[41] Daniel Byman, *Improving U.S. Intelligence Sharing with Allies and Partners*, CSIS Warfare, Irregular Threats, and Terrorism Program (Washington, DC: CSIS, January 2025), 4, 15, 21, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-01/250128_Byman_Intelligence_Sharing.pdf.

[42] U.S. DOD Summary of the JADC2 Strategy, 3, 8.

[43] Sigma Defense *A CJADC2 Primer: Delivering on the Mission of "Sense, Make Sense, and Act"* (September 2023), https://sigmadefense.com/wp-content/uploads/2023/09/CJADC2-White-Paper-Primer5.pdf.