Joint-All Domain Operations is Missing All-Domain Command & Control Support

Date Submitted: 15 MAY 2020

Word Count: 3,352 words

A paper submitted to the Faculty of the United States Naval War College Newport, RI in partial satisfaction of the requirements of the Department of Joint Military Operations.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
	FINAL	N/A

4. TITLE AND SUBTITLE
Joint-All Domain Operations is Missing All-Domain Command & Control Support

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Scott, Kyle D., MAJ, USA

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

A joint force command, tasked with defeating a modern military with comparable warfighting capabilities in a traditional war, will primarily require command and control support (C2S) conveyed by both cyberspace and the electro-magnetic spectrum (EMS) to converge joint cross-domain effects and preserve the advantages offered by network-enabled operations. The Joint Chiefs of Staff will publish the Joint-All Domain Operations (JADO) concept by the end of 2020. This paper uses the US Army's Multi-Domain Operations (MDO) concept as a source document to critique what the JADO concept may include. Specifically, the MDO concept did not appreciate or highlight the necessity of CS2 and network-enabled operations despite its tacitly documenting twenty-eight dependencies on communication systems and its proven value during Operations Enduring and Iraqi Freedom. CS2 and network-enabled operations are essential to generating the combat power necessary to deter and defeat, if necessary, a numerically superior and near-peer competitor like the People's Republic of China. Further, the paper explores the PRC's military strategy for defeating the US, Opposing Operational System, and juxtaposes it with MDO. Finally, it provides doctrine, training, and joint functions recommendations for the US to prevail in Joint All-Domain Operations.

15. SUBJECT TERMS (Key words)
JADO, MDO, C2, C2S, PRC, China, all-domain, multi-domain, network-enabled

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Director, Writing Center
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	N/A		**19b. TELEPHONE NUMBER** *(include area code)* 401-841-6499

Standard Form 298 (Rev. 8-98)

A joint force command, tasked with defeating a modern military with comparable warfighting capabilities in a traditional war, will primarily require command and control support (C2S) conveyed by both cyberspace and the electro-magnetic spectrum (EMS) to converge joint cross-domain effects and preserve the advantages offered by network-enabled operations.[1] The Department of Defense-wide effort to produce a new joint warfighting concept for deterring potential adversaries, like the People's Republic of China (PRC), by the end of 2020, is being led by General John E. Hyten, Vice Chairman of the Joint Chiefs of Staff.[2] The joint concept has only recently been named by the Secretary of the US Air Force (USAF), the Honorable Barbara Barrett, during the Fiscal Year 2021 USAF Posture Statement, "Joint All Domain Operations (JADO)" and there is little published under this moniker.[3] Therefore, this paper will largely explore and critique the JADO concept based on the closely related US Army concept known as Multi-Domain Operations (MDO) and juxtapose it with the People's Liberation Army's Opposing Operational System (OOS) concept for modern warfare.[4]

Successful MDO rest on three tenets: a calibrated force posture, multi-domain formations, and convergence. A calibrated force posture involves staging and having ready the

[1] JP 1 defines Traditional War "as a violent struggle for domination between nation-states or coalitions and alliances of nation-states. With the increasingly rare case of formally declared war, traditional warfare typically involves force-on-force military operations in which adversaries employ a variety of conventional forces and special operations forces (SOF) against each other in all physical domains as well as the information environment (which includes cyberspace)." See: Dempsey 2017, x.

[2] The Secretary of Defense has also signaled that developing a new means to understand and triumph in modern conflict is a high priority by assigning a Defense Science Board Task Force to investigate the new dimensions of conflict during the summer of 2020. See: Griffin 2019, Hitchens 2020.

[3] Barrett and Goldfein 2020, 14.

[4] The USA has been developing their MDO concept since August 2016 when it was previously named Multi-Domain Battle and published its current incarnation under the Training Doctrine Pamphlet 525-3-1 dated December 6, 2018. Further, TP 525-3-1 Appendix E documents the linkages from MDO to published Joint Concepts and service concepts for the USN, USMC, and USAF. Lastly, the Secretary of Defense, Mark T. Esper, and CJCS, Mark A. Milley, approved TP 525-3-1 when they were the Secretary of the Army and the Army Chief of Staff. See: Townsend 2018, E-1; TRADOC 2018.

total force required to thwart any revisionist power's attempt at a *fait accompli* via surprise large-scale combat.[5] More specifically, it entails immediately available, or forward presence forces, able to blunt and delay initial aggressors until expeditionary forces surge forward to halt, then defeat, antagonists.[6]

Table 1. Current Tenets of Multi-Domain Operations

Calibrated Force Posture	Multi-Domain Formations	Convergence
Forward presence forces	Conduct independent maneuver	Cross-domain synergy
Expeditionary forces	Employ cross-domain fires	Layered options
National-level capabilities	Maximize human potential	Mission command/ disciplined initiative
Authorities		Multi-domain command and control (*not included on MDO Logic Map*)

Source: TRADOC Pamphlet 525-3-1 The US Army in Multi-Domain Operations 2028. See: Townsend 2018, v; Appendix A for the complete MDO Logic Map; Appendix F for an evolution of the proposed tenets for JADO.

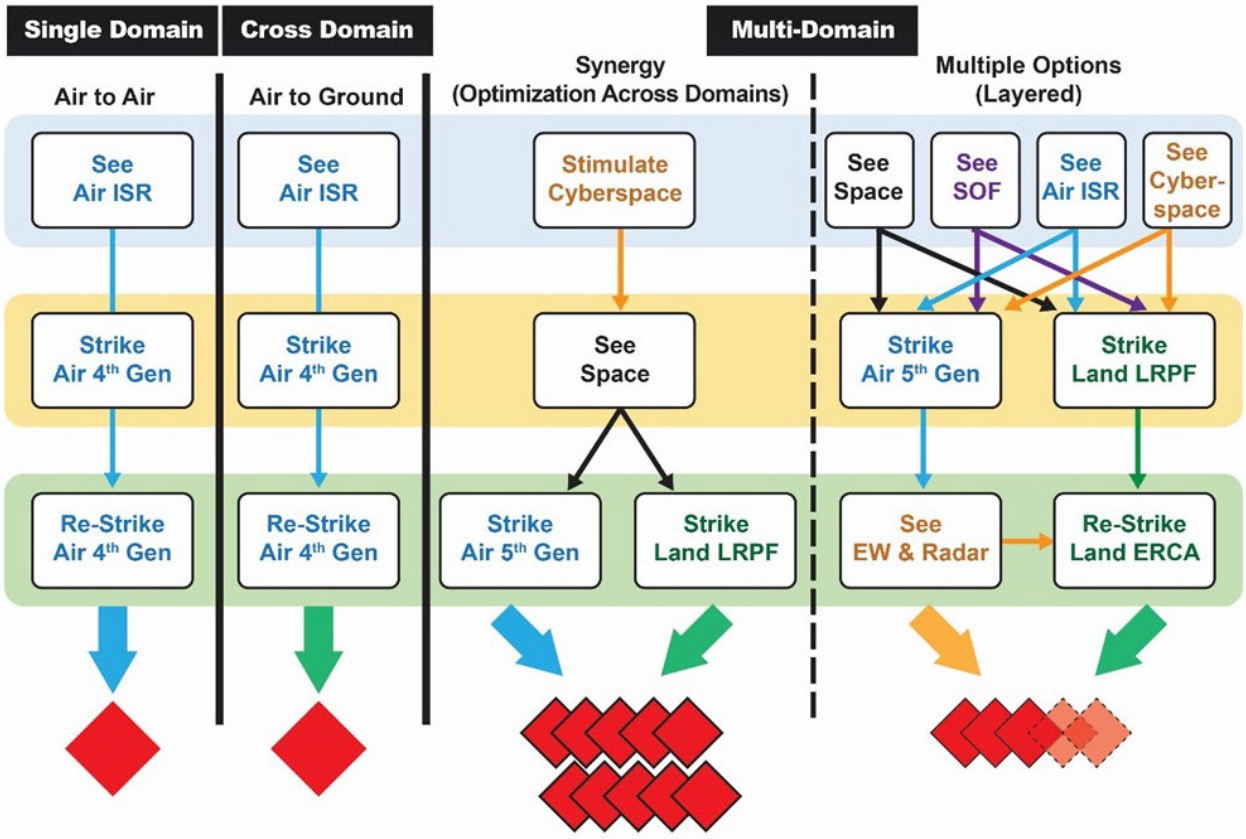
Multi-domain formations are designed, equipped, and trained to survive in contested environments. For instance, friendly forces threatened by enemy units with much shorter lines of communication (LOC), targeted by accurate fires, communications that are disconnected, intermittent, or limited (DIL), and numerically superior foes. MDO propose to overcome such challenges through independent maneuver, employing cross-domain fires, and maximizing human potential. Independent maneuver empowers US fighting forces to take the initiative to concentrate combat power at the decisive space by exploiting otherwise fleeting enemy vulnerabilities. This is expected despite that they may have "to sustain and protect themselves until they regain contact with adjacent and supporting units."[7] Cross-domain fires provide commanders access to a broader catalog of joint fires to penetrate more single domain focused

[5] Townsend 2018, 17-18.
[6] Calibrated force posture also includes national-level capabilities, and their requisite authorities (e.g., intelligence, cyberspace, space-based, and fires), focusing on supporting forward and expeditionary forces increasing their survivability by reducing the time required to bring together theater-level and above resources. See: Townsend 2018, 19.
[7] Townsend 2018, 19.

anti-access technologies and tactics. Finally, maximizing human potential recognizes that people must be carefully selected and rigorously trained to succeed in deterring or overcoming would-be enemies in such a hostile environment.

Convergence integrates all-domains' capabilities via the electro-magnetic spectrum (EMS) and the information environment (IE) to rapidly synergize fires resulting in enemy overmatch. US Army Training and Doctrine Command (TRADOC) illustrates how MDO use mission command to converge capabilities to generate cross-domain synergy from layered options.[8]

Figure 1. Converging capabilities to generate cross-domain synergy and layered options



Source: TRADOC Pamphlet 525-3-1 The US Army in Multi-Domain Operations 2028. See: Townsend 2018, 21.

[8] Note that references to '*Land'* Long-Range Precision Fires would include maritime (e.g., naval surface and subsurface) LRPF. See Figure 3-2: Townsend 2018, 21.

Convergence employs "stimulate-see-strike or see-strike combinations" that mitigate enemy command and control (C2), sensing, and fires.[9] 'Stimulate' suggests using military deception (MILDEC) or offensive actions to motivate enemy platforms to reveal their locations and intent. 'See' references sensing enemy assets via intelligence, surveillance, and reconnaissance means. 'Convergence' is intended to drastically reduce the time required for joint cross-domain integration, allow each echelon to benefit from cross-domain intelligence, sensors, and fires, and to reveal and more easily defeat the enemy's center of gravity.[10]

'Convergence' is MDO's lynchpin for success or failure and relies on robust communication systems. Calibrating force posture and streamlining strategic force projection is not a trivial matter. However, after nineteen years of conflict, it is a well-exercised function that the US is best able to accomplish. Likewise, multi-domain formations conducting independent maneuvers will capitalize on the US military's cultural affinity for disciplined initiative and decentralized execution. Nevertheless, independent maneuver is subject to well-informed leadership with shared tactical understanding that must be nourished by efficacious command and control support (C2S) or they will become emaciated. See Figure 2., Superior C2S. The sub-tenet, cross-domain fires, would have been better encapsulated under convergence and its sub-tenet, cross-domain synergy, rather than under multi-domain formations. Maximizing human potential is an enduring principle for any significant undertaking. Convergence, though, is pivotal and the most ambitious portion of the MDO concept.

[9] Townsend 2018, 20.
[10] "Multi-domain operations today rely on episodic synchronization… executing capabilities after days and weeks of synchronization… in future operations against a peer threat it will require rapid and continuous integration… integrating capabilities within hours." See: Hiu 2020, 23; Townsend 2018, 20-21.

Convergence is what enabled the 1st Infantry Division's staff, during Warfighter Exercise 19-04, a US Army Corps and Division level exercise validating MDO concepts, to overmatch the opposing force with multiple dilemmas. They were able to decimate long-range enemy artillery, multiple launch rocket systems, and tactical ballistic missile systems with division and corps air-ground fires integration.[11] They effectively forecasted the sequence and tempo of air assault forces supported by fires needed to keep the opposing force "stuck in the observe and orient" portion of John Boyd's OODA loop.[12] MDO concepts weathered the headquarters exercise well, but did not face the fog or friction of moving, maneuvering, or sustaining 50,000 actual troops. More importantly, there was no discussion of how DIL communications challenged the friendly's OODA loop or tested each echelon's ability to conduct independent maneuver.

Efficacious mission command is critical for all military endeavors, including convergence, and successful MDO would benefit from a sharp increase in staff and commanders' risk tolerances. However, convergence must have networked and assured communication systems (i.e., C2S) underpinning it as has been: tacitly called for in the MDO pamphlet, pervasively dictated in joint doctrine, and proven in DOD's most recent large-scale combat operations. TRADOC's MDO pamphlet touches on the importance of communication systems versus command and control twenty-eight times in the 102-page document–though mostly as asides.[13]

[11] The article's author, former 1st Infantry Division Chief of Staff, COL Taylor, was a key participant of "Warfighter Exercise 19-4 at Fort Hood. More than 1,400 Soldiers participated with support from more than 4,500 Soldiers, Department of the Army civilians and contractors." See: Taylor and Kay 2019; Thompson 2019.
[12] Former US Air Force Colonel John Boyd is attributed to the observation, orientation, decision, action (OODA) decision-making cycle. See: Alberts, Garstka, and Stein 1999, 292; Taylor and Kay 2019.
[13] See Appendix C: MDO Communication System Dependencies. Townsend 2018 vii, 19, 21, 23, 30, 34-35, 38-39, 43, B-1-B-2, C-5-C-6, C-9, D-1, D-4, D-5, F-2, F-3.

Areas that are dependent on communication systems include:

- independent maneuver,
- cross-domain fires,
- multi-domain C2,
- layered ISR,
- wide-area surveillance,
- decision-making,
- battle visualization, and
- orientation.

More, communication systems serve as key enemy targets; resilient friendly ones are necessary for deterrence.[14] The CJCS Joint Doctrine capstone and keystone publications, reference thirty-nine dependencies on communication systems such as the following: [15]

- Command and Control Support (C2S),
- multinational operations,
- a principle for interorganizational intelligence,
- common operating picture and shared understanding,
- intelligence collection and sharing,
- joint cyberspace operations,
- command-centric leadership,
- an essential element for joint logistics, and
- contingency planning.

Operation Anaconda, a part of Operation Enduring Freedom (OEF), and the Liberation of Iraq during Operation Iraqi Freedom (OIF) are two modern examples of US forces involved in full-scale combat that demonstrate the value and need for networked and assured communication systems. Both conflicts benefited from "extended reach communications and networked information technologies [which] significantly enhanced the ability of US Army commanders to make faster decisions, more easily exploit tactical opportunities, conduct coordinated maneuver while advancing further and faster than at any previous time, and more fully integrate and synchronize joint fires."[16] In Operation Anaconda, ground and air commanders, C2 aircraft,

[14] Additionally, TP 535-3-1 enumerates fourteen MDO capability requirements, five of which are related to communication systems, including: interoperability between all domains and partners, synchronization of forces in dense urban terrain, access to cyberspace information repositories, and resilient communication architectures and networks. Townsend 2018, vii, 19, 30, 38-39, B-1-B-2, D-1.
[15] Joint Publication 6-0 was excluded because it exclusively covers the Joint Communications System. See Appendix B: Joint Doctrine Capstone and Keystone Publications' Communication System Dependencies.
[16] Tisserand and Cammons 2003, ix.

tactical combat aircraft, and ground forces were networked to allow for an impromptu, seven day, close air support campaign that reversed an almost certain defeat for outnumbered and dispersed US forces.[17] In an exhaustive three-volume case study, the US Army War College's John B. Tisserand III and David Cammons led an effort that explains how network-enabled operations (NEO) allowed US Army V Corps and a joint team to rapidly defeat Iraqi military forces and caused the fall of the Ba'athist Regime in Baghdad.[18] For instance, V Corps fires and intelligence communities benefited from Hunter UAV feeds and shared information creating a common operating picture allowing the corps to execute five simultaneous attacks to deceive Iraqi forces and later secure Baghdad.

The DOD C4ISR Cooperative Research Program (CCRP) was proven correct when it postulated, two years before OEF, that NEO would allow "us to move from an approach based upon the massing of forces [solely contiguous operations] to one based upon the massing of effects [non-contiguous operations]."[19] In conflicts earlier than OEF and OIF, the US had limited communication and mobility capabilities. Thus, combat forces (and their enablers) had to be co-located to maintain and protect their LOCs, but also to mutually support and reinforce one another's maneuvers. "As a result, a geographically dispersed force was relatively weak and was unable to respond quickly to or mount a concentrated attack. Locational constraints also paced a force's ability to move rapidly while maintaining cohesion [i.e., communications] and logistics support."[20] For instance, a lack of networked communication systems forced unit commanders

[17] A local Pushtun militia, the Eastern Alliance, abandoned outnumbered US forces on the first day of battle for the Shahikot Valley to 700–1000 entrenched and heavily armed Taliban fighters occupying well-concealed and elevated, sometimes subterranean, fighting positions. See: Kugler 2006, 6, 10, 17-18.
[18] Network Centric Warfare (NCW) is the legacy term network-enabled operations (NEO) found in JP 6-0 Joint Communications System. O'Donohue 2017, I-5.
[19] Alberts, Garstka, and Stein 1999, 91.
[20] Alberts, Garstka, and Stein 1999, 90.

attempting to cope with the fog of war by battle-tracking each element's (higher, lower, and adjacent) geographic relationship by hand with the aid of translucent overlays, maps, and grease pencils. The latency between by-hand battle-tracked friendly locations and reality could vary from, at best, 15 minutes to hours. Ground commanders struggled with the certainty of their own elements' positions, much less appreciating where other friendly or enemy units might be in relation to their own.[21] Uncertainty causes commanders to limit their freedom of maneuver (e.g., audacity and tempo) and slows and restricts organic fires for fear of fratricide.

The MDO concept plans to prevail despite DIL communications through multi-domain command & control composed of "a resilient technical architecture, flexible command relationships, and multi-domain control measures."[22] Mission command, intent-based synergy, and independent maneuver can bridge gaps in commander-centric leadership. However, tactical units must continue to receive the minimum essential information necessary to orient themselves on the battlefield.[23] An example of essential information is assured precision navigation and timing and the resultant Friendly Force Tracking (FFT) that is then widely distributed and overlaid onto a joint common operating picture.[24] During V Corps' drive towards Baghdad, a task force commander with the advantage of having a tank mounted Blue Force Tracking system, understood, without being directed, the need to transition from securing a bridgehead to a hasty defense. The TF commander noticed when an adjacent brigade combat team (BCT) changed their direction of travel towards his position. Accordingly, he pushed his TF five kilometers

[21] Tisserand and Cammons 2003, 6.
[22] Townsend 2018, 23.
[23] See JP 3-0 Joint Operations for more on commander-centric leadership. See: Scott 2018, II-1, II-2.
[24] JP 3-09 Joint Fire Support records that "FFT is the process of fixing, observing, and reporting the location and movement of friendly forces. Inextricably linked, the composite employment of Combat Identification (CID) and FFT is requisite to effective target engagement with minimal risk of friendly fire incidents." Near-real time platform vectors would provide some level of intent in addition to force arrangement. See: O'Donohue 2019, IV-12; Townsend 2018, F-3.

north of the bridge to head off two Iraqi Republican Guard brigades and keep the bridge open for the trailing BCT.[25]

Unfortunately, as command relationships become more exceptional or unfamiliar, or as task organizations become more ad hoc, it only increases units' reliance on superior communication systems to overcome disjointedness. Thus, communication systems are required to enable flexible command relationships and will be insufficient to overcome DIL communications. Independent maneuver encourages all echelons to make the most of fleeting enemy weaknesses, and intent-based synergy is a bulwark against "the most dangerous of all courses of action in the face of [a] peer enemy… to do nothing." There will be few if any circumstances in MDO when taking an operational pause would benefit a command more than its enemy.[26] Nevertheless, even the most solid commander's intent and thoughtful control measures have limited shelf-lives, with their effectiveness subject to erosion by time and unanticipated enemy actions.[27] A unit with empowered subordinates and executing mission-type orders can overcome temporary communication system degradations, but they cannot afford to become a disconnected (i.e., isolated) command.

[25] Tisserand and Cammons 2003, 95, 103.

[26] LTG Cavoli, USAEUR CG, "cautioned us to decide up front 'how we would enter the wood chipper'; how we would identify its forward edge; and once in it, how we would proceed audaciously with the simultaneous commitment of all forms of contact that the division could generate. Once in the "wood chipper," we realized that the most dangerous and risky thing we could do was to stop attacking." See: Taylor and Kay 2019.

[27] MDO control measures would most likely function as Fire Support Coordination Measures and Maneuver Control Measures with both permissive and restrictive control measures, which can be on/order, triggered by enemy action, activated/canceled per phase, or modified mid-battle. "The primary purpose of permissive measures is to facilitate the attack of targets. The primary purpose of restrictive measures is to safeguard forces." See: O'Donohue 2019, IV-8.

Table 2. Current Tenets of Multi-Domain Operations with *Comments*

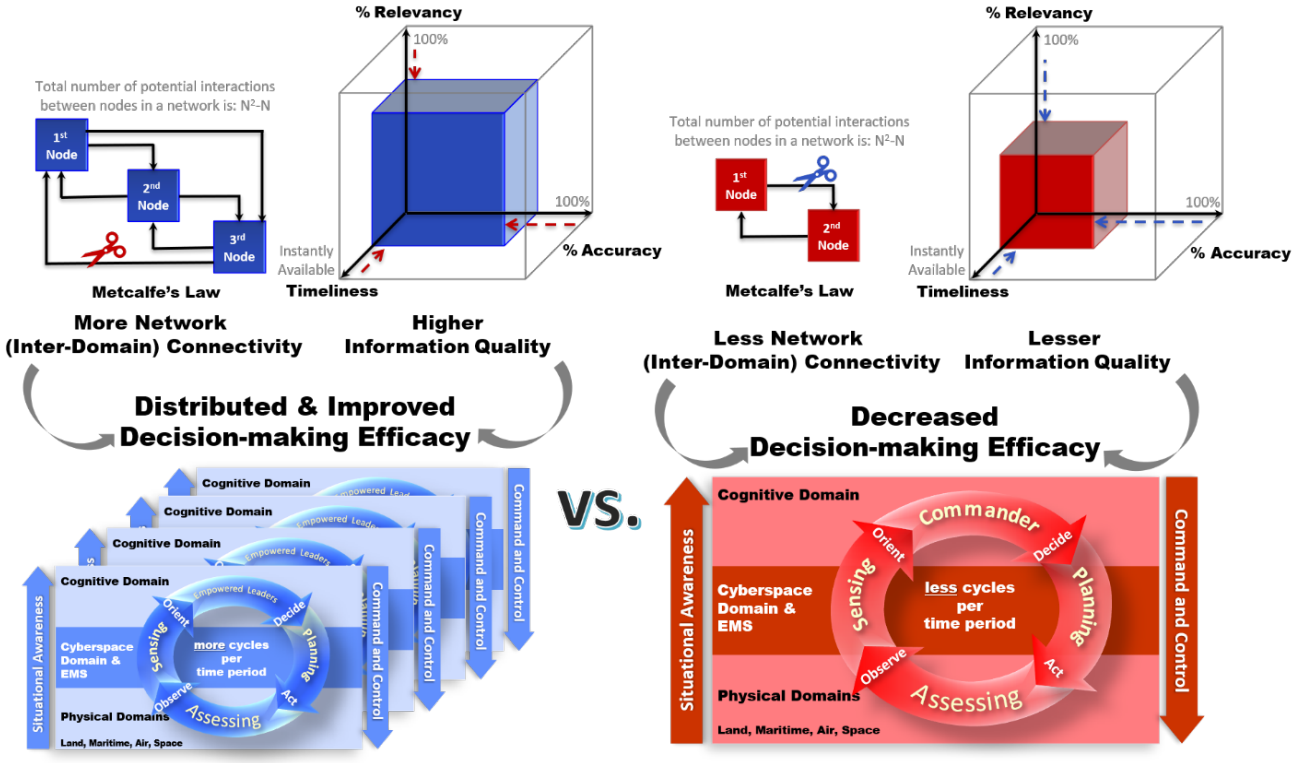
Calibrated Force Posture	Multi-Domain Formations (*delete and replace with Multi-domain Command & Control*)	Convergence (*this is the crux of MDO and must be enabled by Multi-domain Command & Control*)
Forward presence forces (*well-understood problem*)	Conduct independent maneuver (*move under mission command)*	Cross-domain synergy (*should include cross-domain fires*)
Expeditionary forces (*well-understood problem*)	Employ cross-domain fires (*move under cross-domain synergy*)	Layered options
National-level capabilities (*a matter of DOD focus)*	Maximize human potential (*remove; should be a Principle of Joint Operations due to its broad application*)	Mission command/ disciplined initiative (*place under revised Multi-domain command and control*)
Authorities (*a matter of policy*)		Multi-domain command and control (*left off the MDO Logic Map; should be elevated to MDO tenet and expanded)*

Source: Adapted from TRADOC Pamphlet 525-3-1 The US Army in Multi-Domain Operations 2028. See: Townsend 2018, v; Appendix A for the complete MDO Logic Map; Appendix F for an evolution of the proposed tenets for JADO.

A command must not only avoid becoming isolated but must not be denied the benefits offered by NEO. However, NEO relies on efficacious command and control support (C2S) to gain information superiority over a foe. Figure 2. below shows how effectual C2S is constructed: through greater intra- and inter-domain connectivity; increased information quality (e.g., relevancy, accuracy, timeliness); distributed decision-making via informed leaders with shared knowledge; and consequently, more OODA cycles per time period are possible.[28] Contested communications environments will require tactical units to rely more on EMS C2S and even operational-tactical elements will not find cyber-enabled C2S guaranteed.

[28] See Appendix E. for a larger depiction of Figure 2. JP 6-0 Joint Communications System lists four additional information quality attributes; usability, completeness, brevity, and security. Unfortunately, JP 6-0 does not reference C2S, though JP 1 Doctrine for the Armed Forces of the U.S. does. See: O'Donohue 2019, I-3, III-1; Dempsey 2017.

Figure 2. Superior C2S from More Network Connectivity, Higher Information Quality, and Distributed Authority Results in Improved Decision-Making Efficacy.[29]



Sources: Adapted *Network Centric Warfare: Developing and Leveraging Information Superiority* and MIT-Lincoln Laboratory's 2017 Network Communication Course. See Alberts, Garstka, and Stein 1999, 34, 292; Fossa 2017.

David Alberts et al., Director of the DOD CCRP, in their *Network Centric Warfare: Developing and Leveraging Information Superiority*, does a masterful job explaining and providing visuals covering the advantages of NEO. First, his team defines network centric warfare (now network-enabled operations)

> as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.[30]

[29] Note the scissor icons and dashed arrows pushing in to constrain the information quality cubes represent counter CS2 efforts like offensive cyber operations and electronic warfare.
[30] Alberts, Garstka, and Stein 1999, 2.

NEO increase a force's combat power by orders of magnitude, which is critical for defeating a potential enemy who is both closer to their base of operations, if not fighting from their homeland, and is numerically superior to the US.[31]

Only Cyberspace and the EMS can connect the disparate physical domains and the joint functions via the information environment.[32] Routine or prolonged communication system degradations will reverse the aforementioned gains offered by NEO, allowing friction and uncertainty to retard decision-making cycles and interrupt dynamic targeting and supporting kill chains. Maneuver commanders of all domains will need to increase their technological savviness and begin to include assured communications into their position of advantage calculations. Units of action may even find themselves maneuvering to communicate or resist culminating past the operational reach of connectivity instead of the traditional lines of communication.[33]

Additional evidence for the centrality of communication systems and the need to prioritize NCW can be found in the PRC's military strategy to check the US's power and in the Peoples' Liberation Army's (PLA) theory of victory. Eric Heginbotham et al. from RAND Corporation, a US-based research organization, analyzes primary source PRC strategy documents and provides the following:

> Chinese leaders have… contemplated how to defeat the United States by attacking its center of gravity—particularly its dependence on networks. Authoritative Chinese sources describe information warfare (which includes both electronic warfare and cyber operations) as the most important form of warfare. The 2013 Science of Military Strategy, a seminal PLA-wide document published roughly once a decade, stipulates that "The side holding network warfare superiority can adopt network warfare to cause

[31] Forces fighting closer to home will have C2S and EW assets less constrained by Size, Weight, and Power (SWaP) and, thus, will benefit from greater connectivity and more robust jamming capabilities than expeditionary forces.
[32] JP 3-12 Joint Cyberspace Operations explains, "[h]aving access to secure wired or wireless bandwidth is analogous to maintaining LOCs in the physical domains. The ability to divert the flow of data from one physical link to another in the face of threats, for example, from terrestrial cables to satellite communications (SATCOM) links, is an example of freedom of maneuver in [the joint information environment]." See: O'Donohue 2015, ix, II-12.
[33] See: JP 3-0 Joint Operations for Movement to Extend and Maintain Operational Reach. Scott 2018, III-37.

> dysfunction in the adversary's command system, loss of control over his operational forces and activities, and incapacitation or failure of weapons and equipment—and thus seize the initiative within military confrontation, and create the conditions for . . . gaining ultimate victory in war."[34]

Jeffery Engstrom, also from the RAND Corporation, has conducted an exhaustive analysis and synthesis of Chinese primary sources illuminating the PLA's theory of victory, or the way they intend to wage war at the operational and tactical levels to dominate future conflicts.[35] The PLA intends to wage "system destruction warfare," which has remarkable similarities and differences from MDO that reinforce the primacy of NEO and its composite communication systems. System destruction warfare is designed to "paralyze the functions of an enemy's operational system" (i.e., US joint functions) to subjugate a foe's "will and ability to resist."[36] OOS, like MDO: acknowledge the requirement to integrate "joint operations in all domains," including cyberspace and the EMS, are dependent on precision strike warfare and strive to interrupt their adversaries' OODA loops.[37] PLA planners highlight disrupting decision-making cycles, or the time sequence and tempo of "reconnaissance-control-attack-evaluation" processes, as one of three benefits from striking four types of operational system (OS) targets.[38] However, blinding an enemy, by denying command and control elements' real-time situational awareness or preventing their ability to develop and share a common operating picture, is

[34] Peter Mattis, a Fellow in the China Program at The Jamestown Foundation, explains that "[2013] Science of Military Strategy is the product of 35 researchers at the Academy of Military Science — which reports to the Central Military Commission, China's highest military decision-making body" and thus offers an accurate characterization of PRC's military strategy. See: Heginbotham 2015, 272; Mattis 2015.
[35] Engstrom 2018, 1.
[36] The PLA operational system consists of "a 'wide range of operational forces, modules, and elements' through integrated information networks that are 'seamlessly linked,'" e.g., "command system, the firepower strike system, the information confrontation system, the reconnaissance intelligence system, and the support system." Engstrom 2018, xi, 15.
[37] Engstrom 2018, 12-13, 18.
[38] Engstrom 2018, 18.

preferred. The second most desirable is to cause joint functions to fail to meet their purposes by identifying and then blocking where their "bottlenecks" reside.[39]

Table 3. PLA Information Superiority Targets and Desired Effects

Priority	Degrade or Disrupt	Target Example	Desired Effect
First	Command and Control Information flow	SA/COP transmission paths and data visualization/ storage	Information Isolation
Second	OS's essential elements	Unique to the joint function	Non or dysfunctional
Third	OS's network architectures	Transmission paths (e.g., C2 and Fires networks)	none specified
Fourth	OS's time sequence and tempo (reconnaissance-control-attack-evaluation)	Intelligence, surveillance, reconnaissance assets	Interrupt, slow, or paralyze decision-making

Source: Data adapted from Jeffrey Engstrom's Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare. See: Engstrom 2018, 16-18.

Table 3., above, displays how the PLA sees information superiority as its "core precondition for dominance," and how to employ kinetic and non-kinetic fires to render their enemies helpless versus annihilated.[40]

As stated, OOS differs from MDO, by placing information superiority above dominating any specific domain (e.g., air, maritime, land, or space) to make any opposing force inert. Additional differences include taking a non-linear approach and prioritizing network architecture design. MDO ranks fire superiority, mostly kinetic fires, critical to penetrating and disintegrating China's anti-access and area denial systems to allow follow-on maneuver forces to exploit enemy weaknesses.[41] While the DOD views resilient technical architectures as only a component of an MDO sub-tenant.[42] OSS, however, strives for "integrated whole effectiveness,"

[39] Engstrom 2018, 16.
[40] See Appendix D, US DOD's MDO compared with PRC's Opposing Operational Systems, to appreciate how the competing concepts relate to each other. Engstrom 2018, 11.
[41] Townsend 2018, 32-33.
[42] The MDO sub-tent referenced is multi-domain command and control. See: Townsend 2018, 23.

or " the "efficient flow of information, energy, and material" by optimizing its communication network structure.[43] Simultaneously, as laid out in Table 3., the PRC trusts they can rapidly dismantle enemy communication networks. The PLA symbolizes these strategies with two equations; "integrated whole effectiveness" (1+1>2); and "system destruction warfare" (1+1<2).[44] MDO offers a more linear, or spatial approach, to conceptualize how to employ and counter enemy multi-domain capabilities. While OOS explicitly rejects linear, "mechanical-age" thinking and promotes "numerous types of units from multiple services continuously [conducting] operations throughout the entirety of the battlefield."[45] JADO would benefit from learning from OOS by explicitly prioritizing the centrality of NEO.

Deterring and prevailing in a full-scale conflict with peer competitors in 2028 and beyond will require advances in doctrine, tactics, training, and developing more relevant acquisition requirements. The JADO concept should elevate MDO's multi (all)-domain command and control to a principle tenet and nest it underneath mission command, C2S, and NEO. See Table 4. Proposed Tenets of Joint-All-Domain Operations with Comments, below.

Table 4. Proposed Tenets of Joint-All-Domain Operations with *Comments*

Calibrated Force Posture	All-Domain Command & Control	Convergence
Forward presence forces	Mission command/ (*includes independent maneuver and convergence by echelon*)	Cross-domain synergy (*includes cross-domain fires*)
Expeditionary forces	Command & Control Support (C2S)	Layered options
National-level capabilities	Network-enabled operations (NEO)	
Authorities		

Source: Adapted from TRADOC Pamphlet 525-3-1 The US Army in Multi-Domain Operations 2028. See: Townsend 2018, v; Appendix A for the complete MDO Logic Map; Appendix F for the evolution of the proposed tenets for JADO.

[43] Engstrom 2018, 14.
[44] Engstrom 2018, 14.
[45] Engstrom 2018, 11-12.

MDO sufficiently explains how mission command would be enabled once it is applied to a broader joint perspective. Yet, it neglects the importance of the essential structure C2S provides JADO, and how those with most efficacious C2S will gain combat power based on their ability to employ NEO. MDO's convergence cannot work without C2S and NEO that buttress multi-domain command and control. JADO, like OOS, should task cyber and EW communities with first, fortifying US C2S and NEO and, second, countering enemy C2S, before contributing to fires (i.e., offensive cyber fires and direct energy weapons). Sometimes, the best way to aid a fire bucket brigade, is to carry the water to the flames (i.e., keep the warfighter informed) rather than enter the building with the firefighters (execute fires and maneuvers).

Training for JADO must include NEO exercises, at the operational-tactical level and below, that begin with cyber-enabled activities and become degraded to EMS C2S for at least half the exercise time. The other half of NEO training exercises must begin with EMS C2S *only* and progress to cyber-enabled C2S. Only with this methodology will US forces understand how to adapt to changes in information availability. Each tactical echelon's C2S must be structured to function as stub-networks, reliant on as little reach-back as practicable, and able to maintain internal NEO. The J6 will need to structure C2S to prioritize the delivery of essential information requirements '*specific'* to a mission. Training exercises should be used as testbeds to determine what essential information requirements are '*general'* to most missions to prevail in a DIL environment with only a constrained EMS C2S to rely on. Operators will need to practice disciplined message prioritization (e.g., flash, priority, immediate, routine).

Additionally, tactical elements will need to know when and how to maneuver to re-establish connectivity to their higher echelon to prevent their isolation and subsequent defeat-in-detail. Accordingly, Maneuver forces will need to understand information technology and EMS

principles and heuristics to increase their survivability and facility to maneuver to connectivity. Lastly, communication and intelligence planners will need to develop joint operations area-specific information almanacs (e.g., topographic maps, light data, enemy capabilities) that are locally (i.e., encrypted storage) available to support stub-networks. The above is a small sample of how the joint force will need to prepare for JADO.

NEO is a fundamental requirement for JADO. Even empowered units, conducting independent maneuver, executing mission-type orders within their commander's intent, and benefiting from flexible command relationships and all-domain control measures will not recover the combat power lost from network isolation or severe degradation. It can simultaneously inform commanders at all echelons to know when it is advantageous to concentrate or disperse their forces through shared understanding. Informing each tactical level reduces the fog and friction of war, supports calculated risk-taking, and exploits transitory enemy frailties. NEO allows senior commanders to distribute power down to where the most relevant and timely information is available.[46]

[46] Marquet 2014.