Army Futures Command Concept for Command and Control 2028: Pursuing Decision Dominance

COMPETE

PENETRATE

DIS-INTEGRATE

EXPLOIT

RE-COMPETE

14 July 2021

This page intentionally left blank

Executive Summary

1. The *Army Futures Command Concept for Command and Control* 2028*: Pursuing Decision Dominance* (AFCC-C2) describes how the Army of 2028 and beyond capitalizes on the Army's ability to know ourselves, our adversaries, and the operational environment with greater clarity and precision to produce decision advantages through an all-domain-capable command and control (C2) warfighting function and system. In turn, consistently creating decision advantages across all echelons enables Army forces to seize, retain, and exploit the operational initiative and establish overall decision dominance (see figure below). The AFCC-C2 nests with the Army's Multi-Domain Operations (MDO) and Echelons Above Brigade (EAB) concepts. The AFCC-C2 examines the problem of how Army commanders, operating as part of the joint force conducting unified action, will make and distribute decisions that enable operational initiative and overcome the five operational problems described in the MDO Concept (compete, penetrate, dis-integrate, exploit, and re-compete).

Know Ourselves, Our Adversaries, and the Operational Environment	*Achieve Decision Advantages*	*Seize, Retain, and Exploit the Operational Initiative*
Sense and Understand	→ Decide →	Act
Assess		

2. The future Army C2 system comprises *people*, *processes*, *the communications network*, *and a command post constellation (CPC)*. The future Army C2 system enables the rapid receipt, organization, analysis, interpretation, and display of contextually-relevant information to generate comprehensive, multi-domain courses of action at speeds that overmatch adversaries and enemies. Informed by staffs, subordinate leaders, and advanced technology (including artificial intelligence, machine learning, and big data analysis), commanders apply a combination of analytical reasoning and well-developed intuition to make rapid, quality decisions. Once made, decisions are quickly disseminated to subordinates and unified action partners in formats that are easy to understand and that allow for rapid action.

3. People are the core of the future C2 system. The Army requires bold, agile, adaptive, and competent leaders of character who thrive in ambiguity and fast-paced, data-driven operations and who can take disciplined initiative to accomplish their commanders' intents. Future Army leaders must be able to utilize an all-domain and whole-of-government approach to enable cross-domain maneuver, lethal and nonlethal all-domain fires, and unity of effort in the Army, the joint force, and the nation as a whole. Future Army leaders accomplish all C2 functions and activities across an agile and adaptable CPC—the variable arrangement of multiple, distributed, and meshed command nodes cross-functionally organized from home station into the close area.

4. The command nodes that form the future CPC are strategically deployable, tactically mobile, scalable, tailorable, and survivable. All command nodes are connected by a unified and resilient communications network, supported by common, standardized, shareable, and secure data that

links each node to the others to form one cohesively-functioning CPC. However, threats will likely disrupt or deny communications. Leaders and Soldiers, enabled through training, education, and experience and empowered with appropriate capabilities and authorities in all domains and environments, exercise disciplined initiative to preserve continuity of operations and create decision advantages.

5. To realize an all-domain-capable Army C2 system, the AFCC-C2 also describes the following cross-cutting ideas:
- Leader development that fosters disciplined initiative
- Talent management in support of the mission command (MC) approach and MDO
- Operations in the information dimension integral to winning in competition, crisis response, and armed conflict
- Seamless interoperability among unified action partners
- Appropriately tailored authorities and permissions
- Human-machine cooperation, collaborative decision making, and battle management
- Building trust in people, processes, the communications network, and the CPC
- Truth as a weapon against threat disinformation
- Supportive training environments and infrastructure

6. Through development of an all-domain-capable C2 system and attainment of the associated supporting ideas, future Army leaders have the required capabilities to achieve decision advantages. The components of the Army's future C2 system work in unity to integrate combat power across all of the domains, the electromagnetic spectrum (EMS), and the information environment (IE)—and with all other instruments of national power—to seize, retain, and exploit the operational initiative, achieve overall decision dominance, and succeed throughout competition, crisis response, and conflict.
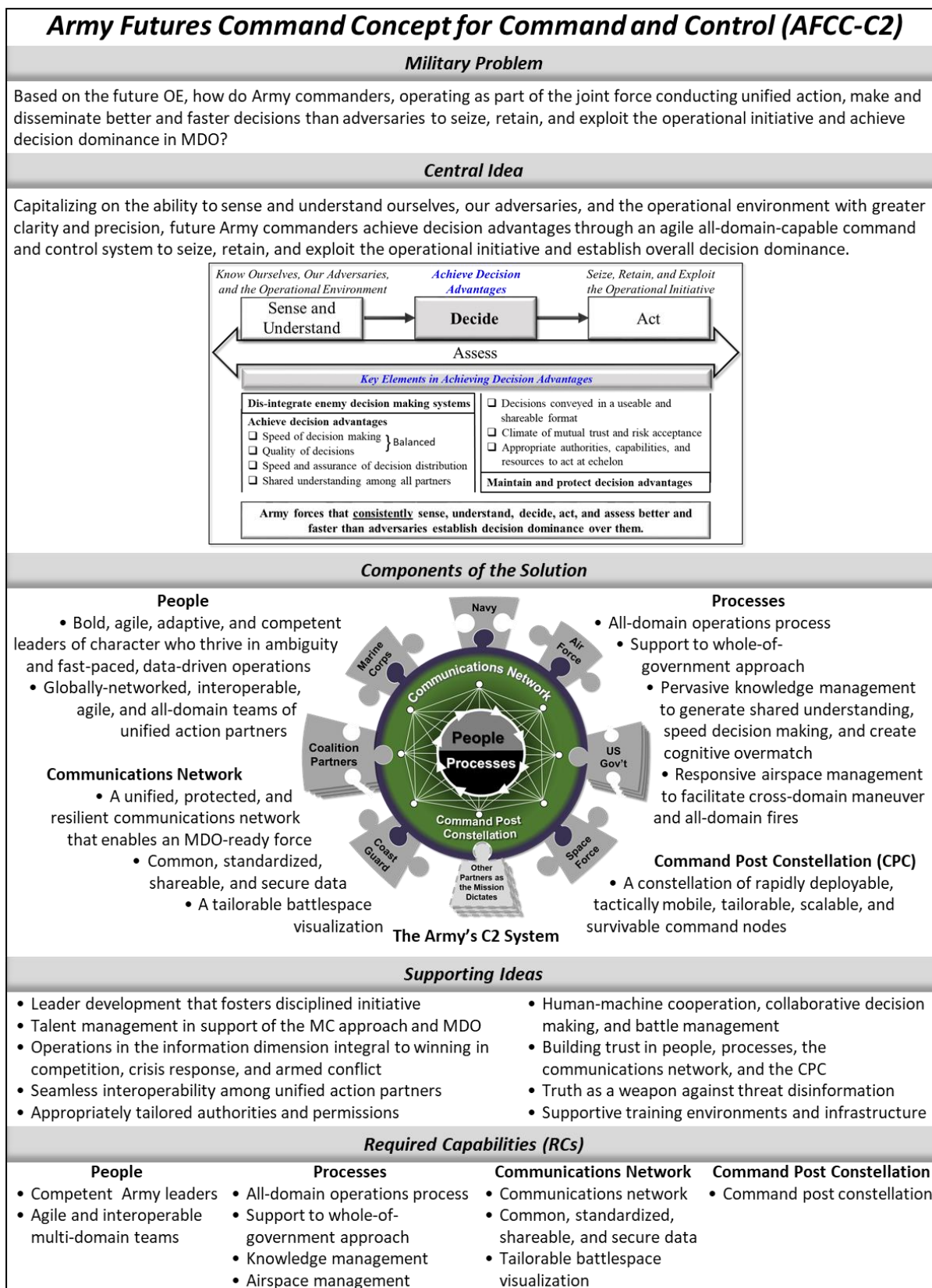
Army Futures Command Concept for Command and Control (AFCC-C2)

Military Problem

Based on the future OE, how do Army commanders, operating as part of the joint force conducting unified action, make and disseminate better and faster decisions than adversaries to seize, retain, and exploit the operational initiative and achieve decision dominance in MDO?

Central Idea

Capitalizing on the ability to sense and understand ourselves, our adversaries, and the operational environment with greater clarity and precision, future Army commanders achieve decision advantages through an agile all-domain-capable command and control system to seize, retain, and exploit the operational initiative and establish overall decision dominance.

Know Ourselves, Our Adversaries, and the Operational Environment — **Achieve Decision Advantages** — *Seize, Retain, and Exploit the Operational Initiative*

Sense and Understand → Decide → Act

Assess

Key Elements in Achieving Decision Advantages

Dis-integrate enemy decision making systems

Achieve decision advantages
- ❑ Speed of decision making ⎱ Balanced
- ❑ Quality of decisions ⎰
- ❑ Speed and assurance of decision distribution
- ❑ Shared understanding among all partners

- ❑ Decisions conveyed in a useable and shareable format
- ❑ Climate of mutual trust and risk acceptance
- ❑ Appropriate authorities, capabilities, and resources to act at echelon

Maintain and protect decision advantages

Army forces that <u>consistently</u> sense, understand, decide, act, and assess better and faster than adversaries establish decision dominance over them.

Components of the Solution

People
- • Bold, agile, adaptive, and competent leaders of character who thrive in ambiguity and fast-paced, data-driven operations
- • Globally-networked, interoperable, agile, and all-domain teams of unified action partners

Communications Network
- • A unified, protected, and resilient communications network that enables an MDO-ready force
- • Common, standardized, shareable, and secure data
- • A tailorable battlespace visualization

Navy · Air Force · US Gov't · Space Force · Other Partners as the Mission Dictates · Coast Guard · Coalition Partners · Marine Corps

Communications Network · People · Processes · Command Post Constellation

The Army's C2 System

Processes
- • All-domain operations process
- • Support to whole-of-government approach
- • Pervasive knowledge management to generate shared understanding, speed decision making, and create cognitive overmatch
- • Responsive airspace management to facilitate cross-domain maneuver and all-domain fires

Command Post Constellation (CPC)
- • A constellation of rapidly deployable, tactically mobile, tailorable, scalable, and survivable command nodes

Supporting Ideas

- • Leader development that fosters disciplined initiative
- • Talent management in support of the MC approach and MDO
- • Operations in the information dimension integral to winning in competition, crisis response, and armed conflict
- • Seamless interoperability among unified action partners
- • Appropriately tailored authorities and permissions

- • Human-machine cooperation, collaborative decision making, and battle management
- • Building trust in people, processes, the communications network, and the CPC
- • Truth as a weapon against threat disinformation
- • Supportive training environments and infrastructure

Required Capabilities (RCs)

People	Processes	Communications Network	Command Post Constellation
• Competent Army leaders • Agile and interoperable multi-domain teams	• All-domain operations process • Support to whole-of-government approach • Knowledge management • Airspace management	• Communications network • Common, standardized, shareable, and secure data • Tailorable battlespace visualization	• Command post constellation

Figure 1. AFCC-C2 logic map

U.S. Army Futures Command
Futures and Concepts Center
Austin, TX 78701-2982

14 July 2021

Force Management

ARMY FUTURES COMMAND CONCEPT FOR COMMAND AND CONTROL 2028

D. SCOTT MCKEAN
Lieutenant General, U.S. Army
Director, Futures and Concepts
Center

History. This pamphlet is a revision of United States (U.S.) Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-3 dated 06 February 2017. Because this publication is altered extensively, not all changed portions are highlighted in the summary of change.

Summary. The U.S. Army Futures Command (AFC) Pamphlet (AFP) 71-20-9 describes broad capabilities the Army of 2028 and beyond will require to enable all-domain command and control (C2). This functional concept drives force design and force development efforts by establishing a common framework within which to design and develop required C2 capabilities for the future. Critically, this concept establishes the intellectual foundation for creating a decision advantage and allowing future Army forces to effectively converge capabilities from, in, and across all of the domains, the electromagnetic spectrum, and the information environment at speeds that overmatch adversaries and enemies. Overall, the concept identifies the C2 capabilities necessary to enable future multi-domain operations (MDO) in a complex, highly competitive, lethal, and hyperactive operational environment against near-peer adversaries.

Applicability. This functional concept guides future force design and development and supports the Joint Capabilities Integration and Development System process. It also supports Army capabilities development processes described in the U.S. Army Futures and Concepts Center (FCC) Concepts and Capabilities Guidance, and functions as the Army's authoritative conceptual basis for developing affordable options for the future force pertaining to C2 across the realms of doctrine, organization, training, materiel, leadership and education, personnel, facilities,

---

*This publication supersedes TRADOC Pamphlet 525-3-3, dated 06 February 2017.

and policy (DOTMLPF-P). This concept applies to all Department of the Army (DA) activities that develop DOTMLPF-P requirements.

Proponent and supplementation authority. The proponent of this pamphlet is the Director, FCC. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. Do not supplement this pamphlet without prior approval from Director, Futures and Concept Center, 210 West 7th Street, Austin, TX 78701-2982.

Suggested improvements. Users are invited to submit comments and suggested improvements via DA Form 2028 to Director, FCC (FCFC-CE), 210 West 7th Street, Austin, TX 78701-2982. Suggested improvements may also be submitted using DA Form 1045.

Availability.   This   AFC   pamphlet   is   available   on   the   AFC   homepage   at https://www.army.mil/futuresandconceptscenter#org-resources.

Summary of Change

AFC Pamphlet 71-20-9
Army Futures Command Concept for Command and Control

This revision —

o Changes the title to reflect doctrine returning to C2 from the mission command (MC) warfighting function and the applicability to 2028 and beyond (cover, title page, and throughout).

o Revises the foreword and logic map and adds an executive summary (pages iii-v).

o Updates the background, assumptions, and operational context that provide the base for the concept's solutions (paragraphs 1-4, 1-5, and chapter 2).

o Uses a threat-informed approach to capability development and updates the military problem, central idea, conceptual solutions, and supporting ideas (chapter 3).

o Revises appendices on required capabilities statements (appendix B), Army science and technology (appendix C), risks of adopting this concept (appendix E), the Army's future communications network operational imperatives (appendix H), and the functional characteristics of the command post constellation (appendix I).

o Adds appendices on this concept's critical dependencies on the development of other Army concepts' capabilities (appendix D), the C2 system's people and processes (appendices F and G), applying C2 system capabilities across the competition continuum (appendix J) and common C2 functions, activities, and tasks (appendix K).

Contents

Figure List

Chapter 1
Introduction

1-1. Purpose

a. The U.S. Army Futures Command Pamphlet (AFC) 71-20-9, *The Army Futures Command Concept for Command and Control* (AFCC-C2) *2028: Pursuing Decision Dominance* identifies those capabilities the Army needs to command and control (C2) during future multi-domain operations (MDO).[1] This revised functional concept builds on the ideas presented in U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (MDO Concept) and TP 525-3-8, *Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045* (Echelons Above Brigade (EAB) Concept). These concepts describe how Army forces, as an element of the joint force, conduct MDO to prevail in competition and crisis response and if necessary, penetrate and dis-integrate enemy antiaccess and area denial systems and exploit the resultant freedom of maneuver to achieve strategic objectives and force a return to competition on favorable terms.

b. The AFCC-C2 poses and seeks to answer the following questions.

(1) What are the key physical and non-physical aspects of the future operational environment (OE) that influence how Army commanders exercise authority, interoperate with unified action partners, direct action, monitor activities, and assess progress throughout the employment of Army forces during MDO?

(2) How should the people, processes, networks, and command posts (CPs) that currently form the supporting C2 system be trained, managed, organized, designed, or configured in the future to allow the timely integration, dynamic synchronization, and optimal convergence of military capabilities from, in, and across all of the domains and with the other elements of national power (diplomatic, informational, economic, financial, intelligence, and law enforcement)?[2]

(3) What capabilities must the Army possess to enable commanders and their staffs to achieve decision advantages in future MDO across the competition continuum?[3]

(4) What key science and technologies (S&T) must the Army pursue to enable the proposed conceptual solution, its components, and the supporting ideas?

1-2. References
Appendix A lists required and related publications.

1-3. Explanation of abbreviations and terms
The glossary explains abbreviations and important terms used in this concept.

1-4. Background

a. The 1990s defense transformation hypothesized that emerging technologies would lift the fog of war to allow unprecedented understanding, permit near-perfect decisions, and facilitate

absolute precision in achieving effects.[4] Despite having supremacy in all operational domains, the last two decades of conflict in Iraq and Afghanistan have reinforced that operations are foremost a complex human undertaking. Commanders must be able to make timely, quality decisions with incomplete information and within the time available. Perfect situational awareness at any echelon has remained an unattainable end state. Furthermore, increased situational awareness and the ability to communicate with new technology can promote overly-centralized control, stifle disciplined initiative and risk acceptance, and become a vulnerability that adversaries will seek to exploit across the competition continuum. Through multiple operations and experiments, senior Army leaders discerned that audacious, agile, imaginative, trained and equipped leaders are critical to the ability to seize, retain, and exploit the operational initiative and expertly integrate combat power across all domains and environments.[5] More than ever before, future Army forces require commanders and subordinate leaders who are able to make rapid, quality decisions in conditions of relative ambiguity and who thrive in fast-paced, data-driven operations.[6]

> **Note:** *Throughout the remainder of this concept, the term "domains" will be used as a shorthand to represent the totality of the operational domains, the electromagnetic spectrum (EMS), and the information environment (IE). In similar manner, "multi-domain" will be used to denote any combination of two or more domains, the EMS, and the IE.*

b. Accordingly, the Army adopted mission command (MC) in the 2003 version of Field Manual (FM) 6-0, *Mission Command: Command and Control of Army Forces* as the "preferred" concept of C2 to guide commanders and provide a means to overcome the fog and friction of war.[7] Since MC's formal inclusion into the Army's authoritative body of knowledge, the Army has continued to review, assess, and make doctrinal improvements and refinements. Notably, Army doctrine recently clarified the use of the term MC to no longer describe multiple things (e.g., the warfighting function, supporting system, guiding philosophy, etc.) to overcome confusion among Soldiers, Army Civilians, and their unified action partners. In 2019, Army Doctrine Publication (ADP) 6-0 *Mission Command: Command and Control of Army Forces* improved clarity and realigned with joint doctrine by returning to a *C2 warfighting function*—while maintaining and reemphasizing MC as the Army's approach to C2. To further realign and promote unified action, the Army re-adopted the joint definition of C2 as the exercise of authority and direction by a properly designated commander of assigned and attached forces.[8] In this same vein, ADP 6-0 renamed the warfighting function's supporting system as the *C2 system*. While inclusive of enabling technology, the C2 system is not itself a technological information system. Instead, the updated ADP 6-0 describes it as a broader *system-of-systems* comprising people, processes, networks, and CPs that function together as a whole to enable commanders to conduct operations.[9]

c. The C2 system is the keystone of the C2 warfighting function and it must firmly support a commander's ability to understand, visualize, describe, direct, lead, and assess operations.[10] While the C2 system provides the people, processes, and tools to support these commander activities, the MC approach provides the overarching principles that guide all leaders—including commanders—in their application of authority, provision of direction, and utilization of resources to accomplish missions. The Army's evolved conception of MC always seeks to empower subordinates and foster disciplined initiative, but does not equate to the unrestrained decentralization of authority and capabilities. Some degree of control or oversight is always necessary.[11] Depending on the situation confronting them, commanders may require a more centralized and consolidated

approach to C2. For example, during the transition to, and initial stages of, multi-domain armed conflict against a near-peer enemy, an extremely centralized approach may be necessary to carefully integrate and precisely converge effects to penetrate and dis-integrate the enemy's antiaccess and area denial systems. Conversely, higher levels of decentralization and control may be more appropriate for follow-on cross-domain maneuver. Overall, the Army seeks to establish a bias toward decentralization of capabilities and authorities and the exercise of disciplined initiative.

d. The communications network is—and will continue to be—a critical component of the Army's C2 system. The *U.S. Army Mission Command Network Implementation Plan—Volume 1* describes the framework that the Army currently uses to guide network modernization efforts in the near- to mid-term for the *fielded force*.[12] Figure 1-1 shows the current lines of effort (LOEs). While informed by this framework, the AFCC-C2 is oriented toward the mid- to far-term and the *future force*. Unlike the implementation plan, the AFCC-C2 considers the entire C2 system (including requirements for the Army's future communications network). The physical and fiscal realities of manning, equipping, and sustaining the Army requires capability developers to use a grounded projection from the current state to a future state.
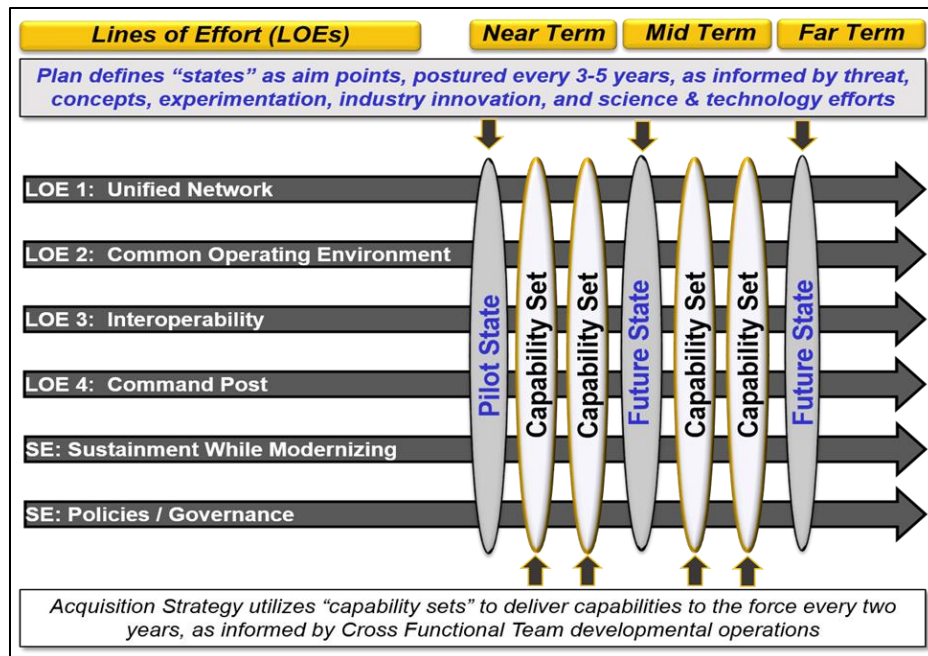
Figure 1-1. Mission Command Network Implementation Plan

1-5. Assumptions

a. The assumptions from the MDO and EAB concepts apply to this pamphlet.[13]

b. The following additional assumptions apply to the Army's ability to C2 in the future.

(1) Even with repositioning and persistent rotational employment of Army forces as part of calibrating future force posture, the largest percentage of the force will remain based in the continental U.S. (CONUS). To seize, retain, and exploit the operational initiative and succeed in

competition, crisis response, and armed conflict, CONUS-based forces will require the ability to be highly expeditionary—in mindset and capability.[14] The rapid deployment of CONUS-based forces will also require the ability to C2 those forces over strategic distances.

(2) Army organizations that are manned, equipped, and trained to operate best in highly decentralized operations will be able to operate effectively under tight centralized control. However, centralized control for long periods of time will be less effective. Army organizations that are manned, equipped, and trained to operate best under centralized control will be unable to operate dispersed and decentralized to the degree and speed necessary to defeat threats in the complex, highly-competitive, and hyperactive physical and non-physical OE of the future.

(3) Army forces will plan, train, and operate with unified action partners to conduct MDO and to integrate and synchronize combat power with the other elements of national power (U.S. and coalition) to succeed and achieve lasting outcomes for the nation.[15] To achieve the degree of interoperability described in this concept, necessary changes to national, joint, Army, and other unified action partners' policies, procedures, authorities, and permissions will be accomplished.

(4) An intelligent, learning, and adaptive enemy will be able to counter or degrade the Army's current and future technological advantages. New capabilities will precipitate new vulnerabilities. In particular, digital technologies (including those in the civilian sector on which the Army depends for strategic movement and enduring sustainment) will present new attack vectors that must be monitored and protected.

(5) The impact of future conflicts will not be confined to a single geographic region; the Army and joint force will be contested globally. Consequently, globally-integrated operations will be essential to success throughout the competition continuum.[16]

1-6. Linkages to the Army Concept Framework

a. MDO Concept.

(1) The MDO Concept describes how future Army forces, as an element of the joint force, conduct MDO to prevail in multi-domain competition and crisis response and when necessary, penetrate and dis-integrate enemy antiaccess and area denial systems to create the freedom of maneuver necessary to achieve strategic objectives and force a return to competition on favorable terms. To accomplish this, the MDO Concept advances three mutually-reinforcing tenets: calibrated force posture, multi-domain formations, and convergence.

(a) *Calibrated force posture* is the combination of capacity, capability, position, and the ability to maneuver across strategic distances. A calibrated force posture requires a dynamic mix of different types of forces that can adapt and change as dictated by the strategic environment: forward presence forces (U.S. and partner, conventional and special operations), expeditionary forces (Army and joint units and capabilities), and national-level cyberspace capabilities, space-based platforms, intelligence, and strike capabilities. This tenet includes the requirements that Army forces be empowered with the required access, authorities, capacities, and host-nation support to understand and operate in all of the domains; form teams rapidly; and interoperate

seamlessly with unified action partners to expand the competitive space, create multiple dilemmas for adversaries and enemies, and achieve overmatch.[17] To achieve a calibrated force posture, Army forces must be expeditionary and commanders must be able to C2 continuously throughout alert, deployment, early entry, and subsequent operations to ensure that deploying forces are able to fight immediately upon arrival and win.

(b) *Multi-domain formations* possess the capacity, endurance, and capability to access and employ capabilities from all of the domains to pose multiple and compounding dilemmas on the adversary. Future Army forces that possess the appropriate authorities and have immediate access to capabilities from all available domains can conduct and employ cross-domain maneuver and lethal and nonlethal all-domain fires to outpace and out-maneuver adversaries and enemies.[18] Future multi-domain formations are enabled by advanced protection systems, reduced signatures, redundant communications hardened against enemy interference, all-domain-capable situational awareness tools including signature obscuration, management, and control capabilities, and strategically-deployable, tactically-mobile, scalable, and highly-survivable CPs.

(c) *Convergence* is the rapid and continuous merging of capabilities from, in, and across all of the domains to optimize effects and overmatch the enemy in decisive spaces. Convergence is enabled by an all-domain-capable C2 system. While future Army forces at echelon must be equipped with or have rapid access to all the necessary domain capabilities and authorities with which to act, they also require leaders and Soldiers who can effectively understand, think, and plan across all of the domains.[19]

(2) The MDO Concept recognizes that MC remains an essential element of all Army operations.[20] Enemies will disrupt friendly communications and plans. However, the MC approach must expand to enable dynamic cooperation across Service and other partner lines—at some risk—to allow the joint force to preserve the ability to continuously and rapidly converge capabilities from all domains; to seize, retain, and exploit the operational initiative despite disrupted communications.[21] The MDO concept points out that one manifestation of MC is intent-based synergy: the dynamic cooperation that enables the sufficient integration of all available domain capabilities to achieve dominant or essential effects at a decisive space and time, acknowledging some degree of risk or collateral cost.[22] The MDO concept stresses that commanders must *deliberately* create and foster conditions favorable to MC so that ever-disparate formations and capabilities are ready to act upon mutual recognition of an opportunity or in response to a battlespace development.

  b. The EAB Concept.

(1) The EAB concept describes how future Army combined-arms formations above brigade gain and maintain the operational initiative at echelon and through the depth and breadth of an extended battlespace. It describes how EAB formations and commanders must—
- Sense and understand the depth and breadth of the battlespace, including in and across all of the domains.
- Decide on a course of action that converges capabilities from all of the domains in decisive spaces with increased speed and tempo to shape the battlespace for success through cross-domain maneuver and lethal and nonlethal all-domain fires.[23]

- Strike the enemy in multiple decisive spaces.
- Possess the endurance to maintain positions of advantage and consolidate gains.

(2) Like the MDO Concept, the EAB Concept recognizes that, for Army forces to succeed in the future OE, MC must become intrinsic to the Army profession.[24] Individual Soldiers and leaders must also work effectively with and leverage expertise from joint and national-level capabilities, organizations, and leaders. The extended distances across an area of responsibility (AOR) and prevalence of multiple U.S., coalition, and interorganizational partners magnify the already complex challenges of integration, communications, collective cooperation, and unity of effort. Future formations will encounter varying degrees of degraded communications due to attacks against Army and joint C2 systems. Consequently, EAB commanders and their formations must be capable of continuing to operate within their higher commander's intent to achieve objectives even when communicatively isolated from the rest of the force.[25] Under these conditions, employing the appropriate amount of control and level of decentralization, coupled with a core bias toward disciplined initiative, play a pivotal role in the success of dispersed formations conducting disaggregated operations.

Chapter 2
Future Operational Environment

2-1. A complex, highly-competitive, and hyperactive physical and non-physical OE[26]

a. The hierarchical conceptual documents discussed above collectively forecast an increasingly complex OE marked by globalization and its effects. These concepts foresee persistent strains on order brought about by intense competition for resources, growing ideological and economic friction, accelerated urbanization, rapid diffusion of information and propaganda, increased migration of disaffected populations, a proliferation of weapons of mass destruction, regional and global pandemics, relentless media scrutiny, and disruptive environmental changes.

b. In this hyperactive future OE, Army forces must also contend with dramatic advances in S&T—including artificial intelligence (AI); quantum computing, sensing, encryption, decryption, and navigation; robotics; autonomous systems; electromagnetic warfare (EW); directed-energy weapons; hypersonics and other long-range precision fires; space; cyberspace; and biotechnology. These S&T advances increase the speed of human interaction, the risk of aggression, the lethality of armed conflict, and the pace and complexity of operations. Complexity increases in competition, crisis response, and conflict as future Army forces fight across the physical and non-physical (virtual and cognitive) battlespace.

c. Given these military and civil considerations, the following sections further detail the relevant conditions within which future Army forces exercise C2. While this chapter deliberately focuses on adversaries and enemies to support a threat-based focus toward capability development, future OE conditions offer similar risk and opportunity to Army forces and their unified action partners.

2-2. Perpetual competition below the threshold of armed conflict[27]

a. Future adversaries and enemies are in constant multi-domain competition with the U.S. and its allies. Because of the high political, economic, and human-life costs of armed conflict, threats try to achieve their political objectives without triggering armed conflict. Future adversaries utilize sophisticated asymmetric and hybrid tactics to challenge the U.S. and its allies' security interests.[28] These tactics leverage clever and well-timed combinations of: information warfare; space and cyberspace operations; EW; nonlethal directed-energy weapons; non-attributable chemical, biological, and radiological attacks; and limited lethal strikes.[29] Adversary and enemy tactics also embrace irregular warfare to prepare, infiltrate, isolate, and incite dissent and disruption in nations that are a target of their aggression.

b. Army forces will be confronted with sophisticated state-sponsored information warfare artfully combined with conventional and unconventional military operations. Use of information warfare obfuscates the true intent of ground and special purpose forces operating near borders or in neighboring nations.[30] Future threat approaches also include advanced weapons and technology applied and mixed innovatively with crude, simple, and unsophisticated means to create parity or overmatch against Army forces.[31] Future enemies and adversaries take advantage of ambiguous aspects of international law and capitalize on war-averse attitudes that make countries hesitant to enter conflict when legitimacy questions persist. Threat forces use information warfare and psychological operations to cause populations to support or allow aggression even to the detriment of their own country.[32] Therefore, Army leaders must understand adversary and enemy philosophies, motives, histories, and methodologies. Possessing the appropriate authorities, Army leaders must have sufficient expertise in the conduct of *proactive* operations in the information dimension to thwart these competitive approaches. For domestic, friendly, and neutral audiences, future Army leaders must become undeniable sources of objective truth.[33]

2-3. Contested in all of the domains

a. The expansion and availability of technology propelled by the proliferation of available information enable threats, including near-peer competitors, non-state actors, and super-empowered individuals, to aggressively contest operations across all of the domains and warfighting functions.[34] A growing global interconnectivity fueled by advances in electronics increases rapid access to information and as a result, increases the velocity and momentum of human interaction and events. Technology previously unavailable to less-resourced nations and individuals is now readily accessible and often used with little regard for moral or ethical consequences. In the timeframe of this concept, lethal and nonlethal systems are easier to afford, access, and manufacture, providing a greater number of threats with the ability to find or create new opportunities across the entire competition continuum.[35] In this future where the technological playing field is more level, the advantage will go to the side with better trained and prepared soldiers who can expertly employ technology, sense and think in all of the domains, synthesize and leverage vast amounts of data, and find creative combinations of joint, multinational, and interorganizational capabilities to solve operational and tactical problems.

b. Future enemy forces use ground-based, long-range, area and precision anti-surface and air defense systems—integrated with air, maritime, cyberspace (to include social media), and space

strike capabilities—to deny Army and joint forces access to the conflict zone. If entry is achieved, enemy extended-range, massed fires, augmented with precision munitions engaging high-payoff targets, challenge traditional large-scale staging, assembly, maneuver, sustainment, and CP employment. Gaining and maintaining freedom of maneuver is increasingly difficult. Future advanced enemy and adversary sensors and unmanned systems threaten Army headquarters and formations across the depth of the expanded battlespace and provide the enemy with dynamic situational awareness and precision targeting opportunities. In space, cyberspace, and the EMS, adversaries take advantage of Army and coalition reliance on space-based intelligence, surveillance, and reconnaissance, environmental monitoring, and positioning, navigation, and timing; networked information systems, including secure satellite communications; and other lethal and nonlethal network-enabled systems. These enemy actions create a complex and hyperactive environment, speed and shorten engagements, and drive decision times down. At increasingly lower echelons, commanders and staffs must be able to quickly discern threats and their capabilities, know when their network assets have been compromised or attacked, determine attribution, and possess the right mix of domain capabilities, authorities, and expertise to respond and protect people, equipment, and data.

c. Future threats contend aggressively in the IE throughout the entire competition continuum, seeking to deny support from civilian, political, and military audiences. Increasingly, they use propaganda, disinformation, misinformation, and skillful deception to shape the environment to present a skewed picture, create uncertainty, confound decision making, and slow friendly counteraction. Future enemies attempt to distort and prevent accurate situational understanding by—and between—military and civilian audiences. Once adversaries achieve strategic or operational objectives, often below the threshold of armed conflict, they use information to legitimize and consolidate gains while projecting an image of sustained military strength. To accomplish their objectives, they develop and employ sophisticated computer bots and algorithms to affect how individuals and groups process, perceive, judge, and make decisions.[36] Overall, future threats seek to fracture the joint force's coherence along the "seams" between operational domains and Service functions, alliance members, and civilian and political support for military operations.[37] In the future, the truth is more difficult to ascertain, and the side that can rapidly control, manage, and use information gains a definite cognitive position of advantage.[38]

d. The ability for threats to contest in all of the domains broadens and expands the breadth and depth of the future competitive space. This broadening occurs in time, domains, geography, and actors. Enemies and adversaries expand their influence through unending multi-domain competition and achievement of strategic objectives short of what the U.S. traditionally considered war. They also expand the competitive space by making space, cyberspace, EW, and information key components of all operations. Threats expand the competitive space geographically through employment of these non-physical capabilities that are themselves less constrained by geographic location and time. A significant consequence of this physical, virtual, and cognitive expansion is that the homeland—including military installations and the defense industrial base—can no longer be considered a sanctuary. Lastly, future enemies and adversaries broaden the competitive space by employing an increasing number of non-traditional actors, including proxies and surrogates, to pursue their objectives.[39] Accordingly, future Army forces must be able to sense, understand, visualize, represent or display, and describe the expanded battlespace to create shared understanding and unity of effort among themselves and their unified action partners.

2-4. Greater lethality and weapon ranges

a.   Advancements in weapons technology, multi-domain sensors, communications, and information-processing capabilities dramatically increase lethality.[40] Future enemies detect, track, and target Army forces (including their CPs) and activities throughout the depth of the expanded battlespace from home station to the tactical edge and across all of the domains, and seek to gain direct and indirect fires overmatch with increasingly capable conventional and unconventional forces. Technological advancements allow future enemies to integrate directed-energy weapons (lethal and nonlethal), guided missiles, direct-fire platforms, and autonomous weapon systems precisely, in combination, and with greater overall effect. As threat human-machine interfaces and AI mature, future Army forces become potentially vulnerable to faster kill chains with devastatingly lethal and destructive firepower. Future enemies employ AI and autonomous systems to expedite targeting unconstrained by ethical norms that might require a human decision maker in, on, or initiating the sensor-to-shooter loop.[41]

b. The proliferation of weapons of mass destruction presents an increasing danger to military forces and civilians overseas and in the homeland. Military bases and other sites of national importance for C2, deployment hubs, and sustainment nodes will be targeted with lethal and nonlethal effects causing massive disruptions, confusion, and delays in the Army's ability to deploy and respond. Rogue states, radical ideologues, and criminals may gain access to chemical, biological, radiological, and nuclear weapons, along with technologies to employ them, such as guided missiles and remotely-piloted aircraft. These devastating weapons punctuate the need for rapid, well-informed decisions that deter their use, or best mitigate their effects. Additionally, future Army forces must work closely with civil authorities to harden key military and civilian infrastructure and ensure a balanced force posture. Future Army forces must be empowered with the necessary authorities so that they respond quickly to any threat. As potential high-payoff targets for enemy firepower, friendly command nodes must be more survivable, including the ability to sense and understand, obscure, minimize, or otherwise manage and control identifying C2 signatures.

2-5. Degraded communications

a.   Future threat weapons technologies place communications networks at direct risk of disruption. Advanced data and information storage and management, data mining, and AI enable threats to develop innovative heuristics for conceptualizing and managing engagements across all of the domains. The enemy interrupts, denies, and destroys friendly communications networks as a central part of its operational concept. Army CPs are vulnerable to attacks in and through cyberspace and the EMS, as well as conventional indirect and air-delivered fires. CPs also face the threat of chemical, biological, radiological, and nuclear attacks. Future threats attack space systems and supporting communications nodes from cyberspace and by ground-launched or air-launched anti-satellite weapons—both ballistic and directed-energy.

b. Enemies and adversaries leverage EW capabilities to deny, disrupt, and degrade the Army, other Service, and coalition partner capabilities and digital networks. They time these attacks to maximize the effects of other actions in the battlespace. For instance, enemies and adversaries

seek to simultaneously degrade sensors, information systems, and transport pathways used to create multi-domain battlespace visualization and shared understanding; disrupt or prevent information collection, processing, and dissemination; inhibit the flow of logistics; and neutralize the full use of all joint fires, particularly precision munitions. Consequently, the Army's future communications network must be resilient and defensible, providing adequate access and transport throughput in degraded network conditions. Soldiers and Army Civilians who build, operate, maintain and protect the network must have the capabilities to fight through and establish communications windows of superiority to allow forces to continue to operate through denied, disconnected, intermittent, and low-bandwidth communications environments. Most importantly, Army forces must actively train and prepare to operate using the MC approach under these degraded communications conditions for significant periods of time.[42] To continue to operate with degraded communications and continue to seize, retain, and exploit the operational initiative, commanders at echelon must have the appropriately tailored authorities and permissions needed to act in all of the domains.

2-6. Increased urbanization and global connectedness

a. Urbanization and the proliferation of communications and information technology increase the probability of operating in a highly congested and contested IE, under continuous surveillance, and within complex human terrain. Enemies' willingness to employ lethal capabilities in close proximity of populations, contrasted with U.S. and allied reluctance to endanger noncombatants, compound the task of threat identification and targeting.[43] Constricting topography and poor infrastructure of many dense urban areas expose friendly movement, allowing enemies to disrupt forces operating from or into these areas. These same characteristics pose significant challenges for communications, reconnaissance, surveillance, and achieving tactical surprise. An urban area's distinct physical, cognitive, and operational characteristics and demands increase the complexity of planning, decision making, and conducting military operations.[44]

b. Adversaries and enemies manipulate the media—both social and traditional public—to expand their influence and build support in domestic, neutral, and allied nations. Radical ideologues, in particular, hide in and among sympathetic populations within dense urban terrain to conceal their identities and intentions. They use the interconnected world to spread their radical ideas and skillfully influence the media to present only their biased version of events. Globally-networked populations react to these prejudiced versions of events at the speed of the internet, complicating friendly ability—both military and civilian leaders—to discern an accurate, intelligence-driven understanding of the situation.

c. Future hybrid threats mix ideological, political, and criminal activities to gain positions of advantage against friendly forces. They develop and employ tactics and methods that hinder U.S. forces from directly attacking their organizational capabilities. Two primary methods are 1) preventing attribution and shielding to create deniability, and 2) exploiting U.S. policy constraints and political divisions to deter U.S. engagement.[45] Hybrid threats punctuate the need for a whole-of-government response and approach.

d. Based on potential threat exploitation of the projected increase in urbanization and global connectivity, future Army forces must be able to rapidly discern the truth and, for the public and

our unified action partners, Army forces must become a trusted and reliable source for the objective truth. Conversely, future Army forces must also possess greater capabilities and expertise to plan, integrate, and conduct operations in the information dimension, including information warfare as permitted, and deception against threats from theater-strategic to tactical levels.

2-7. Conclusion

The future Army force's ability to conduct MDO in a complex, highly-competitive, and hyperactive physical and non-physical OE is dependent upon a dynamic approach to C2. Commanders must have the agility to rapidly adapt to myriad circumstances that may be present by using an agile integrative warfighting function and supporting system that emphasize the following:

a. People—Army leaders of character grounded in the competencies of the Army profession able to recognize, understand, anticipate, and adapt quickly to changing conditions.

b. Maintaining shared understanding of the OE, problems, and potential solutions among a collaborative and diverse array of unified action partners, and contributing to a whole-of-government approach to winning in competition, crisis response, and armed conflict.[46]

c. An Army culture and ethos that foster candor, morality, trust, disciplined initiative, innovation, and risk acceptance.

d. The physical, cognitive, temporal, and virtual synergies created through the integration, synchronization, and convergence of all available destructive, constructive, and information capabilities across all of the domains and at speeds to outpace threats.[47]

e. Fluid adaptability in forming and reforming organizations and the ability to rapidly integrate partners and enable a whole-of-government approach to deter malign actors operating below the threshold of armed conflict, defeat aggression, and protect and advance national objectives.[48]

f. A robust, resilient, and defensible communications network and more mobile, scalable, tailorable, and survivable CPs dispersed over greater distances.

Chapter 3
Achieving Decision Advantages

3-1. Military problem

Based on the future OE, how do Army commanders, operating as part of the joint force conducting unified action, make and disseminate better and faster decisions than adversaries to seize, retain, and exploit the operational initiative and achieve decision dominance in MDO?

3-2. Central idea

Capitalizing on the ability to sense and understand ourselves, our adversaries, and the operational environment with greater clarity and precision, future Army commanders achieve decision advantages through an agile all-domain-capable C2 system to seize, retain, and exploit the

operational initiative and establish overall decision dominance.[49] (See figure 3-1 for key elements in achieving decision advantages.)
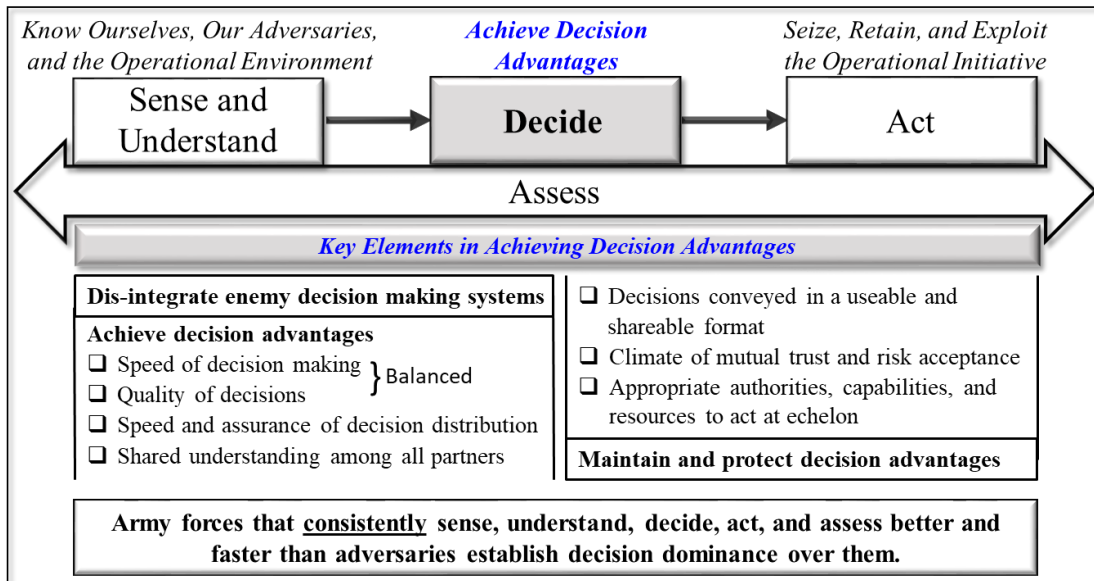
Figure 3-1. Key elements in achieving decision advantages

3-3. Solution synopsis

   a. The emerging *Joint All-Domain Command and Control Vision* (JADC2 Vision) succinctly describes the achievement of future decision advantage.[50]

   To win in great power war, the Joint/Coalition force will exercise C2 to maintain decision advantage while countering adversary strategies to defeat our ability to C2. Decision advantage entails acquiring timely and accurate information superiority and the ability to translate information into action at speed and scale (i.e., faster than the adversary). Commanders translate decision advantage into operational advantage though decision speed. Decision advantage enables the employment of combinations of all-domain effects to paralyze and collapse the opponent's system of decision-making, compromise their execution, and shatter their will to resist, while protecting our own force.[51]

   b. Based on the JADC2 Vision, figure 3-1 groups the elements of decision advantage into three categories: 1) dis-integrate enemy decision making systems (critical to the MDO Concept's central idea and the EAB Concept's solution of converging multi-domain effects in depth), 2) achieve decision advantages (central idea of this concept), and once achieved, 3) maintain and protect those decision advantages to achieve overall decision dominance. These three categories highlight this concept's dependence on required capabilities from other functional and supporting concepts within the Army concept framework that enable the achievement, maintenance, and protection of decision advantages (see appendix D).

   c. To achieve decision advantages in multi-domain competition, crisis response, and armed conflict, the Army must identify and develop the capabilities of the future C2 system—as a system

of systems—through a comprehensive, holistic analysis and modification of each component. The future C2 system enables the timely convergence of effects across all of the domains by facilitating the seamless flow of information from and between Army, joint, and other unified action partners' sensors, other network points of presence, and information systems. In turn, commanders and their staffs are able to rapidly sense, understand, decide, and act better and faster than an adversary or enemy. With an all-domain-capable C2 system, commanders and their staffs continuously plan, prepare, execute, monitor, and assess sequential and simultaneous operations throughout the depth and breadth of their battlespace and converge multi-domain capabilities in decisive spaces to seize, retain, and exploit the operational initiative and achieve overall decision dominance.

3-4. Components of the solution

a. This section outlines the conceptual solutions that generate the required capabilities (RCs) to support the modifications demanded of the future all-domain-capable C2 system to achieve decision advantages. These do not prescribe specific DOTMLPF-P solutions. Instead, they identify the broad, interrelated capabilities needed for the future force. From these, subject-matter experts develop specific solutions through outcomes-based, integration-focused, and resource-informed research, experimentation, and analysis. These conceptual solutions tie directly to the RC statements found in appendix B and the S&T focus areas in appendix C. Analysts must understand these solutions collectively to avoid individual, and potentially conflicting, interpretations of the RCs.[52] (Figure 3-2 summarizes the components of the solution.)
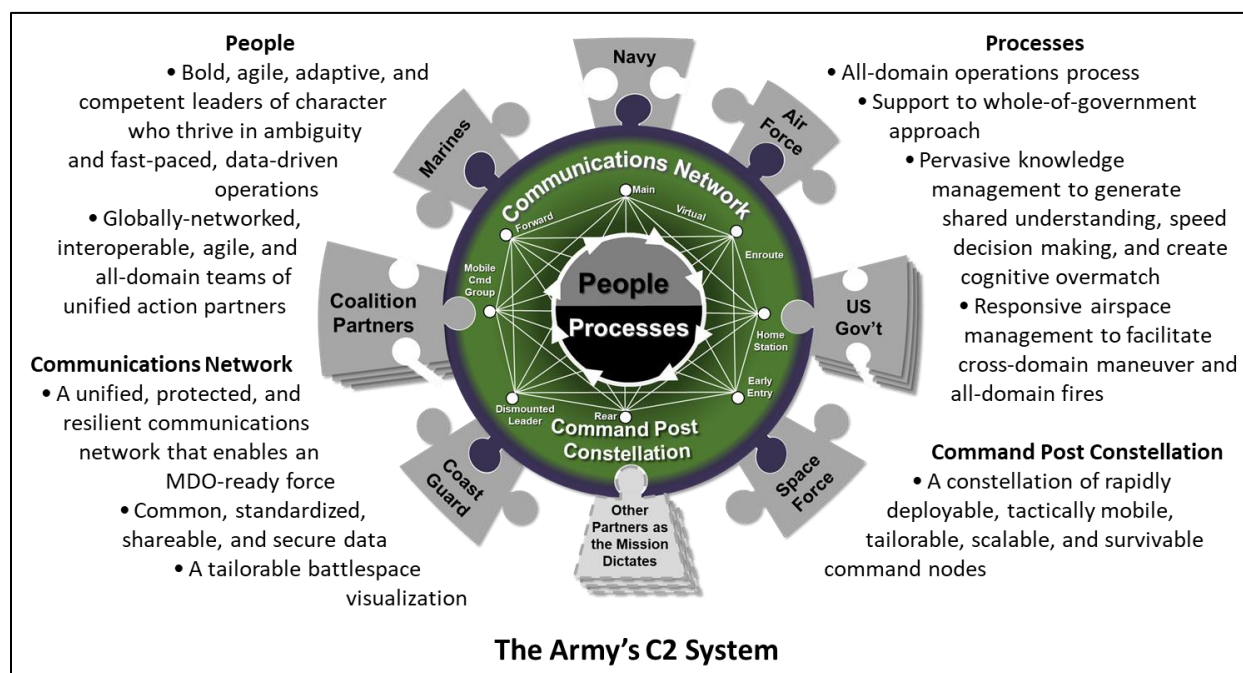
Figure 3-2. Components of the solution

b. When changing or modifying one system component, operational commanders and capability developers must consider its impact on the other components individually as well as their arrangement and relationships with each other.[53] While capability developers may focus force modernization efforts on improving a single component (or on even a smaller subcomponent within), any changes or modifications will likely impact the other components and the critical

17

interdependencies among them. Improving one component above others may incrementally improve the function of the Army C2 system, but likely not to the speed and scale necessary to simultaneously integrate, synchronize, and converge capabilities from all of the domains to out-think, out-maneuver, and outpace future near-peer threats. Operational commanders must conduct a continuous assessment of their fielded C2 systems and constantly adapt the organization and operation of their *people, processes, communications network, and command post constellation (CPC)* to gain or maintain decision advantage. Together, commanders and capability developers must establish a common understanding of the C2 system's components and their relationship to each other and to the system as a whole to discern progressive near-, mid-, and far-term capability requirements.[54]

c. **People**. Key people within the Army C2 system are commanders, seconds-in-command, subordinate commanders (including unified action partners), senior noncommissioned officers and enlisted advisors, staffs, liaison officers (to and from partners), and those who build, operate, maintain, and protect the communications network and command nodes. The C2 system centers on commanders. Commanders make decisions, clearly convey intent to provide purpose, direct action, and motivate and empower subordinates for success. As an extension of their commanders, other members of their C2 systems assist commanders in creating shared understanding, making quality decisions, and rapidly distributing mission orders and directives in an understandable and useable format. When addressing the system's people component, commanders and capability developers must also consider how *individuals* come together and operate as competent, cohesive, and well-trained headquarters and human-networked *unified-action-partner teams*. Given equal access to technological tools, decision advantages will fall to the side whose decision makers are more adaptable and speedy problem solvers, who have the most robust access to actionable information and intelligence, and who are more empowered through decentralized authorities and capabilities.[55] (See appendix F for a detailed discussion of the future C2 system's people.)

(1) *Bold, agile, adaptive, and competent leaders of character who thrive in ambiguity and fast-paced, data-driven operations*.[56] The MC approach to command remains wholly applicable to the future.[57] It is founded on well-developed leaders—enabled by state-of-the-art equipment (including AI-enabled decision support and battle management), streamlined procedures, and common, standardized, shareable, and secure data—that simplify complex activities and extend capabilities and authorities to the lowest practical level. The MC approach is based on the belief that commanders and subordinate leaders are most effective when they articulate a clear intent to empowered Soldiers and Army Civilians who share a common appreciation of the environment, problems, potential solutions to those problems, and risks involved. Commanders make quality decisions, integrated through an efficient, effective, and domain-comprehensive operations process and communicated within a framework of accurate battlespace visualization and overall shared understanding. Bold, agile, adaptive, and competent Soldiers and Army Civilians who thrive in ambiguity and fast-paced, data-driven operations rapidly turn commander's decisions into decisive action.[58]

(2) *Globally-networked, interoperable, agile, and all-domain teams of unified action partners.* The Army provides globally-networked (socially and technologically), interoperable, and agile teams of active and reserve component Army forces and other unified action partners that are rapidly deployable, mission-tailorable, and responsive to combatant commander needs and

the Army's enduring requirements across the competition continuum.[59] Future Army forces rapidly form cohesive, multifunctional teams while combining their diverse knowledge, expertise, and capabilities across all of the domains to create physical, cognitive, temporal, and virtual overmatch. Through flexible command relationships and agile, adaptable formations, future Army forces achieve advantage by swiftly configuring, adapting, and reconfiguring as needed to bring a different set of forces and capabilities to bear against any problem.[60] While maintaining preeminence in the application of landpower, future Army forces adjust, adapt, and transform land-centric thinking, processes, and capabilities to support future MDO and a whole-of-government approach to campaigns and operations.

d. **Processes**. The Army's overarching framework for making decisions, organizing forces and capabilities, and putting decisions into action is the operations process: planning, preparing, executing, monitoring, and continuously assessing operations.[61] Each warfighting function has one or more functional integrating processes that support the overall operations process. And like the overall operations process, each supporting process must consider how it contributes to supporting a whole-of-government approach to winning. Two key supporting processes that cut across warfighting functions are knowledge management and airspace management. (See appendix G for a more detailed discussion of future C2 processes.) All future processes must support greater joint, coalition, and whole-of-government unity of effort.

(1) *All-domain operations process*. Due to the uncertain future environment and the Army's previous focus on counterinsurgency and other operations dominated by stability tasks, the Army refocused on the conduct of the operations process at all echelons, with unified action partners, and across the full range of military operations.[62] Army training and education reemphasized crisis-action planning and large-scale operations characterized by lethal and destructive offensive and defensive tactical tasks.[63] For the future, the Army must continue along this path. In addition, it must determinedly broaden its expertise to include the seamless integration of joint, multinational, and interorganizational capabilities into plans and operations to create temporary windows of superiority across multiple domains and throughout the depth and breadth of the physical, cognitive, temporal, and virtual battlespace; seize, retain, and exploit the operational initiative; and succeed throughout the competition continuum.[64]

(2) *Support a whole-of-government approach*.[65] Achieving national aims in future OEs requires the timely integration, dynamic synchronization, and optimal convergence of all instruments of national power as part of a combined, whole-of-government approach that avoids redundant, competing and conflicting efforts.[66] The military's operational defeat of an enemy is only a part of the larger campaign. The overall objective is to create a secure environment to facilitate a better political, social, or economic outcome. Future multi-domain competition, crisis response, and armed conflict require the timely integration, dynamic synchronization, and optimal convergence of the activities and capabilities of civilian partners with military operations. As part of a larger joint and U.S. government undertaking, the Army organizes in a manner that facilitates an integrated whole-of-government approach, making it easier to generate the breadth and depth of knowledge and capabilities necessary to achieve clearly identified, mutual objectives.[67] As the central process of the C2 system, commanders and their staffs employ the operations process to integrate available elements of national and coalition power in time, space, and purpose. They

achieve this by assiduously integrating unified action partners into the process, and applying their knowledge and capabilities into making quality decisions.

(3) *Pervasive knowledge management to generate shared understanding, speed decision making, and create cognitive overmatch*.[68] Knowledge management is crucial to creating decision advantages against near-peer threats. Future knowledge management streamlines the flow of information and intelligence and ensures commanders, staffs, and subordinates are not overwhelmed by the volume and availability of information, but instead are provided—or can derive—the required knowledge when they need it to make sound, ethical decisions and solve problems.[69] Knowledge management is applied continuously to optimize how data, information, and knowledge are collected, developed, and shared throughout the operations process (and supporting processes, activities, and procedures), within and among their distributed command nodes, across echelons, and with unified action partners.[70] Knowledge management is also employed to organize, adapt, and reorganize staffs as needed to generate and exploit knowledge rapidly, and to streamline an organization's battle rhythm and decision cycles across time zones, planning and event horizons, and with partners.

(4) *Responsive airspace management to facilitate cross-domain maneuver and all-domain fires*.[71] Future airspace management enables the safe, efficient, effective, and flexible use of assigned airspace among Army forces and their unified action partners for greatest operational effect. Future Army forces exploit the benefits of increased interoperability as part of joint all-domain C2 to create seamless airspace coordination, integration, and regulation at echelon between Army and joint airspace users and other unified action partners. With advancements in technology and a greater number of unmanned aircraft systems employed at all echelons, Army forces conduct real-time airspace management to deconflict flight paths and trajectories, make maximum use of its assigned airspace use while preventing fratricide, optimize aerial capabilities and effects, and enable MDO.

e. **Communications network.** The Army's future communications network encompasses all communications capabilities and associated procedures for collecting, processing, storing, displaying, disseminating, and managing data and information. From the highest Army echelons to the individual Soldier or Army Civilian, it is the Army's interoperable contribution to the larger Department of Defense (DOD) communications network.[72] Like the holistic nature of the C2 system of which it is a part, the Army's communications network is the totality of enterprise and deployed networks operating seamlessly as a unified whole. The Army communications network consists of—

- Network transport
- Information, information-management, and battle-management systems (including a tailorable battlespace visualization capability)
- Warfighting and business applications
- Network services
- Sensors and other network points of presence

- Data

> **Note:** *The AFCC-C2 describes the future communications network. For actions taken on or in the communications network, refer to the Army Futures Command Concept for Cyberspace and Electromagnetic Warfare Operations.*

(1) *A unified, protected, and resilient communications network that enables a multi-domain-ready force.*[73] The Army's future communications network is composed of an integrated and distributed architecture of subordinate network segments and nodes, transport, supporting infrastructure, platforms, devices, sensors and other points of presence, warfighting and business applications, services, and data arranged throughout bases, posts, camps, stations, facilities, and deployed locations that connect and support the entire Army. The future communications network provides the Army's (active and reserve) non-stop, day-to-day communications needs, and is flexible, tailorable, responsive, interoperable, and resilient enough to support an expeditionary Army operating with any set of unified action partners and in any environment.[74]

(a) The Army's future communications network is designed and built holistically to operate with and enable MC principles, supporting warfighting processes, necessary business procedures, and security requirements.[75] The communications network is defensible and maintains critical functionality even when large portions are destroyed or rendered inoperative. However, when the communications network is severely disrupted, units and individuals can disconnect information, information-management, and battle-management systems, continue to conduct operations on individual systems or as part of smaller local networks (including local sensors, platforms, and command nodes), and reconnect and resynchronize data and operations later within the larger communications network when connectivity is restored. Applications, interfaces, and visualization tools are simple, intuitive, and tailorable to the natural aptitudes and limitations of each operator. Investment strategies for the communications network include sustained leader development and organizational and technical training.[76]

(b) Overall, the future communications network must facilitate the following C2 operational imperatives that enable future MDO. (See appendix H for a detailed discussion of the communications network and these operational imperatives.)
- Continuity of command
- Expeditionary, dispersed, and decentralized operations
- Interoperability with unified action partners
- Convergence of capabilities and their effects from, in, and across all of the domains
- Rapid force tailoring, dynamic task organization, and support of commander's priorities
- Leverage of data and information[77]
- Collaborative development of shared understanding
- Parallel planning and rapid order development and dissemination
- Fusion of operational, sustainment, and civil information with intelligence
- Training, wargaming, rehearsals, and in-stride decision making

(2) *Common, standardized, shareable, and secure data.* All future technology intended to connect to the Army's communications network must be designed to organically interoperate as

part of a joint common operating environment, and send and receive common, standardized, shareable, and secure data among all components and—to the greatest extent possible—unified action partners.[78] *Common data* is data that is synchronized to ensure that all users see the same representation of reality. Common data is authoritative and available to all users at the speed available through the communications network. *Standardized data* is a data storage schema that includes data form, format, structure, tagging, domain values, and semantics. *Shareable data* is data that can be discovered, accessed, understood, and transformed into a digestible format to internal and external users without changing the intent of the representation, including any mission partner or legacy system not compliant with standardized data models. *Secure data* is data that is protected against unauthorized use and manipulation.

(a) Common, standardized, shareable, and secure data is critical to the AI, machine learning (ML), and big data analysis that supports decision making, and to linking all sensors to the right command nodes and the best shooters. Without common, standardized, shareable, and secure data, the necessary improvements in the speed and quality of decision making, the ability to converge capabilities across all of the domains to create windows of superiority, and the capability to seamlessly interoperate technically with partners will not be possible.[79] Common, standardized, shareable, and secure data is at the heart of the Army's and the joint force's ability to out-think, out-maneuver, and outpace any competitor, deter aggression, and win in multi-domain competition, crisis response, and armed conflict with the lowest costs to the Army and the nation.[80] These required data qualities are achieved through two primary methods. First, *new* data can be created at the outset to be common, standardized, shareable, and secure. Second, *existing* data can be analyzed in whatever location and format that it is found in, and the results translated or converted to take on these qualities sufficiently to be widely, rapidly, and securely distributed and used among unified action partners.[81] Both approaches are required for the future timeframe of this concept. (See appendix H for more discussion of these two approaches.)

(b) Common, standardized, shareable, and secure data is necessary, feasible, and achievable in the timeframe of this concept. However, senior leaders must view data as a strategic asset that must be operationalized. As such, they must aggressively pursue and ruthlessly enforce Service adherence to established data criteria.[82] While standardizing data structures, applications, and information systems to develop interoperability and a common user experience, the communications network maintains the flexibility to incorporate emergent technology quickly. The Army's future communications network must be linked and allow users to access and pull data or have relevant data pushed to them. Linked and accessible data allows users to manipulate and analyze that data, and create new, intuitive presentations to help commanders and staffs develop a shared understanding of operational and mission variables and the cause-and-effect relationships among them.

(3) *A tailorable battlespace visualization*. A tailorable battlespace visualization capability enables a shareable display of relevant information tailored to the user's requirements and based on common data and information from across one or more domains, the EMS, the IE, and warfighting functions. It allows for continuous shared situational understanding among all unified action partners. This future visualization capability can be easily filtered to each individual's security clearance and need to know.

f. **CPC**. *A constellation of rapidly deployable, tactically mobile, tailorable, scalable, and survivable command nodes*. The future CPC is the variable arrangement of multiple, distributed, and meshed command nodes cross-functionally organized from home station to the close area.[83]

(1) The CPC allows commanders to adapt to the environment and situation that they face. The multiple command nodes that may form the future CPC are connected by the communications network. These command nodes provide the physical locations from where the C2 system's people meet (in person or virtually) to perform the functions that enable C2 and the timely integration, dynamic synchronization, and optimal convergence of capabilities from all of the domains with other elements of national power. All command nodes are able to seamlessly link to each other to form one cohesively-functioning CPC—though each node and the people within are designed and prepared to operate under the MC approach should communications be disrupted.

(2) The future Army CPC is designed as a fully-integrated, sociotechnical system of communications network capabilities, vehicles, energy-efficient shelters and workspace, power generation and distribution equipment, and other ancillary equipment and supporting infrastructure capable of dividing into multiple command nodes dispersed around the extended battlespace but connected and operating as a unified whole.[84] (See appendix K for common C2 functions.) The future Army CPC is fielded as a complete capability package that includes long-term education, training, and life-cycle sustainment strategies. To increase agility, realize the MC approach, and enable expeditionary operations, the nodes that form the CPC are smaller and less complex, strive to automate routine functions, decrease cognitive burden, optimize human interaction, and support self-forming teams. Among multiple survivability considerations, the future Army CPC is aware of its own visual, thermal, radio frequency, acoustic, and seismic signatures and can, as necessary, decrease, obscure, or otherwise manage and control these identifying signatures.[85] (See appendix I for a detailed discussion of the CPC and the functional characteristics that enable the achievement of decision advantages during future MDO.)

3-5. Supporting ideas

a. The following section describes the cross-cutting supporting ideas that contribute to the realization of the components of the solution described above. (See figure 3-3 for the list of the supporting ideas.)

Supporting Ideas	
• Leader development that fosters disciplined initiative • Talent management in support of the MC approach and MDO • Operations in the information dimension integral to winning in competition, crisis response, and armed conflict • Seamless interoperability among unified action partners • Appropriately tailored authorities and permissions	• Human-machine cooperation, collaborative decision making, and battle management • Building trust in people, processes, the communications network, and the CPC • Truth as a weapon against threat disinformation • Supportive training environments and infrastructure

Figure 3-3. Supporting ideas

b. *Leader development that fosters disciplined initiative*.[86] A bias for action through disciplined initiative becomes ingrained in the Army culture and ethos primarily through leader development and organizational training.[87] MC is at the center of the Army's ability to achieve a decision advantage and win decisively.[88] All Army leaders (Soldiers and Army Civilians) are proficient in exercising MC when conducting operations, military functions, and daily administrative activities

throughout the operating and generating force.[89] While the objective is to institutionalize MC into the Army's culture and ethos, it is a perishable quality vulnerable to neglect and the influence of new technology that allows leaders to micromanage subordinates easily.[90] Army leaders, particularly at senior levels, must emphasize and demand the MC approach in training and everyday activities. The Army will fail in future competition, crisis response, and large-scale combat against near-peer threats unless it can effectively employ the MC approach. However, it cannot be "turned on at the flip of a switch." The MC approach must be stressed and practiced daily in training and all garrison activities.[91]

(1) Comprehensive, realistic, and challenging education and training develops the knowledge and experience necessary to create trusted, ethical leaders, Soldiers, and teams with an expeditionary mindset capable of conducting MDO under all conditions.[92] Fundamental changes to training and education are required to develop future Army leaders with adequate understanding of other Service and joint capabilities and processes, and Army leaders who actively seek to build multi-domain teams and drive a whole-of-government approach to multi-domain competition, crisis response, and conflict.[93] Leader development is critical as Army leaders will ultimately determine whether MC will, or will not, thrive and flourish.[94] Future Army leaders must be skilled trainers, teachers, motivators, and communicators capable of building a candid and collaborative climate among a diverse group of unified action partners. They must develop bold, agile, and innovative subordinates and model the courage to trust, the confidence to delegate, and calmness in the face of adversity. Finally, future Army leaders must demonstrate the patience and restraint to allow lower echelons to develop the situation through decisive action and the moral nerve to underwrite honest mistakes. By doing so, future Army forces achieve extraordinary results, remain the preeminent land force, and become indispensable multi-domain team members.[95]

(2) While self-development and personal study are essential to growing Army leaders capable of exercising MC, all leaders are personally and professionally responsible for the development of bold, agile, innovative, and ethical subordinates.[96] MC does not exist unless leaders actively promote and develop these traits in their subordinates. Developing bold, agile, and innovative leaders of character capable of exercising MC requires personal will, commitment, and time. These qualities thrive in units and organizations with leaders who model and develop them in every Soldier and Army Civilian as a part of organizational and institutional leader development. Without active leader commitment to its development, MC has little chance of realizing its potential.[97] Ultimately, the extent to which MC is realized within Army forces is determined by the decisions, actions, and resolute influence of all Army's leaders, from the Secretary and Chief of Staff of the Army to team and section leaders.[98]

c. *Talent management in support of the MC approach and MDO.* Leader commitment to developing subordinates with strength of character capable of successfully employing the MC approach and conducting MDO is made clear through teaching, coaching, mentoring, and counseling subordinates.[99] However, the ability to execute these responsibilities is also taught, developed, identified, and equitably rewarded.[100]

(1) Fundamental reform and revitalization of Army talent management policies and procedures include alignment of accessions, education, assignments, position tenure, time-in-grade requirements, certifications, evaluations, promotions, command selections, and

compensation. Future reforms will reflect the commitment to progressive and sustained leader development that nurture the leader attributes essential to MC and support the development of flexible career paths that cultivate the multi-domain skills and knowledge necessary to make rapid, quality, data-driven decisions and conduct MDO.[101]

(2) Critical to developing and managing talent, the Army revitalizes and invests in the continuous development of its faculties at its leader development institutions and its observer-coach-trainers at its combat training centers (CTCs) to ensure and exploit institutional and operational unity of effort.[102] Proven leaders, tacticians, and logisticians skilled in applying the mission command principles are selected to teach, coach, train, and develop future commanders, leaders, Soldiers, and Army Civilians. Moreover, a sustained faculty and CTC trainer education program (as a close partnership) keeps pace with change and ensures that the professional military and civilian education system and CTC exercises deliver the outcomes required to support the Army's current and future needs.[103]

(3) These talent management modifications balance individual talents to Army needs, and challenge, develop, inspire, and retain innovative Army leaders capable of transforming the Army to meet the multi-domain demands of the future.[104] Without these changes, the Army is unlikely to imbue the MC approach and MDO-mindset within the force successfully.[105] With these changes, the Army's future leaders, Soldiers, and Army Civilians possess the cognitive abilities, knowledge, diversity, judgment, emotional and social intelligence, and warfighting skills necessary to build and sustain cohesive teams with the right mix of domain capabilities. Lastly, these changes serve to create future Army leaders who can synthesize and use data, make rapid, quality decisions, adapt to complex situations, and think, plan, and act in multiple domains to create decisive overmatch against future threats.[106]

d. *Operations in the information dimension integral to winning in competition, crisis response, and armed conflict*. In future MDO, deep sensing; protecting information; providing information to inform, educate, or influence; and conducting information warfare (including military deception) are decisive to winning in competition, crisis response, and armed conflict, particularly in the information and cognitive dimensions of the battlespace. Employing effects in the IE can be as important as maneuvering physically. As such, Army leaders persistently plan, integrate, and synchronize information capabilities and activities to inform and educate domestic and foreign-friendly audiences, inform and influence foreign neutrals, counter disinformation and propaganda, affect threat decision making, and shape the larger IE to gain, maintain, and exploit the operational initiative. Future Army leaders understand and accept information engagement and information warfare as critical and essential features of MDO.

e. *Seamless interoperability among unified action partners*.[107] Future globally-integrated MDO place a premium on partnering.[108] Partnering increases the depth and breadth of the knowledge, expertise, and capabilities required to deter and defeat future adversaries and enemies. Interoperability, both within the Army itself and with unified action partners, improves agility and is essential to rapidly forming and reforming joint and coalition multi-domain teams.[109] A high degree of interoperability must be realized by all Army warfighting functions and supporting activities. However, achieving it begins with the C2 warfighting function.[110]

(1) Interoperability is viewed commonly in purely technical terms. In the future, the level or degree of interoperability to succeed requires equal emphasis on the human and procedural aspects to address cultural and organizational differences.[111] In particular, an appreciation of cultural and policy differences, an ability to communicate cross-culturally and in the partner's native language, and a willingness to leverage diverse capabilities and perspectives are necessary to effectively team with unified action partners. Achieving interoperability begins with developing a shared conceptual understanding among Army forces and unified action partners of how forces and organizations conduct and sustain MDO and apply a whole-of-government approach throughout the competition continuum.

(2) While this concept takes the approach that many of the Army's current integration processes are, at their base level, sufficiently broad to allow necessary adaptation and modification during the concept's timeframe, it does not rule out that some processes may need to be abandoned altogether and new processes developed and instituted. Wherever possible, the Army and other Services must adopt joint processes outright.[112] Rather than modifying Army-only processes, wholesale adoption of joint processes (and shared terms) gains efficiencies and drives the interoperability required by future MDO.[113] However, any future integration processes—joint or Army-specific—must be comprehensive and habitually consider capabilities from all available domains that can be brought to bear to accomplish assigned missions across the physical, cognitive, temporal, and virtual aspects of the battlespace.

f. *Appropriately tailored authorities and permissions*. A complex, highly-competitive, and hyperactive physical and non-physical OE—with an inherent lack of predictability—greatly increases the need for and value of agility. To operate in all of the domains with the necessary agility and apply capabilities at the speeds required to out-think, out-maneuver, and outpace threats in future MDO, Army forces and their unified action partners require tailored authorities and permissions extended to the lowest practical echelon.[114] These expanded authorities cover three broad areas—access, surveillance, and employment—and allow Army forces to conduct MDO to deter adversaries from escalation, counter their information and irregular warfare, undermine their efforts to coerce partners with the threat of armed conflict, and set conditions in case of conflict. In competition, crisis response, and conflict, authorities to operate in the space and cyberspace domains and the IE are granted earlier and faster to enable Army forces to be proactive, make decisions, set the operational tempo, and overall, gain, maintain, and exploit the operational initiative.[115]

(1) In competition, future Army forces need access to and presence in military and civilian networks that enable them to operate to gain information advantages. In crisis response and armed conflict, future Army forces and their partners must have appropriate authorities and permissions, with skills honed through iterative training, to employ capabilities such as electromagnetic attack, offensive cyberspace, space control measures, and lethal strikes—especially to support a rapid transition from competition through crisis to conflict. Tailored authorities must also enable the Army's role as a force provider and allow the notification and mobilization of planned and contingency reserve component forces.

(2) To achieve the decision speeds required for future MDO, conditions-based authorities and permissions are established for the use of compartmented capabilities and programs previously

held at the combatant command, Secretarial, or higher level. Conditions-based authorities and permissions are those that are delegated to a subordinate under pre-determined circumstances including loss of communications and the criticality of the situation.[116] Whether commanders may further delegate conditions-based authorities and permissions is an essential element that must be specifically stated.

(a) Conditions-based authorities and permissions must balance the risk that subordinates' missteps may have on the strategic or operational situation versus the risk to operations from missing opportunities (opportunity costs) or not rapidly countering threat actions (inaction costs). Building on multiple training repetitions, commanders consider which authorities and permissions to grant by thoroughly examining the aspects of risk that may lead to strategic or operational blunder, particularly those actions that would result in radical escalation, damaged alliances, or diminished public support. The opportunity or the minimization of threat effects gained through speed of action must sufficiently outweigh the risks of taking action normally held at a higher echelon.

(b) Shared understanding and the ability to take disciplined initiative are key to the proper distribution of authorities and permissions. The establishment of conditions-based authorities and permissions require all commanders to also have a shared understanding of risk. These risk considerations are formerly included with the conditions-based authorities and permissions. Conditions-based authorities, permissions, and identified risks are tested and validated extensively in experimentation, continually assessed and refined in training and exercises, and subject to formal periodic reviews.[117] Through shared understanding and trust, supported by common data and information across echelons, future Army commanders understand risk and use conditions-based authorities appropriately to accomplish their higher-level commander's intent.

(3) An important aspect of authorities and permission relates to the use of AI to autonomously make quality decisions and take action. The autonomy granted to AI to make and execute decisions is based on two primary factors. First is the accuracy and precision of the AI. Over time, demonstrated accuracy and precision develop trust. Second is the acceptance of the associated risk. These factors are not static and change over time as technology matures, algorithms are refined and sharpened, Army forces train and gain technical expertise, and the political, operational, or tactical situation affecting risk decisions emerges and develops. (See the discussions of AI in the next two supporting ideas.)

g. *Human-machine cooperation, collaborative decision making, and battle management*. AI with widest access to networked sensors and large volumes of seemingly disparate data and information can rapidly make sense of information and feedback from Army and all other linked data sources to generate decision-quality information and provide reasoned probability predictions, decreasing the cognitive burden on commanders and staffs and increasing the speed and quality of decision making. An AI-enabled C2 system can also aid commanders and staffs in monitoring the environment, recognizing and prioritizing targets and opportunities, making accurate assessments, and otherwise managing and controlling the operation during execution. Future AI can be programmed to learn and adapt to a particular commander's or staff leader's information requirements, preferred visualization or display formats, cognitive processes, and other individual peculiarities without reinforcing potentially negative personal biases. However,

like humans, AI (and machines in general) have strengths and weaknesses in their application. Machines can communicate faster with each other than with humans.[118] AI is better suited to perform some analytical tasks than others. As such, AI must be oriented toward repetitive, time-consuming tasks that machines can do best, while humans focus their talents and energies on the creative tasks that they do best.[119]

(1) Humans and AI can cooperatively inform each other of the quality and degree of risk associated with the recommendations and decisions they produce. AI can monitor personnel and provide feedback on Soldiers' current abilities to make quality decisions based on factors such as amount of sleep, hormone levels, mental focus, personal life complications, and other biomarkers and human-state considerations. This feedback helps commanders and staff leaders to better understand the quality of information and decisions coming from within their command as well as a check on their own personal decisions. Conversely, AI can provide a constant status of its own ability to make quality decisions based on influential factors such as incomplete, compromised, or spoofed data; faulty sensors; degraded network connectivity; computing hardware or software failures, malfunctions, or abnormalities; learned or unwittingly-programmed biases; and other environmental factors.[120] While no information is perfect, future AI includes a means to evaluate the accuracy, reliability, and objectivity of information based on voluminous amounts of data, recent and historical trend comparisons, and real-time situational developments.[121]

(2) Future human-machine teaming can contribute significantly to the survivability of the communications network and command nodes. AI, ML, and big data analysis can help create self-healing networks by autonomously redirecting communications from one means of transport to another through a linked mesh network. AI and ML can also be used to detect and isolate adversary intrusions into the future communications network. Future AI-enabled machines may duplicate essential C2 functions and activities and create the necessary redundancy at multiple command nodes that are situationally dispersed throughout the expanded all-domain battlespace. AI-enabled decision-making tools and battle management systems may augment or replace some staff while also reducing the potential for cognitive overload. This is particularly applicable for tedious, time-intensive, or repetitive accounting tasks more easily and accurately performed by machines.

h. *Building trust in people, processes, the communications network, and the CPC.* Trust contributes to overall speed and agility. The Army's future all-domain-capable C2 system requires trust of, and trustworthiness in, each component of the system to function effectively. In each of these components, trust is built as a result of realistic and repeated experimentation and training under expected operational conditions at all echelons.[122] Through this trust-but-verify cycle of testing, training, and adapting, leaders develop trust in themselves, their subordinates, their processes, and their technology. Trust speeds decision making.

(1) Trust in people. Subordinates take disciplined initiative readily when their leaders empower them and they are valued and trusted as part of a team.[123] Agile, cohesive teams develop within a climate of mutual trust between and among Army leaders, Soldiers and Army Civilians; Army leaders and other unified action partners; and between Army and governmental leaders within domestic and foreign populations.[124] Through iterative training with joint partners, Army and other-Service leaders gain a more refined understanding of how to leverage and combine each other's capabilities and partner in novel ways to overmatch adversaries and win.

(2) Trust in processes. The processes used in competition, crisis response, and conflict must be the processes practiced on a daily basis at home station. To the maximum extent possible, Army leaders should utilize the same operations, knowledge management, information management, and other warfighting integrative processes in garrison and training as in actual operations. To provide multiple, realistic repetitions that help develop trust, Army leaders leverage the future synthetic training environment capable of replicating the speeds and ranges of current and future weapons and technology.

(3) Trust in the communications network. Commanders and their staffs must be able to trust the various components of the communications network, and be comfortable operating in a degraded network environment. Commanders must be able to sense and understand what data and information must be transported at what echelon to ensure mission-critical data gets to where it needs to go in time to achieve the effects required.

(a) Trust in data. Future MDO will run on real-time trustworthy data. Data becomes trustworthy when it is common, standardized, shareable, and secure.[125] The future communications network must be designed with built-in cybersecurity to enable Army forces to discover or create, easily access, readily share, and leverage trustworthy data. Future Army forces must be able to trust in the validity and currency of the data provided by joint and other unified action partners, that mission partners will protect data shared with them, and that future technological systems and applications will be able to rapidly identify and isolate malicious or errant data.[126]

(b) Trust in AI. Future Army commanders remain accountable for the decisions that they may make based on AI-generated knowledge and recommendations. Therefore, future Army commanders must continuously develop and reinforce trust in AI and other technological systems to provide them reliable information to inform their decisions in the same manner as they develop and maintain trust in human staff and subordinate commanders.[127] If a commander cannot trust the recommendations and data synthesis provided by an AI application, then the AI may have the opposite effect of that intended.[128] The speed and quality of decision making would actually be diminished.[129] To remain trustworthy, future AI-enabled systems must display or describe the underlying assumptions and logic chains that support their recommendations in a format that is easily understood by commanders and staffs.[130] When properly implemented, DOD's five ethical principles for AI—responsible, equitable, traceable, reliable, and governable—will help build the trust necessary to exploit AI-enabled decision making.[131] Importantly, the trustworthiness of AI is directly related to the trustworthiness of the data it consumes—and AI can help determine if data has been manipulated nefariously.

(4) Trust in the CPC. Future Army commanders develop the necessary processes, procedures, and policies—and trust in their subordinates ability to follow them—to ensure that dispersed command nodes interoperate and support the commander and subordinate headquarters as required, particularly command nodes operating at great distances and in different time zones. The institutional Army and operational commanders work together to educate, train, and prepare Soldiers and Army Civilians to be trustworthy so that, even when dispersed and not under direct leadership, they will have the training and capabilities (including authorities) required and be fully capable of accomplishing assigned missions and tasks.

i. *Truth as a weapon against threat disinformation.* Supported by the actions of their intelligence organizations, future adversaries and enemies employ information capabilities in a deliberate, whole-of-nation disinformation campaign to confuse opponents and achieve strategic objectives at minimal cost. The intentional spread of misinformation and use of disinformation is also an effective tactic against political rivals.

(1) Consequently future Army commanders counter misinformation and disinformation through the release of timely and accurate Army-related information to thwart threat activity, defend the Constitution, and protect national interests.[132] Through public affairs and within operational security constraints, future Army commanders preempt, identify, and counter attempts at malign narrative through the distribution of legitimate, timely, and truthful information regarding Army operations, equipment, and personnel across the various information platforms. Friendly domestic and foreign audiences, as well as neutrals, seek and trust future Army leaders for the objective, apolitical truth.[133]

(2) Threat audiences, however, remain critical targets for future commanders' own misinformation and disinformation narratives. In armed conflict, there is no moral requirement to furnish the truth to the enemy.[134] Balancing truth telling with friends and disinformation with enemies requires commanders and appropriate staff members that understand operational security concerns and the false narratives that are being employed as weapons against the nation's enemies.[135]

j. *Supportive training environments and infrastructure.* The most effective way to prepare Army leaders is to replicate the relevant aspects of the complex future environment accurately. Whether in the classroom, at home station, or in CTCs, the Army's future training environments and infrastructure support the development and execution of context-based, problem-solving exercises against a top-tier, free-thinking opponent to challenge and develop critical and creative thinking, and ethical decision making.[136] The future training environments and infrastructure also support higher-classification training requirements (individual and organizational), unified action partner participation, and greater Soldier access to increase all-domain understanding within the force and with partners.

(1) The Army's future physical and synthetic training environments—including experiments, wargames, table-top exercises, models, and simulations—closely replicate the effects of employing information capabilities on key audiences, the effects of key audiences and the rapid, viral nature of social media on Army operations, and how well information capabilities are being employed for effect. Additionally, an overabundance of information is also replicated in future training environments. Army leaders—with and without the assistance of AI—become skilled at identifying, prioritizing, and analyzing the most important data and information from the vast quantities available. The threats' ability to identify and target command nodes and degrade communications is a constant condition also represented in future training environments. However, physical and synthetic training environments allow the replication of future signature management and control systems, decoys, and other camouflage, concealment, and deception capabilities to hide critical forces and capabilities (including command nodes) and mislead threats. Generally, future training environments enable Army forces to design and develop lethal, cohesive,

trustworthy, and multi-domain teams capable of operating in a complex, highly-competitive, and hyperactive physical and non-physical OE against near-peer adversaries and enemies.[137]

(2) Future training and exercises are designed specifically to test policies, processes, and procedures for rapidly delegating the authorities and permission necessary to act to gain advantage in competition, crisis response, and conflict. The Army will also use experiments to test future conditions-based authorities to identify how advanced capabilities can be employed properly and to ensure that risk is properly identified and understood by superiors and subordinates alike. Based on lessons learned, changes are made to better streamline authorities and educate leaders of the responsibilities entrusted to them with greater authorities and permissions.

(3) Army leaders apply innovative training approaches that capitalize on AI to enhance human abilities and improve the speed and quality of decision making. Commanders streamline training management by offloading data-centric training management tasks to AI systems. They leverage these systems to create training plans, model complex maneuver qualifications, and identify additional skills and training needed to achieve them. Leaders exploit AI strengths to refine and assess virtual skills while developing the human skills and creativity needed to solve ill-structured problems and develop leadership skills, risk acceptance, ethical decision making, and social and emotional intelligence. AI systems enhance readiness by returning meaningful training time to leaders by managing and analyzing individual and collective training data and suggesting training efficiencies and improvements.[138]

(4) Recognizing that people acquire and develop knowledge, skills, and abilities in different ways and at different rates, the training and education infrastructure is tailorable to individual needs whether in a field or classroom environment, on a major installation or remote site, or in CONUS or an overseas location. Individual accommodations help expand learning and leader development beyond episodic attendance in formal schools allowing individuals to reach their unique potential. This infrastructure includes a robust capability for mobile and collaborative, peer-to-peer learning and tutoring, and the flexibility to adjust quickly and accommodate initial feedback from students undergoing training. Further, the infrastructure is able to adapt to feedback from reality-based assessments of earlier program graduates serving in subsequent leader and staff positions, and to lessons learned from operational unit training or real-world activities. This is applying MC approach to create a shared understanding of individual and operational training and education requirements between the operational and institutional Army, and to encourage and empower individuals to take the initiative for self-development and fulfill their responsibilities as stewards of the Army profession.

Chapter 4
Conclusion

a. The Army faces a highly complex, competitive, hyperactive, and potentially lethal OE and prepares to conduct the full range of military operations throughout the entire competition continuum and against a multitude of threats anywhere in the world. The nature of the future security environment and the broad range of potential missions combine to present Army forces with unfamiliar, ill-structured, and emergent situations requiring them to operate in unanticipated

ways. These conditions and challenges require the intuitive application of MC's fundamental principles and the artful application, shrewd integration, and synergistic convergence of available destructive, constructive, and information capabilities throughout all of the domains. Development and application of the MC approach to C2 and a future all-domain-capable C2 system serve to overcome surprise and uncertainty, promote initiative and adaptability, create decision advantages, and facilitate success in multi-domain competition, crisis response, and armed conflict.

b. The AFCC-C2 broadens the Army C2 warfighting function. This adjustment enlarges the warfighting function's role to facilitate greater interoperability and the ability to conduct future MDO. This concept proposes that the warfighting function expand beyond simply integrating warfighting functions—to combining and dynamically synchronizing Army combat power across all of the domains *and with* all instruments of national power, U.S. and coalition.[139] Future Army forces adjust their C2 system to better assist joint and national authorities in converging all instruments of national power to protect and proactively advance national interests. Future Army forces understand and are full contributing members to a whole-of-government approach to protecting and achieving national interests.[140]

c. Future C2 system capabilities allow Army forces to make and disseminate better and faster decisions than an adversary; gain, maintain, and exploit the operational initiative; and achieve decision dominance. While the AFCC-C2 addresses capabilities across all components of the future all-domain capable C2 system, it prioritizes the human element and the changes necessary for bold, agile, and innovative leaders, Soldiers, and Army Civilians and cohesive joint, multinational, and interorganizational teams to win in a complex, highly-competitive, and hyperactive physical and non-physical OE. Technological tools, effective multi-domain processes, and the right authorities at the right echelon are critical enablers that must be achieved, but the development of bold, agile, adaptive, and competent Army leaders of character that thrive in ambiguity and fast-paced, data-driven operations will remain the key competitive advantage for success against any future threat.[141]

Appendix A
References

Across all references: Army regulations (ARs), Department of the Army (DA) pamphlets, Army doctrine publications (ADPs), Army field manuals (FMs), Army techniques publications (ATPs), and DA forms are available at Army Publishing Directorate Home Page https://armypubs.army.mil/. TRADOC publications, TPs and forms are available at TRADOC Publications website at https://www.tradoc.army.mil/Publications-Resources/. Joint publications (JPs) are available at the Joint Electronic Library at http://www.dtic.mil/doctrine.

Section I
Required references

ADP 6-0
Mission Command: Command and Control of Army Forces

TP 525-3-1
The U.S. Army in Multi-Domain Operations 2028

TP 525-3-8
The U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045

Section II
Related references

ADP 3-0
Operations

ADP 3-28
Defense Support of Civil Authorities

ADP 5-0
The Operations Process

ADP 6-22
Army Leadership and the Profession

ADP 7-0
Training

Alberts, S., et al. (2015, September). *C2 by Design: Putting Command and Control Agility Theory into Practice*. Alexandria, VA: Institute for Defense Analysis. Retrieved from https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/SFRD/2016/D-5614.ashx

Alexander, K. (2013, August). The Army's way ahead in cyberspace. *Army Magazine, 63 (8)*, 22-25.

Ancker, C. (2013, March-April). The evolution of mission command in U. S. Army doctrine, 1905 to the present. *Military Review*. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20130430_art008.pdf

AFP 71-20-1
Army Futures Command Concept for Maneuver in Multi-Domain Operations 2028

AFP 71-20-2
Army Futures Command Concept for Brigade Combat Team Cross-Domain Maneuver 2028

AFP 71-20-3
Army Futures Command Concept for Intelligence 2028

AFP 71-20-4
Army Futures Command Concept for Special Operations 2028

AFP 71-20-5
Army Futures Command Concept for Aviation 2028

AFP 71-20-6
Army Futures Command Concept for Fires 2028

AFP 71-20-7
Army Futures Command Concept for Protection 2028

AFP 71-20-8
Army Futures Command Concept for Cyberspace and Electromagnetic Warfare Operations 2028

AFP 71-20-10
The U.S. Army Concept for Space 2028

AFP 71-20-11
Army Futures Command Concept for Sustainment 2028

AFP 71-20-12
The U.S. Army Concept for Medical 2028

AR 25-1
Army Information Technology

AR 34-1
Interoperability

AR 5-12
Army Use of the Electromagnetic Spectrum

ATP 3-12.3
Electronic Warfare Techniques

ATP 3-13.1
The Conduct of Information Operations

ATP 3-57.50
Civil Affairs Civil Information Management

ATP 5-0.1
Army Design Methodology

ATP 6-0.5
Command Post Organization and Operations

ATP 6-01.1
Techniques for Effective Knowledge Management

ATP 6-22.6
Army Team Building

Barno, D. (2014, July 10). The Army's next enemy? Peace. *The Washington Post*. Retrieved from http://m.washingtonpost.com/opinions/the-armys-next-enemy-peace/2014/07/10/f02b5180-f0dc-11e3-914c-1fbd0614e2d4_story.html

Barno, D. & Bensahel, N. (2015, November 5). Can the U.S. military halt its brain drain? *The Atlantic*. Retrieved from http://www.theatlantic.com/politics/archive/2015/11/us-military-tries-halt-brain-drain/413965/

Bērziņš, J. (2014, April). *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Center for Security and Strategic Research, National Defence Academy of Latvia. Retrieved from http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx

Better Data Management Can Win Wars. (2020, July 16). Association of the United States Army. Retrieved from https://www.ausa.org/news/better-data-management-can-win-wars

Blannin, P. (2018, May 4). The good operations: Notes on a whole-of-government approach to national security. Modern War Institute. Retrieved from https://mwi.usma.edu/good-operation-notes-whole-government-approach-national-security/

Brown, R. & Perkins, D. (2017, August 18). Multi-domain battle: Tonight, tomorrow, and the future fight. *War on the Rocks*. Retrieved from https://warontherocks.com/2017/08/multi-domain-battle-tonight-tomorrow-and-the-future-fight/

Bunker, R. (2020, May). Mission command and armed robotic systems command and control: human and machine assessment. *Land Warfare Paper*, (132). Arlington, VA: Association of the United States Army. Retrieved from https://www.ausa.org/sites/default/files/publications/LWP-132-Mission-Command-and-Armed-Robotic-Systems-Command-and-Control-A-Human-and-Machine-Assessment.pdf

Capstone Concept for Joint Operations (CCJO): Joint Force 2030

Clarke, S., et al., editors. (2016). *The Ethics of Human Enhancement: Understanding the Debate*. Oxford, UK: Oxford University Press.

Corbett, A. (Undated). *Mission Command*. Norfolk, VA: Naval Warfare Development Command. Retrieved from https://www.nwdc.navy.mil/.../Corbett%20-%20Mission%20Command%20document.pdf

Covey, S.M.R. (2006). *The Speed of Trust: The One Thing That Changes Everything*. New York, NY: Free Press.

Curthoys, K. (2014, December 2). Study: Mental cues, conditions that affect performance. *Army Times*. Retrieved from http://www.armytimes.com/story/military/pentagon/2014/12/03/iitsec-brain/19824701/

DA. (2014). Army Strategic Planning Guidance 2014. Retrieved from http://www.army.mil/info/references/

DA. (2019, October). Army People Strategy. Retrieved from https://people.army.mil/wordpress/wp-content/uploads/2019/10/The-2020-Army-People-Strategy-Final.pdf

DA. (2015). Army Vision: Strategic Advantage in a Complex World. Retrieved from http://usarmy.vo.llnwd.net/e2/rv5_downloads/info/references/the_army_vision.pdf

DA. (2019, November 15). HQDA EXORD 009-20: Army Data Plan Implementation in Support of Cloud Migration. Available upon request through the proponent.

DA, Chief Information Officer/G-6. (2014, August 1). Annex B to LandWarNet 2020 and Beyond Enterprise Architecture: Definitions and Guidance for the Common Operating Environment. Retrieved from http://ciog6.army.mil/Portals/1/Architecture/2014/20140801-Annex_B_Definitions_Guidance_COE_V2-0.pdf

DA, Chief Information Officer/G-6. (2016, March). Shaping the Army Network: 2025-2040. Retrieved from http://ciog6.army.mil/Portals/1/Shaping%20the%20Army%20Network%202025-2040.pdf

DA, Chief of Staff of the Army Strategic Studies Group-I. (2013, July). Testing Assumptions about the Role of Land Power in 2030 Final Report. Washington, DC. Available upon request through the proponent.

DA, U.S. Army Center for Lessons Learned. (2020, April 08). *New From the Front: The Army Interoperability Measurement Systems AIMS*. Fort Leavenworth, KS. Retrieved from https://call2.army.mil/docs/doc18020/18020.pdf

DA. (2020, November 6). *U.S. Army Mission Command Network Implementation Plan Volume 1—Framework*. Available upon request through the proponent.

Dahm, M. (2020, June 5). Chinese debates on the military utility of artificial intelligence. War on the Rocks. Retrieved from https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/

Dempsey, M. (2011, February). Leader development. *Army Magazine*, 61(2), 25-28.

Dempsey, M. (2012, April 3). Mission Command White Paper. Retrieved from http://www.jcs.mil/content/files/2012-04/042312114128_CJCS_Mission_Command_White_Paper_2012_a.pdf

Department of Defense Dictionary of Military and Associated Terms

Deptula, D. (2020, July 9). Moving further into the information age with joint all-domain command and control. *C4ISRNET*. Retrieved from https://www.c4isrnet.com/opinion/2020/07/09/moving-further-into-the-information-age-with-joint-all-domain-command-and-control/

Derleth, J. (2018, February 28). Fostering a whole-of-government approach to national security from the bottom up. *Military Review*. Retrieved from https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Feb/Fostering-Security/

DOD. (2020, January 31). Deputy Secretary of Defense Joint All-Domain Command and Control Cross Functional Team Establishment Memorandum.

DOD. (2020, October 08). DoD Data Strategy. Retrieved from https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

DOD. (2018, December 13). DOD Directive 3000.05: Stabilization. Retrieved from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300005p.pdf?ver=2018-12-13-145923-550

DOD. (2013, August 5). DOD Instruction 8320.02: Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense. Retrieved from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/832002p.pdf

DOD. (2015, August 3). DOD Instruction 8320.07: Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense. Retrieved from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/832007p.pdf?ver=2019-06-06-091932-567

DOD. (2016, September 15). DOD Instruction 8420.02: DoD Satellite Communications (SATCOM). Retrieved from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/842002p.pdf

DOD. (2019, June 5). DoD Digital Modernization Strategy: DoD Information Resource management Strategic Plan FY 19-23. Retrieved from https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

DOD. (2020). Joint All-Domain Command and Control Vision (draft version 0.6).

DOD. (2018). Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, U.S. Department of Defense. Retrieved

from https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

DOD, Chief Information Officer. (2013, September 11). Electromagnetic Spectrum Strategy 2013: A Call to Action. Retrieved from http://dodcio.defense.gov

DOD, Defense Advanced Research Projects Agency. (Undated). *DARPA and the Brain*. Retrieved from https://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative

DOD, Defense Innovation Board. (2019, October 31). *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*. Retrieved from https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF

DOD, Defense Innovation Board. (2019, October 31). *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense Supporting Document*. Retrieved from Retrieved from https://media.defense.gov/2019/Oct/31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_DOCUMENT.PDF

DOD, The Joint Staff. (2018). Description of the National Military Strategy 2018. Retrieved from https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf

DOD, Office of the Undersecretary of Defense for Acquisition, Technology, & Logistics. (2011, October). Unmanned Systems Integrated Roadmap FY2011-2036. Retrieved from https://apps.dtic.mil/docs/citations/ADA558615

Doty, J. & Fenalson, J. (2013, July). Mission command and mission accomplishment. *Army Magazine, 59(9)*, 16-18.

Dunlap, C. (2017, May-June). Lawfare 101: A primer. *Military Review*. Retrieved from https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Dunlap-Lawfare-101/

Esper, M. (2020, June 2). Secretary of Defense Memorandum, Subject: *Message to the Department—Support to Civil Authorities*.

Flournoy, M. & Chefitz, G. (2020, April 1). Breaking the logjam: How the Pentagon can build trust with Congress. *Defense News*. Retrieved from https://www.defensenews.com/opinion/commentary/2020/04/01/breaking-the-logjam-how-the-pentagon-can-build-trust-with-congress/

Flynn, C. & Richardson, J. (2013, July-August). Joint operational access and the global response force: Redefining readiness. *Military Review,* 38-44. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20130831_art009.pdf

FM 3-12

Cyberspace and Electronic Warfare Operations

FM 3-13
Information Operations

FM 3-13.4
Army Support to Military Deception

FM 3-14
Army Space Operations

FM 3-16
The Army in Multinational Operations

FM 3-52
Airspace Control

FM 3-55
Information Collection

FM 3-57
Civil Affairs Operations

FM 3-61
Public Affairs Operations

FM 6-0
Commander and Staff Organization and Operations

FM 6-02
Signal Support to Operations

FM 6-22
Leader Development

FM 7-0
Train to Win in a Complex World

Freedberg, S. (2021, March 17). Army's new aim is decision dominance. *Breaking Defense*. Retrieved from https://breakingdefense.com/2021/03/armys-new-aim-is-decision-dominance/

Freedberg, S. (2021, March 30). Army won't repeat mistakes of FCS: Gen. Murray exclusive. Breaking Defense. Retrieved from https://breakingdefense.com/2021/03/army-wont-repeat-mistakes-of-fcs-gen-murray-exclusive/

Freedberg, S. (2020, March 13). 'No timeout' in future wars: Army Gen. Murray exclusive. *Breaking Defense*. Retrieved from https://breakingdefense.com/2020/03/no-timeout-in-future-wars-army-gen-murray-exclusive/

Freedberg, S. (2020, May 18). Project convergence: Linking Army missile defense, offense, & space. *Breaking Defense*. Retrieved from https://breakingdefense.com/2020/05/project-convergence-linking-army-missile-defense-offense-space/

Friedman, B. & Garard, A. (2020, April 7). Clarifying command: Keeping up with the (John Paul) Joneses. *War On the Rocks*. Retrieved from https://warontherocks.com/2020/04/clarifying-command-keeping-up-with-the-john-paul-joneses/

Garamone, J. (2015, September 22). Dempsey talks caution, whole-of-government approach. *DoD News*. Retrieved from http://www.defense.gov/News-Article-View/Article/618120/dempsey-talks-caution-whole-of-government-approach

Goldfein, D. & Raymond, J. (2020, February 27). America's future battle network is key to multidomain defense. *Defense News*. Retrieved from https://www.defensenews.com/opinion/commentary/2020/02/27/americas-future-battle-network-is-key-to-multidomain-defense/

Grigsby, W., et al. (2013, November-December). Mission command in the regionally aligned division headquarters. *Military Review,* 3-9. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20131231_art004.pdf

Guthrie, T. (2012, June). Mission command: Do we have the stomach for what is really required? *Army Magazine, 62(6)*, 26-28.

Herr, T., et al. (2020, December). *How Do You Fix a Flying Computer? Seeking Resilience in Software-Intensive Mission Systems*. Atlantic Council. Washington, DC. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2020/12/Seeking-Mission-Resilience.pdf

Higginbottom, M., & Adkison, R. (2012, July). At the tip of the spear: Mission command on the move in a networked force. *Army Magazine, 62(7)*, 32-36.

Hitchens, T. (2020, October 27). Data sharing hurdles stymie JADC2: CSAF Brown. Breaking Defense. Retrieved from https://breakingdefense.com/2020/10/data-sharing-hurdles-stymie-jadc2-csaf-brown/

Ibarra, H. & Scoular, A. (2020, November-December). The leader as coach. *Harvard Business Review*. Retrieved from https://hbr.org/2019/11/the-leader-as-coach

Johnson, D., et al. (2019). *The U.S. Army and the Battle of Baghdad: Lessons Learned—And Still to be Learned*. Rand Corporation. Santa Monica, CA. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3076/RAND_RR3076.pdf

Joint Concept for Integrated Campaigning

Joint Operating Environment 2040

Joint Operational Access Concept

Joint Warfighting Concept

JP 3-0
Joint Operations

JP 3-14
Space Operations

JP 3-33
Joint Task Force Headquarters

JP 3-52
Joint Airspace Control

JP 3-85
Joint Electromagnetic Spectrum Operations

Kay, L. (2016, July 27). Managing the Gray Zone is a gray matter challenge. *Small Wars Journal*. Retrieved from http://smallwarsjournal.com/jrnl/art/managing-the-gray-zone-is-a-gray-matter-challenge.

Kott, A. & Delano, K. (2020, November). Cyber resiliency through the lens of COVID-19. *Army Magazine, 70 (11)*, 46-49.

Lilley, K. (2016, February 16). Warrant officer forecast: What's in store for the Army's technical experts. *Army Times*. Retrieved from http://www.armytimes.com/story/military/2016/02/21/warrant-officer-forecast-whats-store-armys-technical-experts/80056360/

MacFarland, S. (2020, March). Joint operations need a guiding hand. *Army Magazine, 70(3)*, 8-12.

Machak, J. (2015, June). Better exit interviews: Opportunities for organizational improvement. *Army Magazine, 65(6)*, 56-57.

Matthews, W. (2015, April). Supersoldiers: Can science and technology deliver better performance? *Army Magazine, 65(5)*, 40-44.

McConville, J. (2021, March 16). *Army Multi-Domain Transformation: Ready to Win in Competition and Conflict, Chief of Staff Paper #1*. Retrieved from https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf

McConville, J. (2021, March 1). *The Army in Military Competition, Chief of Staff Paper #2*. Retrieved from https://api.army.mil/e2/c/downloads/2021/03/29/bf6c30e6/csa-paper-2-the-army-in-military-competition.pdf

McConville, J. & McCarthy, R. (2020, April 10). DA Memorandum: *Mandatory Implementation of Army Data Services Requirements*. Retrieved from https://armypubs.army.mil/publications/administrative/pog/CPOG.aspx

McConville, J. & McCarthy, R. (2020). *Project Convergence*. Retrieved from https://www.milsuite.mil/book/docs/DOC-871428

McMaster, H. (2003, April 7). *Crack in the Foundation: Defense Transformation and Underlying Assumption of Dominant Knowledge in Future War*. U.S. Army War College Strategy Research Project. Carlisle Barracks, PA.

McMaster, H. (2016, March 31). Lieutenant General Don Holder's free, non-binding advice for battalion and squadron commanders. *The Strategy Bridge*. Retrieved from http://www.thestrategybridge.com/the-bridge/2016/3/31/leadership-through-example

Michelson, B. (2013, September-October). Character development of U.S. Army leaders: The laissez-faire approach. *Military Review,* 30-39. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20131031_art007.pdf

Mikkelsen, K. & Jarche, H. (2015, October 16). The best leaders are constant learners. *Harvard Business Review*. Retrieved from https://hbr.org/2015/10/the-best-leaders-are-constant-learners.

Milley, M., et al. (2020, May 01). *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education & Talent Management*. Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs_pme_tm_vision.pdf?ver=2020-05-15-102429-817

Milley, M. (2015, October). Winning matters: Especially in a complex world. *Army Magazine, 65(10)*, 21-26.

Miller, C. (2020, November 16). [Memorandum]. *Message to the Department—Acting Secretary Miller's Goals*. Retrieved from https://media.defense.gov/2020/Nov/16/2002536467/-1/-1/0/MESSAGE_TO_THE_DEPARTMENT_ACTING_SECRETARY_MILLERS%20GOALS_OSD010972_20_FOD_FINAL.PDF

Mission Command Center of Excellence, Army Capabilities Manager for Mission Command and Command Posts. (2019, September 27). *The Army Mission Partner Environment Concept of Operations*. Fort Leavenworth, KS. Available upon request through the proponent.

Murphy, P. & Milley, M. (2016, April 7). [Record Version]. Statement by the Honorable Patrick J. Murphy, Acting Secretary of the Army and General Mark A. Milley, Chief of Staff United States Army before the Committee on Armed Services United States Senate. Washington, DC.

National Security Agency Committee on National Security Systems. (2015, April 6). *Committee on National Security Systems Instruction (CNSSI) No. 4009: Committee on National Security Systems (CNSS) Glossary*. Fort Meade, MD. Retrieved from https://www.cnss.gov/CNSS/openDoc.cfm?u5zjeVOXbaR2OX/FD6uW/w==.

Perkins, D. (2012, June). Mission command: Reflections from the Combined Arms Center commander. *Army Magazine, 62(6)*, 30-34.

Pomerleau, M. (2020, November 21). Is the Pentagon's 'fragile' network ready to handle a slew of connected weapon systems? *C4ISRNET*. Retrieved from https://www.c4isrnet.com/it-networks/2020/11/20/is-the-pentagons-fragile-network-ready-to-handle-a-slew-of-connected-weapon-systems/

Pomerleau, M. (2019, September 5). The Army wants more coders alongside operators. *Fifth Domain*. Retrieved from https://www.fifthdomain.com/dod/army/2019/09/05/the-army-wants-more-coders-alongside-operators/

Powell, C. (2018, April 23). Memory-boosting brain implants are in the works, Would you get one? *NBC MACH*. Retrieved from https://www.nbcnews.com/mach/science/memory-boosting-brain-implants-are-works-would-you-get-one-ncna868476

Pryer, D. (2013, November-December). Growing leaders who practice mission command and win the peace. *Military Review,* 31-41. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20131231_art008.pdf

Reinforcement Learning (RL). (2020, January 30). *Techopedia*. Retrieved from https://www.techopedia.com/definition/32055/reinforcement-learning-rl

Rother, M. & Rosenthal, M. (2018, Summer). An approach to becoming agile in a dynamic world: Helping employees develop scientific thinking empowers them to solve problems and make decisions. *Target*. Retrieved from https://www.ame.org/approach-becoming-agile-dynamic-world

Ryan, M. (2013, July-September). A short note on PACE plans. *Infantry Magazine*. Retrieved from https://www.benning.army.mil/infantry/magazine/issues/2013/Jul-Sep/pdfs/Ryan.pdf

Schare, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. New York, NY: W. W. Norton & Company.

Schmidt, T. (2020, November). Developing officers with a higher degree of brain power. *Army Magazine, 70 (11)*, 7-10.

Schmidt, T. (2020, June). Playing head games is more crucial than ever. *Army Magazine, 70 (6)*, 14-16.

Shackelford, S. (2020, March 21). The battle against disinformation is global. *Fifth Domain*. Retrieved from https://www.fifthdomain.com/international/2020/03/20/the-battle-against-disinformation-is-global/

Shafley, B. (2020, May 13). Put the commander back in commander's intent. *Center for International Maritime Security*. Retrieved from http://cimsec.org/put-the-commander-back-in-commanders-intent/43587

Shaw, S. (2013, October-December). Rally point for leaders: Building an organization's mission command culture. *Infantry, 102(4)*, 20-25.

Sheets, C. (2020, April 10). Is it Time for an Operations MOS? *NCO Journal*. Retrieved from https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2020/April/Operations-MOS/

Storlie, C. (2020, March). Apply artificial intelligence to improve combat training. *Army Magazine, 70(3)*, 14-16.

Storr, J. (2003, Autumn). A command philosophy for the information age: The continuing relevance of mission command. *Defence Studies*, (3) 3, p. 119-129. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/14702430308405081

Sukman, D. & Davis, C. (2020, March-April). Divided we fall: How the U.S. force is losing its joint advantage over China and Russia. Military Review. Retrieved from https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2020/Sukman-Divided/

Tan, M. (2020, March). Under pressure: Overtasked commanders need time management help. *Army Magazine, 70(3)*, 42-44.

Thorpe, J., Girling, K., & Auger, A. (2017, July 13). Maintaining military dominance in the future operating environment: A case for emerging human enhancement technologies that contribute to soldier resilience. *Small Wars Journal*. Retrieved from http://smallwarsjournal.com/jrnl/art/ maintaining-military-dominance-in-the-future-operating-environment-a-case-for-emerging-huma

Trevithick, J. (2020, May 11). This is what ground forces look like to an electronic warfare system and why it's a big deal. *The Drive*. Retrieved from https://www.thedrive.com/the-war-zone/33401/this-is-what-ground-forces-look-like-to-an-electronic-warfare-system-and-why-its-a-big-deal

Tunnell, H. (2020, July-August). Tactical data science. *Military Review*. Retrieved from https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2020/Tunnell-Tactical-Data-Science/

U.S. Army Combined Arms Center (CAC) and ARCIC. (2015, October 1). *The Mission Command Network: Vision & Narrative*. Fort Leavenworth, Kansas. Available upon request through the proponent.

U.S. Army CAC. (2015, September). *Talent Management Concept of Operations for Force 2025 and Beyond*. Fort Leavenworth, KS. Available upon request through the proponent.

U.S. Army FCC and CCDC. (2020, January 9). *Discovery Enabler Concept of Operations—Artificial Intelligence: Reinforcement Learning to Enable Decision Overmatch*. Fort Eustis, VA. Available upon request through the proponent.

Vergun, D. (2016, January 19). Solarium: Warrants need training, Army over-relies on contractors. *Army.mil*. Retrieved from http://www.army.mil/article/161079/Solarium__Warrants_need_training__Army_over_relies_on_contractors/

von Clausewitz, C. (1975). *On war*. (Ed. and trans. Michael Howard and Peter Paret). NJ: Princeton University Press.

Votel, J. (2020, June 8), An apolitical military is essential to maintaining balance among American institutions. *Air Force Times*. Retrieved from https://www.airforcetimes.com/opinion/commentary/2020/06/08/an-apolitical-military-is-essential-to-maintaining-balance-among-american-institutions/

Wallace, W. (2013, November). Another training revolution coming. *Army Magazine, 63(11)*, 39-43.

Wallace, W. (2020, April). Multi-domain operations in context. *The Landpower Essay Series*, (20-4). Arlington, VA: Association of the United States Army. Retrieved from https://www.ausa.org/sites/default/files/publications/LPE-20-4-Multi-Domain-Operations-in-Context.pdf

Wass de Czege, H. (2012, May-June). Difficult missions: What logic to apply and what action to take. *Military Review,* 55-60. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20120630_art010.pdf

Wesley, E. & Simpson, R. (2020, April). Expanding the battlefield: An important fundamental of multi-domain operations. *Land Warfare Paper*, (131). Arlington, VA: Association of the United States Army. Retrieved from https://www.ausa.org/sites/default/files/publications/LWP-131-Expanding-the-Battlefield-An-Important-Fundamental-of-Multi-Domain-Operations.pdf

White House (The). (2017, December). *National Security Strategy of the United States of America*. Washington, DC: The White House. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Whitford, A. (2015, May-June). The path to Mission Command. *Military Review,* 40-47. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20150630_art011.pdf

Woods, K. & Greenwood, T. (2018, 1st Quarter). Multidomain battle: Time for a campaign of joint experimentation. *Joint Force Quarterly*, 88, pp. 14-21.

Work, B. & Selva, P. (2015, December 8). Revitalizing wargaming is necessary to be prepared for future wars. *War on the Rocks*. Retrieved from http://warontherocks.com/2015/12/revitalizing-wargaming-is-necessary-to-be-prepared-for-future-wars/

Work, R. & Dougherty, T. (2020, October 6). It's time for the Pentagon to take data principles more seriously. *War on the Rocks*. Retrieved from https://warontherocks.com/2020/10/its-time-for-the-pentagon-to-take-data-principles-more-seriously/?fbclid=IwAR2x6g-2Xd9ISOyxfhXIoYTI8BZxkXZjjLsylBQkBWstOb2foJPguhnA4EU

Zweibelson, B. (2016, January 12). US, allies must 'stop fixating' on ISIL & friends; 'frankly, we are losing.' *Breaking Defense*. Retrieved from http://breakingdefense.com/2016/01/us-allies-must-stop-fixating-on-isil-frankly-we-are-losing/

Appendix B
Required Capabilities

B-1. Introduction
The AFCC-C2 RCs are based on the broad ideas and the RCs from MDO and EAB concepts, proponent analytical work, lessons learned from almost two decades of conflict, and the solutions and supporting ideas found in chapter 3 and the supporting appendices of this pamphlet.

B-2. Required capability statements

a. Integrity of intent. The following capability statements are not stand-alone; they must be understood based upon this concept and not the reader's own interpretation. Each conceptual RC is followed by reference paragraphs from this concept and if applicable, the hierarchical MDO and EAB concepts. These references are termed integrity of intent and are included to help readers understand the context and intent of the RC, thereby reducing the likelihood of misinterpretation. The integrity of intent also assists in guiding and framing analysis during subsequent capability development.

b. RCs to achieve decision advantages and overall decision dominance. Developing, preparing, and equipping future Army leaders, Soldiers, Army Civilians, and organizations to apply the MC fundamental principles, integrate and converge combat power across all of the domains and with all elements of national power, achieve decision advantages, and develop overall decision dominance throughout the competition continuum requires the following capabilities.

(1) Future Army forces require the ability to identify, recruit, develop, assess, manage, and retain *competent leaders, Soldiers, and Army Civilians* grounded in Army professional ethics and tactical and technical proficiencies; skilled in applying fundamental Army leader competencies and the MC approach; and capable of organizing, employing, and adapting the C2 system for

success in all of the domains, as part of unified action, and across the competition continuum (AFCC-C2: 3-4.b, 3-4.c.(1), 3-5.b, 3-5.c, 3-5.e, 3-5.f, 3-5.g, 3-5.h.(1), 3-5.h.(3).(b), 3-5.i, 3-5.j, C-2, E-2.a, E-2.b, E-2.d, E-2.e, & F-2 and MDO: B-2.n).

(2) Future Army forces require the ability to rapidly form, deploy, and re-form *globally-integrated, networked, and interoperable teams of Army forces and unified action partners* that are responsive to combatant and subordinate commanders' operational needs throughout competition, crisis response, and armed conflict (AFCC-C2: 3-4.b, 3-4.c.(2), 3-4.e.(2), 3-5.g, C-2, E-2.d, & F-3; MDO: B-2.b, B-2.i, 3-5.e, 3-5.h.(1), & 3-5.j; and EAB: B-2.c & B-2.d).

(3) Future Army forces require an appropriate level of understanding of all Services' domain capabilities, limitations, vulnerabilities, and interdependencies; the requisite authorities and permissions at echelon; and the ability to form and lead teams able to *expertly plan, prepare for, execute, monitor, and assess operations and converge Army, joint, multinational, and interorganizational capabilities with other elements of national power* to create unity of effort in all of the domains, as part of unified action, and across the competition continuum (AFCC-C2: 3-4.b, 3-4.d.(1), 3-5.d, 3-5.e, 3-5.f, 3-5.g, 3-5.h.(2), 3-5.h.(3).(b), 3-5.i, 3-5.j, C-3, & G-2; MDO: B-2.f, B-2.g, & B-2.i.; and EAB: B-2.f).

(4) Future Army forces require the ability to *understand and support U.S. Government agency led efforts* to enhance another nation's governance, economic development, essential services, rule of law, and other critical governmental functions with the aim of resolving or mitigating factors of instability, producing sustainable outcomes, creating favorable conditions for long-term deterrence, and overall, protecting national interests in all of the domains, as part of unified action, and across the competition continuum (AFCC-C2: 3-4.b, 3-4.d.(2), 3-5.e, 3-5.h.(1), 3-5.h.(2), 3-5.i, 3-5.j, C-3, G-3, & J-4.b and MDO: B-2.b, B-2.d, & B-2.l).

(5) Future Army forces require the ability to skillfully *manage knowledge, information, and data* from all of the domains to create shared understanding, accelerate learning, facilitate collaboration, enable rapid decision making, and build learning organizations, as part of unified action, and across the competition continuum (AFCC-C2: 3-4.b, 3-4.d.(3), 3-5.e, 3-5.g, 3-5.h.(2), 3-5.h.(3).(b), 3-5.j, C-3, & G-4; MDO: B-2.h & B-2.i; and EAB: B-2.d).

(6) Future Army forces require the ability to dynamically *manage Army and unified action partner use of assigned airspace* to enable cross-domain maneuver, lethal and nonlethal all-domain fires, aerial supply and distribution, and timely multi-domain convergence; optimize the employment of all aerial capabilities while preventing fratricide; and allow greatest flexibility in achieving the commander's intent, priorities, and risk guidance, as part of unified action, and across the competition continuum (AFCC-C2: 3-4.b, 3-4.d.(4), 3-5.e, 3-5.f, 3-5.g, 3-5.h.(2), 3-5.h.(3).(b), 3-5.j, C-3, & G-5; MDO: B-2.m; and EAB: B-2.k).

(7) Future Army forces require a *communications network* that facilitates human, procedural, and technical interoperability and collaboration across all of the domains and warfighting functions; enables execution of the operations process and the timely convergence of all joint, multinational, and interorganizational capabilities; supports force projection and expeditionary movement, the global and local dispersion and decentralization of forces, and uninterrupted

sustainment; provides for agile command and control at all echelons for the conduct of cross-domain maneuver and the integration of lethal and nonlethal all-domain fires; and allows for the continuity of command, as part of unified action, and across the competition continuum (AFCC-C2: 3-4.b, 3-4.e.(1), 3-5.e, 3-5.g, 3-5.h.(3), 3-5.j, C-4, E-2.c, & H-2; MDO: B-2.e; and EAB: B-2.d).

(8) Future Army forces require *common, standardized, shareable, and secure data* to enable interoperability, make better and faster decisions, support human-machine teaming, and seamlessly link any sensor to the right command nodes and the best shooters, as part of unified action, and across the competition continuum (AFCC-C2: 3-4.b, 3-4.e.(2), 3-5.e 3-5.f, 3-5.g, 3-5.h.(3).(a), 3-5.h.(3).(b), 3-5.j, C-4, E-2.c, & H-3; MDO: B-2.e; and EAB: B-2.d).

(9) Future Army forces require an all-domain-capable, *tailorable battlespace visualization capability* for continuous shared situational understanding as part of unified action and across the competition continuum (AFCC-C2: 3-4.b, 3-4.e.(3), 3-4.h, 3-5.e, 3-5.g, 3-5.h.(3), 3-5.j, C-4, E-2.a, E-2.c, & H-4; MDO: B-2.i; and EAB: B-2.b & B-2.d).

(10) Future Army forces require the ability to enable commanders and their staffs to *disperse into multiple, meshed command nodes from home station to the close area* and from which they can understand, visualize, describe, direct, lead, monitor, assess, and continuously adapt to the operational environment as part of unified action and across the competition continuum (AFCC-C2: 3-4.b, 3-4.f, 3-5.e, 3-5.f, 3-5.g, 3-5.h.(3).(b), 3-5.h.(4), 3-5.j, C-5, & I-2 and MDO: B-2.i & B-2.k).

Appendix C
Science and Technology in Support of the C2 System

C-1. Introduction

a. This appendix describes a broad set of science and technology (S&T) opportunities with the potential to improve the future Army C2 system. It is an unclassified statement of potential S&T enablers and the operational context in which they will be employed. The enablers are aligned with the capabilities the Army must possess to achieve the speed and agility required for successful C2 in future MDO. Based on this concept's central idea, this appendix is organized around the main components of the C2 system: people, processes, the communications network, and the CPC. This appendix is not a final statement of C2 needs and requirements. Government, commercial, and academic researchers and developers and other Services must work in partnership with Army capability developers to select and develop capabilities which will result in better and faster decisions than adversaries. Each major section below includes an area for inclusion of current, planned, and closely-related research activities.

b. In the past, TRADOC annually provided a description of warfighter S&T needs to the U.S. Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) as a means to focus Army S&T efforts to achieve future capability needs. With the recent creation of the AFC, that process shifted to the Army centers of excellence (CoEs)—a decentralized effort to

inform capability development efforts. Accordingly, the MCCoE continues to explore relevant C2 technologies in close cooperation with its ASA(ALT) partners. The focus of S&T efforts for over the past three years has been AI and other efforts that support the realization of an AI-enhanced force. The emphasis on AI techniques and applications will continue into the foreseeable future and is included in this appendix where appropriate.

c. C2 capabilities described in this appendix align with the Army's MDO and EAB concepts and support Army contributions to future joint capability development efforts. MDO will place high demands on the Army's ability to sense, understand, decide on, and strike targets from the close area to the strategic deep fires area from, in, and across all of the domains.[142]

d. This appendix identifies key technologies and emerging scientific research areas with greatest promise for transforming the Army's C2 system. The future all-domain-capable C2 system must, where appropriate, replace time-consuming human processes with machine-speed data-to-information processing that quickly and effortlessly provide leaders and Soldiers with comprehensive situational awareness and understanding across organizations and with unified action partners. A new generation of S&T will enable leaders and Soldiers to C2 in increasingly powerful ways over the next 20 years. Automation, effortless user interfaces, augmented reality, immersive virtual environments, and reliable connectivity based on heterogeneous technologies supporting a unified communications network will transform, in unimaginable ways, the art and science of C2 for the next generation of Army leaders and Soldiers.

C-2. People within the C2 system

a. The most important component of the C2 system is people—commanders and those who assist them and exercise control on their behalf. An effective C2 system accounts for the human physical and cognitive requirements and limitations. Simultaneously, it exploits and enhances uniquely human skills. People dedicated to the C2 system include commanders, seconds-in-command, command sergeants major, staffs, liaison officers, and network and cyberspace operators among others.[143] This appendix focuses on those enhancements that directly impact people's ability to perform their C2 tasks as part of the C2 system. It focuses on those S&T technologies to support the human application of judgment to transform data and information from sensors and information systems to knowledge and understanding. Human enhancements with a goal of improving the acquisition of knowledge take many forms, but all are targeted at improving cognitive performance. All discussions of S&T to support the C2 system's people fall under the umbrella term of human enhancements.

b. *Technology in support of people*. Human enhancement is defined as any kind of genetic, biomedical, or pharmaceutical intervention aimed at improving human dispositions, capacities, or well-being, even if there is no pathology to be treated. This topic is fraught with ethical, cultural, and practical considerations and this appendix acknowledges, but does not address, those concerns except to say that now is the time for the Army to begin considering the implications of exploring this science.[144] Our culture already acknowledges that several forms of enhancements already occur. Common examples include elective plastic surgery, blood doping and performance-enhancing drugs, various dietary supplements, and fertility treatments. New discoveries in this area will eventually find military application. For the purpose of focusing the discussion, this

appendix only addresses those S&T capabilities in support of human enhancement that are directed at improving cognitive performance. These include both machine interfaces and new methods of providing relevant information to humans, and the cognitive enhancements designed to improve knowledge acquisition.

(1) Cognitive enhancements. Cognitive enhancements are interventions that aim to improve mental functioning. Most cognitive enhancement strategies can be considered to work as either biochemical, physical, or behavioral interventions. The need to maintain Soldier cognitive performance over long deployments, combined with periods of 24-hour operations is well documented. The complexity of the future complex, highly-competitive, and hyperactive physical and non-physical OE will require even greater cognitive performance from Soldiers.

(2) Biochemical enhancements. Having the ability to maintain cognitive acuity, regardless of the time on the current shift or deployment, is paramount to success in the future OE. The Army has always offered coffee to Soldiers, knowing that caffeine helps improve cognitive performance. Other enhancers familiar to most people are glucose and nicotine. There are other, perhaps more notorious, performance enhancers including Benzedrine and methamphetamine that have been used in previous wars. This concept does not advocate for providing Soldiers with chemical compounds not approved by the Food and Drug Administration. However, the Army will do well to carefully monitor the ongoing public debate and research on the use of synthetic stimulants such as Adderall, Ritalin, Modafinil, and similar compounds used as cognitive enhancers.[145]

(3) Physical enhancements. This category of cognitive enhancements includes human genetic engineering and other technological advances that require biophysical augmentation. This research has the potential to impact the Army C2 system through improved Soldier abilities.[146]

(a) The Defense Advanced Research Projects Agency is working on neural implants to help with traumatic brain injuries in Soldiers. However, the same technology offers the potential to boost memory and cognitive performance, control complex machines, and accelerate learning in healthy Soldiers. By the end of 2021, industry is projected to have technologies to implant in human subjects. For example, Paradromics, a San Jose-based startup, plans to sell a "cortical modem," an implant capable of reading brain states and stimulus signals at a rate of 1 gigabyte of data per second.[147] Obviously, a technology like this has direct application to enhancing Soldier performance, particularly within those specialties requiring multi-tasking and memory associated with managing large amounts of data.

(b) Augmented reality and virtual reality systems offer a less invasive way to provide enhancements to physical capability.
- *Augmented reality.* Augmented reality systems overlay computer-generated information and images on a real-world background to create an augmented view of the world around a person. Near-future Soldiers equipped with augmented reality glasses could receive messages, detailed routes to a destination, exact locations of friendly personnel, and precise distance and direction information for anticipated or reported enemy locations through an effortless hands-free visual interface.[148]
- *Virtual reality.* Virtual reality systems create a completely simulated environment through the use of headsets that typically occlude the real-world around a person to allow them to

experience a virtual, 3-dimensional world. These kinds of systems are currently being used as immersive training environments for small unit actions and tactics. As resolution improves and headset weight is reduced, virtual reality headsets could replace traditional monitors throughout the CPC and subordinate command nodes. This capability would allow the staff to view a tailorable battlespace visualization, develop knowledge products, attend briefings and meetings, collaborate, and communicate in a virtual environment from home station to the close area.

C-3. C2 processes

a. This section focuses on S&T that will improve C2 processes and procedures. Commanders and their staffs establish and use processes and procedures to organize activities within their headquarters and throughout the force. A process is a series of actions or steps taken to achieve a specific end. One example is the overarching operations process, but there are many other processes, procedures, and activities used at all levels of the Army. Two interrelated activities important to decision making are knowledge management and information management. These two activities assist commanders with progressively adding meaning at each level of processing and analyzing to help build and maintain their situational understanding. There are four levels of meaning. From the lowest level to the highest level, they include data, information, knowledge, and understanding. At the lowest level, human processing transforms data into information. Human analysis then refines information into knowledge. Commanders and staffs then apply judgment to transform knowledge into understanding. (See figure C-1.)
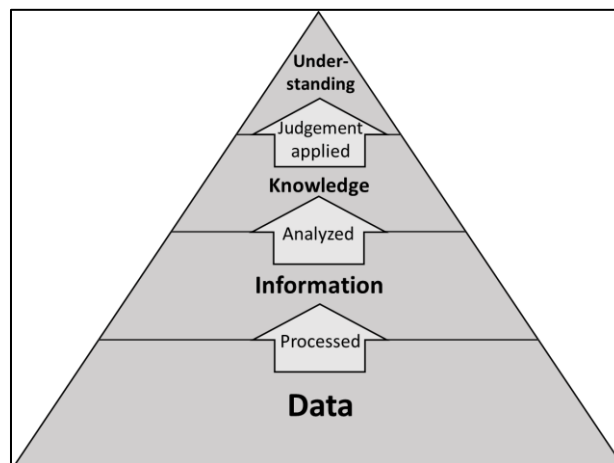
Figure C-1. Creating understanding

b. *Technology supporting C2 processes*. To achieve understanding with the speed and accuracy required in the future OE, Army information, information-management, and battle-management systems must have the ability to automate routine procedures and processes and rapidly transform data into information. This human-machine teaming allows humans to focus on developing the knowledge products necessary to achieve and share a clear understanding of the situation and make better and faster decisions. The following are some specific areas for further research to support C2 processes:

(1) Documents simultaneously written for humans and machines. Human-machine teaming enables the creation of hybrid organizations composed of humans and autonomous vehicles.

Humans and machines must act in concert with each other to achieve mission objectives. The current force produces plans, orders, graphic control measures, and other products in human-readable format. To fully integrate human and autonomous machines, the future Army force requires the means to produce orders, graphic control measures, rules of engagement, and other guidance in a format that is both machine and human readable. The serial productions of these documents, first as human readable, then as machine readable will be too slow and introduce errors through the translation process.

(2) AI-enabled information routing and sharing tools. Effective information sharing throughout the operations process introduces an efficient flow of correct, timely data and information. Shared data and information enables commanders, staffs, and subordinates across all warfighting functions to understand the situation and communicate timely decisions to the force. AI-enabled C2 information systems can display a wide variety of data and identify patterns, anomalies, and relevant information. These AI-enabled C2 information systems can enable staff and unified action partners to share information throughout the entire operations process. AI-enabled information, information-management, and battle-management systems can facilitate efficient routing of information across staffs, echelons, and unified action partners and display information for better shared understanding across the entire organization.

(3) AI-enabled planning and execution tools. To realize many of the capabilities described in this concept, the Army must leverage AI techniques like reinforcement learning.[149] This science offers the possibility of understanding and visualizing the hyperactive nature, complexity, and scale of future MDO so well as to achieve cognitive overmatch against near-peer adversaries. Reinforcement learning has the potential to enable the adaptive planning and rapid decision making necessary to achieve the operational initiative necessary to succeed in the future OE. Possibilities include the following:

(a) Create and exploit potential windows of superiority during deliberate planning. Reinforcement learning facilitates deliberate planning to enable the timely integration, dynamic synchronization, and optimal convergence of effects from, in, and across all of the domains and the creation and exploitation of windows of superiority. An AI-enabled decision-support tool with reinforcement learning as the backbone, incorporated in deliberate operational planning, has the potential to offer new and novel courses of action for commanders and their staffs to consider. Reinforcement learning can develop and propose plans that present as much ambiguity as possible to enable threat deception. Simultaneously, it can provide commanders and staffs with a means to identify and understand risks associated with proposed courses of action.

(b) Continually sense, identify, and quickly exploit emerging windows of superiority. During operations, windows of superiority will emerge throughout the battlespace at different echelons, but recognizing and exploiting them requires capabilities that rely less on deliberate planning cycles and more on continuous, integrated planning. Information, information-management, and battle-management systems enabled by reinforcement learning have the potential to perform rapid resource allocation of platforms and capabilities to exploit windows of superiority.

(c) Continually sense and identify emerging windows of friendly vulnerability. Threat forces will also seek opportunities to identify, create, and exploit friendly vulnerabilities. Reinforcement learning enables the Army and joint force to recognize and mitigate risks as operations unfold.

(d) Respond to individual user differences and drive customized knowledge management. Planning at EAB requires the collection and analysis of an overwhelming amount of information. Processes enabled by reinforcement learning that incorporate feedback and adaptation mechanisms reduce the time required for commanders and staffs to understand the operational environment while reducing cognitive burden.

(4) AI-enabled data analysis tools. The future OE will pose significant new challenges for the Army. Competition with our adversaries, especially in the non-physical battlespace will require the Army to interact with new kinds of data and data sources. Collection of this data is the responsibility of agencies other than the Army. However, in order to understand the adversary's malign attempts to destabilize allies and partners or create and exploit ambiguities in international law and social and cultural unrest, these data sets must be available to the Army and the joint force.

(a) A Defense Intelligence Agency program called Machine-Assisted Analytical Rapid-Repository System (MARS) is an example of current technology that can make existing databases a part of a more flexible data environment.[150] The data could then be available to inform a whole-of-government approach to evolving strategic and operational challenges. For the Army, the information would support operational design and contingency planning processes and products. According to national and international laws and partnership agreements, potential data sets include:
- International, national, corporate, and individual financial transaction information.
- International social media use, trends, behaviors, and preferences.
- International, national, state, and local criminal activity patterns and police records.
- International industrial purchase information.
- Regional and local electromagnetic spectrum-use baselines.

(b) The data requirements for developing comprehensive all-domain situational understanding across the entire competition continuum places a high value on developing AI tools and techniques to streamline the processes of identifying the best sources of data for ingestion and analysis. The Army will require AI tools and techniques to find and analyze data in whatever location and format that data is in. Hybrid teams of humans and AI working together to analyze problems and apply large, complex data sets could develop imaginative and effective tactical and strategic courses of action inconceivable by machines or humans alone.

C-4. The communications network

a. The communications network is critical to successful MDO. The communications network enables commanders to transfer data and information and control forces. Commanders determine their information requirements and train their staffs and organizations on using the communications network to meet these requirements. These capabilities relieve staffs from handling routine data, and enable extensive information sharing, collaborative planning, execution, monitoring, and assessment that promote shared understanding and disciplined initiative.

(1) The communications network encompasses all Army communications capabilities and associated procedures for collecting, processing, storing, displaying, disseminating, and managing information. It is the totality of enterprise and subordinate tactical networks operating seamlessly as a unified whole. It consists of multi-path network transport; information, information-management, and battle-management systems; warfighting and business applications; network services; sensors and other network points of presence; and data. The communications network supports Soldiers through the end-user applications and information services to enable the transformation of data and information into knowledge and understanding.

(2) This appendix elicits the S&T research areas that can improve the information systems that enable the execution of C2 functions and tasks. The C2 warfighting function enables the timely integration, dynamic synchronization, and optimal convergence of the various warfighting functions and domain capabilities by maintaining awareness and understanding of the specific situation and overall OE. Executing future MDO will significantly increase the complexities and risks to C2. To meet Army requirements for future MDO, the future all-domain-capable C2 system requires near-term development of smart capabilities, applications, and information, information-management, and battle-management systems. S&T activities to support future Army C2 system requirements must operate within an integrated smart ecosystem as part of joint all-domain C2, whether competing against near-peer adversaries or converging capabilities in support of armed conflict. There are a number of network S&T areas that warrant further research.

b. *Technology in support of the communications network.*

(1) Fit-for-purpose cloud. This architecture strategy optimizes connectivity and data transfer by aligning IT infrastructure proportionally with the relative importance of the business line, product, or service that it supports. Critical units receive greater infrastructure resources and higher service levels.

(2) Blockchain. Blockchain technology offers a decentralized, transparent, and immutable ledger option to secure data. It verifies user access to the blockchain, providing a high level of traceability and trust in the data being accessed. Blockchain uses cryptography to secure the data ledgers preventing data alteration and it eliminates a central point to attack the system creating a big advantage for use with AI, ML, and big data in the military.

(3) Hybrid cloud-computing stack. This technology could transform the battlespace by providing instantaneous access to secure cloud technology during large-scale combat. Future warfighters engaged in MDO could have widespread, cross-platform, and secure access to mobile devices to view a tailorable battlespace visualization creating more accurate shared situational understanding in real time.

(4) Internet-of-battlespace-things. The internet-of-battlespace-things is a system of interrelated computing devices, mechanical and digital machines, and objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. This allows personnel to leverage battlespace data

quickly to identify available manned and unmanned systems and deploy them to desired locations within the battlespace.

(5) Human-machine interface improvements. The varied nature of commander and staff interactions with information systems is important to consider. They must have access to decision-quality information whether stationary or moving on foot or in a ground, air, or waterborne C2 platform. The human-machine interface requirements for each C2 platform could be different. The Army requires broad research and development in hardware, power, and the applications to drive the hardware. However, human-machine interface is as much about process as it is design.

(a) The following future operational requirements demand a transformation in human-machine interfaces:

- *Multi-tasking*. With a decrease in the number of warfighters, yet an increase in the number of weapons, sensors, and applications, the warfighters of the future will manage more systems concurrently. Future Army forces cannot afford a 1:1 correspondence of warfighter to each system.
- *Mission awareness*. Soldiers and leaders will be required to maintain a very high level of awareness of their environment as they focus on mission goals. Rapidly changing situations require that they attend to information applicable to more than one command echelon and multiple information systems and devices. Tailorable, easy-to-use user interfaces will simplify task switching and improve mission awareness.
- *Supervisory control of systems*. There will be an increasing reliance on computer systems to perform procedural functions to offload that burden from Soldiers. With increasing automation, the role of the Soldier changes from a data collector and analyzer to a decision maker working in cooperation with automation.

(b) Human-machine interfaces must support natural human interaction patterns. These human-modeled interactions enable humans to learn from the smart application and its underlying model for explaining AI-generated results, and the smart application to learn from humans if refinement or model re-training is required. AI-enabled analytics for decision making (for example, graph analytics, causation models, prediction analytics, and OE risk detection) require new information visualizations to achieve shared understanding of all of the domains.

(6) Interaction patterns for AI-enabled information systems. New user interface and interaction patterns are required for smart C2 applications to reduce training and cognitive burdens. The application user interface and interactions for AI-generated results, recommendations, and analytic results are still emerging and unfamiliar to operational users. Future Army C2 information, information-management, and battle-management systems require advanced user interfaces or interaction techniques that maximize effectiveness of human-machine interactions supporting C2 processes, decisions, and shared understanding.

(a) AI applications, the underlying models, and human-machine interfaces must enable explanations to users for results, recommendations, or anomalies detected. Research and development are needed for C2 applications to enable model transparency, explainable AI-generated results, and develop interaction patterns that enable users to correct or update the model when necessary.

(b) Conversational and behavioral user-interface capabilities could shift the burden of training machines supporting human teams from the human to the machine. Research and experimentation will determine if conversational user-interfaces, eye tracking, and other physiological cues can reduce the system training requirements for AI-enabled C2 information systems. These interfaces could revolutionize human-machine teaming by allowing C2 information systems to be trained in real time as Soldiers are simply performing their duties. This opportunistic sensing and training can make systems more adaptable and customizable to the needs and abilities of each Soldier.

c. *Science and research in support of the Army communication network.*

(1) Low-earth-orbit micro satellites and high-altitude systems. Persistent, meshed, and relatively inexpensive low-earth-orbit micro-satellites and unmanned high-altitude aerial systems can support the Army's future communications network. Their low cost and resistance to attack will add robustness to current space-based communications. These systems allow for a high launch cadence, which further strengthens their resilience and recoverability and may deter adversaries from physically attacking satellites. These systems can provide additional sensing capability. As an example, low-earth-orbit micro satellites and high-altitude systems have the capability to provide continuous 2D and 3D mapping and sensing of the Earth. Integrated into future C2 information systems, satellite- and high-altitude-supported 2D and 3D representations will enable enhanced planning, preparation, execution, monitoring, and assessment of operations.

(2) Extremely heterogeneous networking. The exceedingly complex and varied environments and requirements associated with the future Army communications network demand an extremely diverse set of communications technologies such that the unique characteristics of each technology can be leveraged as appropriate throughout the communications network to meet the particular challenges and missions being faced at any given time and location.[151] This requires the development of novel communications modalities (all spectral bands, line-of-sight and beyond-line-of-sight operation, beamforming, directional networking, relays, and networking protocols), along with the prerequisite foundational modeling and characterization needed to optimize the operation of those modalities. It also requires the ability (potentially employing AI) needed to autonomously and dynamically adapt the operation of the communications network to provide the functionality and capacity necessary to jointly support multiple simultaneous missions and operational environments across the communications network. Extremely heterogeneous networking enables the use of the communications technology that is best suited for a given mission and environment, while using AI for decentralized and autonomous network control that ensures the interoperability of the diverse component communications technologies.

(3) Semantically-adaptive network control. This technology enables operational assets to dynamically adapt analytic applications and network resources in response to and in anticipation of environmental dynamics and evolving mission requirements. Future operations will have access to highly agile analytics that autonomously adapt their deployment configuration and deployment across distributed platforms based on available situational understanding to promote robustness and resilience during MDO. Semantically-aware applications supporting tactical and strategic operations learn to anticipate and adjust to emerging requirements and tasks by leveraging

advanced learning techniques (for example, knowledge graph querying, semantically- and context-aware networking, multitask learning, and distributed AI).

C-5. The command post constellation

a. The CPC provides physical or virtual locations from which the other three components of the C2 system operate (people, processes, and the communications network). The command nodes that make up the CPC vary in size, complexity, and focus. Command nodes may comprise vehicles, containers, and tents, or be integrated into existing buildings. Commanders systematically arrange platforms, signal nodes, and support equipment in ways best suited for a particular OE. Command nodes are high-payoff targets for adversaries, particularly those possessing capabilities for advanced intelligence, surveillance, and reconnaissance, long-range fires, and offensive cyberspace and EW capabilities. A number of S&T research areas have the potential to improve C2 functions and protection.

b. *Technology in support of the CPC.* Ensuring the continuity and survivability of C2 functions and capabilities is obtained by balancing multiple materiel and non-materiel considerations to include fewer vehicles and personnel; hardening and protecting resources from enemy and weather effects (component information systems as well as supporting infrastructure); more effective camouflage and concealment; decreasing, obscuring, or otherwise managing the visual, thermal, radio frequency, acoustic, and seismic signatures; early detection and identification of threats; intentional capability duplication and diversification among command nodes; a robust multi-path network transport; the ability to displace rapidly; and deception, dispersion, command and communications node positioning, and other innovative employment tactics and techniques. Given the importance of command nodes, their protection and survivability are critical. The following are select research areas where the Army can realize necessary modernization of the future CPC:

(1) Energy. This includes power cells that improve energy density for dismounted or remote operations; ambient power generation sufficient to enable burst communications; and wireless power that supplies nearby user needs to reduce or eliminate the Soldier's physical burden.

(2) Camouflage. Other materials must enable forces to remain unseen or avoid detection from threat forces. Smart ink and paints will camouflage forces from all manner of detection, not just visual, and will prevent the enemy from effectively targeting command nodes and the people within.

(3) Protection.

(a) Armor. Future armor will include materials that provide greater protection with reduced weight for Soldiers and systems. These materials may be rigid, or have properties that enable them to redirect forces to reduce or eliminate harm to friendly forces. These could be applied to command nodes to make them more survivable after detection and targeting.

(b) Directed-energy weapons. Directed-energy weapons to defeat unmanned aircraft systems and indirect fire attacks on deployed command nodes and tactical units are necessary for the future.

This would enhance the overall survivability of the CPC as well as protect key communications nodes.

(c) Signature management. Future command nodes require a self-aware signature management capability to provide rapid feedback on EMS threat exposure and allow the rapid employment of tactical deception systems to confuse and confound an adversary's ability to target command nodes via the EMS.

(4) Position, navigation, and timing. The future battlespace will be highly contested within the EMS and alternatives to satellite-based position, navigation, and timing will be required to achieve operational overmatch in a congested, contested, and denied communications environment.

(5) Mobility. Future command nodes require the ability to frequently and rapidly displace in a manner of minutes to reduce vulnerability to indirect fires threats. Vehicle-mounted command node infrastructure with self-contained power and communications and the ability for the staff to conduct C2 processes on-the-move greatly increase the survivability of the future CPC.

c. *Science and research in support of the CPC*.

(1) Flexible antenna radio frequency energy harvesting. This research focuses on conversion of Wi-Fi, Bluetooth, and cellular signals into usable electrical energy using a small, thin piece of transparent material that can be wrapped around surfaces to absorb their signals. This capability is a flexible, always-on way to harvest energy from signals to power other information, information-management, and battle-management systems, significantly reducing the amount of fuel consumed to power devices and increasing resiliency of systems that rely upon power.[152]

(2) Optical wireless communication technology. Light fidelity (Li-Fi) is a subset of optical wireless communication technology that focuses on transmitting data at high speeds over the visible light, ultraviolet, and infrared spectrums. When this technology is used within a command node, it alleviates the need for the time-consuming task of running data lines. Since the light cannot pass through walls, it does not produce an easily detectable signature. Optical wireless communication technology can contribute to improving the mobility and survivability of future command nodes.[153]

C-6. Conclusion

This appendix provides a broad set of S&T relevant opportunities with the potential to improve the Army's future C2 system. These S&T opportunities are aligned with concept's conceptual solutions and analyzed in terms of the future C2 capabilities the Army must possess to achieve the speed and agility required to succeed in future MDO. The appendix is not a final statement of C2 needs and requirements. Government, commercial, and academic researchers and developers and our sister Services must work in partnership with Army capability developers to select and develop capabilities which will result in better and faster decisions than adversaries.

Appendix D
AFCC-C2 Dependencies on Other Concepts

D-1. Introduction
This appendix describes the required capabilities from other Army concepts that enable 1) dis-integrating enemy decision making systems, 2) achieving decision advantages, and 3) maintaining and protecting decision advantages to create overall decision dominance. The AFCC-C2 depends on the development of these capabilities to support the realization of the ideas contained within this concept.

D-2. C2 dependencies on other warfighting functional and supporting concepts

  a. *Dis-integrating enemy decision-making systems*.

    (1) Aviation. The AFCC-C2 depends on the aviation supporting concept for the capabilities needed for precision and area, scalable (nonlethal to lethal) fires against the anticipated target set during joint and combined air-ground operations to enable the dis-integration of enemy decision-making systems.

    (2) Cyberspace and electromagnetic warfare operations. The AFCC-C2 depends on the cyber and electromagnetic warfare supporting concept for the capability to synchronize and assess offensive cyberspace operations to attack enemy and adversary facilities, platforms, sensors, systems, networks, critical infrastructure, key resources, and information and enable the dis-integration of enemy decision-making systems.

    (3) Fires. The AFCC-C2 depends on the fires functional concept for the capability to employ multi-domain fires in a contested EMS environment, all of the domains, and the information environment to enable the dis-integration of enemy decision-making systems.

    (4) Maneuver.

    (a)   The AFCC-C2 depends on the maneuver functional concepts for the capability to deny adversary sensors across all of the domains and environments from the operational support area to the deep maneuver area and enable the dis-integration of enemy decision-making systems.

    (b)   The AFCC-C2 depends on the maneuver functional concepts for the capability to continuously converge lethal and nonlethal effects in all of the domains while conducting semi-independent maneuver in all environments and enable the dis-integration of enemy decision-making systems.

    (c)   The AFCC-C2 depends on the maneuver functional concepts for the capability to stimulate adversary systems, making the adversary susceptible to detection, exploitation, destruction, or neutralization and enable the dis-integration of enemy decision-making systems.

    (5) Space. The AFCC-C2 depends on the space supporting concept for offensive space control capabilities. Offensive space control consists of offensive operations conducted for space

negation. Negation provides the scalable ability to prosecute space systems or services. Future Army space forces operating in a complex operational environment require the ability to conduct operational preparation of the environment (to include adversary space and space enabled systems), as well as be able to conduct deception, disruption, denial, and degradation as part of dis-integrating enemy decision-making systems.

(6) Special operations. The AFCC-C2 depends on the special operations supporting concept for the capability of Army special operations forces to penetrate and dis-integrate critical standoff nodes such as C2 facilities, weapons launch and recovery sites, munition storage areas, transport capabilities, and lines of communication. The convergence of joint and Army conventional and special operations presents enemy commanders with multiple and compounding dilemmas that will delay, disrupt, or destroy their ability to counter joint force initiatives due to the dis-integration of enemy decision-making systems.

b. *Achieving decision advantages*.

(1) Aviation.

(a) The AFCC-C2 depends on the aviation supporting concept for the capabilities required to move personnel, equipment, and supplies by air. Future commanders require reliable aviation capabilities to transport friendly forces and associated equipment from land or sea bases, to austere or unprepared landing zones and forward points of need to rapidly place a force in a position of advantage, reposition forces in preparation for operations, resupply forces, support the movement of select individuals, or to evacuate the sick and wounded which enables achieving decision advantages.

(b) The AFCC-C2 depends on the aviation supporting concept for Army aviation to integrate C2 system capabilities essential for providing C2 on the move, battlefield circulation of leaders, and extending the range of communications network capabilities to enable achieving decision advantages.

(2) Cyberspace and electromagnetic warfare operations. The AFCC-C2 depends on the cyberspace and electromagnetic warfare operations supporting concept for the capabilities required for offensive and defensive cyberspace operations enabling achieving decision advantages.

(3) Intelligence.

(a) The AFCC-C2 depends on the intelligence functional concept for the capability to conduct information collection in all domains throughout the competition continuum to provide depth and redundancy to support commanders' situational understanding in all operational environments to enable the information advantages required for achieving decision advantages.

(b) The AFCC-C2 depends on the intelligence functional concept for the capability to sense deep into the battlefield across all of the domains to enable the information advantages required for achieving decision advantages.

(c) The AFCC-C2 depends on the intelligence functional concept for advanced analytic capabilities to solve advanced problems which will enable the information advantages required for achieving decision advantages.

(4) Fires. The AFCC-C2 depends on the fires functional concept for the capability to detect, classify, and track aerial targets at sufficient range to effectively identify threats in a timely manner to enable achieving decision advantages.

(5) Maneuver.

(a) The AFCC-C2 depends on the maneuver functional concepts for the capability to seize, retain, and exploit the initiative consistent with the commander's intent in all conditions to enable achieving decision advantages.

(b) The AFCC-C2 depends on the maneuver functional concepts for the capability to maneuver while monitoring, regulating, manipulating, and obscuring signatures across all of the domains while also denying the adversary's ability to sense and target friendly forces to enable achieving decision advantages.

(c) The AFCC-C2 depends on the maneuver functional concepts for the capability to develop and disseminate multi-domain situational understanding to satisfy information requirements at a tempo the adversary is unable to match to enable achieving decision advantages.

(d) The AFCC-C2 depends on the maneuver functional concepts for the capability for commanders to task-organize their formations with the flexibility required to conduct semi-independent maneuver at a tempo the adversary is unable to match which will enable achieving decision advantages.

(6) Space.

(a) The AFCC-C2 depends on the space supporting concept for space support operations capabilities. This includes the operational control of payloads and services for wideband satellite communications and the ability to provide sustained, responsive space capabilities to enable achieving decision advantages.

(b) The AFCC-C2 depends on the space supporting concept for the capability to access secure, assured, protected, dedicated, persistent, multi-band, inter-theater, and intra-theater beyond-line-of-sight communications to enable achieving decision advantages.

(c) The AFCC-C2 depends on the space supporting concept for the capability of space situational awareness of friendly, adversary, and commercial space operations to enable the information advantages required for achieving decision advantages.

(7) Special operations. The AFCC-C2 depends on the special operations supporting concept for the whole-of-government capability of civil affairs forces to enable commanders to sense and

understand the civil component of the OE. Civil affairs forces are key to planning, coordinating, and conducting defense support to stabilization and the governance efforts abroad that help consolidate gains and lead to the transfer of responsibility for civilians to other legitimate authorities.   These civil affairs capabilities enable the whole-of-government approach for achieving decision advantages.

(8) Sustainment. The AFCC-C2 depends on the sustainment functional concept for the whole-of-government capability of Army contracting and financial specialists to provide relevant information on the state of host-nation economy, banking insights, labor relations (to include attitudes towards U.S. and coalition forces), and other economic insights to their commanders and unified action partners to enable the information advantages required for achieving decision advantages.

c. *Maintaining and protecting decision advantages*.

(1) Cyberspace and electromagnetic warfare operations. The AFCC-C2 depends on the cyberspace and electromagnetic warfare operations supporting concept for the capability to conduct defensive cyberspace operations, including response actions and internal defensive measures, to enable maintaining and protecting decision advantages.

(2) Fires. The AFCC-C2 depends on the fires functional concept for the capability to employ ground-based long-range precision fires, and air and missile defenses, integrated with unified action partners, to increase range, lethality, and efficiency throughout the battlefield and at all echelons which enables maintaining and protecting decision advantages.

(3) Maneuver. The AFCC-C2 depends on the maneuver functional concepts for the capability to consolidate gains continuously to ensure lasting outcomes and a more favorable security environment within the AOR which enables maintaining and protecting decision advantages.

(4) Protection.

(a) The AFCC-C2 depends on the protection functional concept for the capability to protect friendly forces, platforms, and equipment from enemy attack and against environmental hazards to enable maintaining and protecting decision advantages.

(b) The AFCC-C2 depends on the protection functional concept for the capability to protect critical infrastructure (oil fields, dams, nuclear facilities, industrial facilities, ammunition depots, airfields, roads, ports, rail transportation nodes, or anything that creates hazards on the battlefield) that are exploitable by the adversary and reduce freedom of action across the battlefield to enable maintaining and protecting decision advantages.

(5) Sustainment. The AFCC-C2 depends on the sustainment functional concept for the capability to rapidly aggregate and disaggregate logistic nodes, and increases in organic sustainment capabilities at echelon. MDO requires formations with greater freedom of action and endurance, supported with greater agility and flexibility from the sustainment warfighting function

to mass sustainment effects without massing sustainment formations which enables maintaining and protecting decision advantages.

(6) Medical. The AFCC-C2 depends on the medical supporting concept for force health protection capabilities to identify, assess, and protect Army forces from health hazards. The Army heath system force posture must support multi-domain formations operating independently from multiple locations, globally and at home, to align with the maneuver and protection concepts which will ultimately enable maintaining and protecting decision advantages.

(7) Space. The AFCC-C2 depends on the space supporting concept for the capability to protect access to space-based and space-enabled systems, and to detect and geo-locate sources of electromagnetic interference against friendly platforms and systems to enable maintaining and protecting decision advantages.

Appendix E
Risks of Adopting the AFCC-C2

E-1. Risks from concept hierarchy
The implementation risks stated in the EAB concept apply equally to this concept.[154] The AFCC-C2 has identified the following additional risks.

E-2. Risks within the AFCC-C2

a. *Overreliance on technological capabilities*. Army forces may become overly reliant on technological capabilities limiting their ability to operate in denied, disconnected, intermittent, and low-bandwidth communications environments. Units effective at maximizing the capabilities of technological enablers may be most at-risk by their loss. In the past, operating degraded included continuing to operate in the complete absence of certain enablers. The increased use of and reliance on the communications network and other technological enablers may create situations where organizations perceive that without certain enablers, operations are no longer possible. Organizations that allow the complete atrophy of non-network-enabled skills will require a minimum technological capability to remain effective. This minimum defines what it means for them to operate degraded. Training and routine practice on analog and manual systems and processes help mitigate this risk. Units need to incorporate events that practice analog or manual techniques routinely to ensure in the absence of space enablers, the communications network, and other technology, they remain combat effective and able to accomplish missions.[155]

b. *Overburdening leaders and Soldiers with technology*. Technology has the potential to radically transform the future Army force's ability to C2 and conduct MDO. Employed incorrectly, however, it can have debilitating effects.

(1) Technology can increase Army forces' ability to sense the battlefield across all of the domains and at greater distances. Technology can allow Army forces to create and share more data and knowledge with each other and their unified action partners, thereby improving understanding of operational and mission variables and fostering unity of effort. Future AI-

enabled technological decision support tools can allow leaders to make better and faster decisions, distribute their orders rapidly, and direct forces precisely. It can also allow future Army forces to maneuver semi-independently and shoot farther and with greater lethality. Technology can allow Army forces to conduct these and other activities at a level and pace that outmatches future adversaries and enemies.

(2) If not developed, managed, and integrated properly, however, future technology could harm human performance and as a result, could have the opposite effect than intended. Providing too many devices to a single Soldier or organization may divide attention among them and create levels of frustration such that the technologies actually detract from mission accomplishment. Similarly, technology may provide too much information, create cognitive overload, and slow decision making and action.

(3) Capability developers must be able to understand and measure the potential perceptual and cognitive loads—in addition to the traditional physical loads—placed upon Soldiers to ensure that Soldier performance is optimized.   To the greatest extent, technology must move independently and accomplish tasks autonomously to reduce physical, perceptual, and cognitive burdens and allow leaders and their Soldiers to focus on the most critical tasks and the ones that humans can do best. Just as leaders have to manage the physical loads that Soldiers carry, leaders and capability developers must consider perceptual and cognitive burdens and adjust "loads" accordingly.

c. *Misplaced trust in the ability to sense and understand perfectly*. As an extension of the risk above, Army leaders may operate with an implicit assumption that the data presented to them— particularly based on and displayed by sophisticated technological systems—is an exact representation of ground truth.

(1) The proliferation of sensors and information systems can create the illusion of perfect clarity from a distance and entice commanders to penetrate to lower levels of command and take over the fight. This micromanagement of the fight inhibits trust and can undercut the speed of operations as subordinates begin to become accustomed to waiting to be told what they must do. This misperception may also result in tolerating what might otherwise be unacceptable risk and forgoing the development of necessary risk mitigation strategies. It might also have the opposite effect. Commanders may only consider the data visually displayed and not consider critical intangibles such as leadership, training levels, experience, and unit cohesion. In this circumstance, they may fail to accept prudent risk and forgo critical opportunities.

(2) To combat the dangers of the potential for misplaced trust, leaders at all levels must be educated and trained to think scientifically and remain skeptical and question their assumptions, data, and reports.[156] Oppositely, however, they must not succumb to decision paralysis by waiting until they have unquestionably accurate and complete data and information. Just as commanders have different levels of trust for human subordinates, they must develop the judgment necessary to determine the amount of trust that should be given to specific technologies. This trust comes from hard, repetitive training under realistic conditions that challenges subordinates and tests the limits of their equipment and technology. Tough training improves subordinates' abilities. It also allows commanders to see that technology can perform as designed or, if not, identifies the faults

that need to be repaired or modified. In both cases, realistic training enables subordinates and technology to become trustworthy.

    d. *Imprudent application of the MC approach*.

    (1) The MC approach to C2 must be understood accurately and routinely employed during garrison activities and training to be applied properly during actual operations. The MC approach cannot be reduced to simple formulas. Its fundamental principles require varying amounts of judgment in their application. For example, the amount of control, the echelon to which decision-making authorities and warfighting capabilities (including authorities and permissions) are decentralized, and the level of risk to accept are dependent on the OE, the current situation, and how well leaders have developed their subordinates and applied the other MC principles.

    (2) Army leaders cannot apply the MC approach directly to other unified action partners that have not trained and prepared for its use. Many future partners may operate under centralized control only and by following detailed orders and instructions; disciplined initiative may not be part of their organizational culture.[157] Army leaders must prepare to adjust their leadership to accommodate partner capabilities and needs.[158] However, creating shared understanding; providing a clear intent, purpose, and priorities; promoting boldness, agility, and innovation; building a networked, cohesive team; and cultivating candor and trust are applicable to conducting any operation with any group of unified action partners.

    e. *Regression to a risk-averse environment*.

    (1) Returning to a risk-avoidance or "zero-defects" command climate creates an environment in which junior leaders are reluctant to take initiative or exercise individual judgment for fear of punishment for failure.[159] Some senior leaders in this setting might seek to protect subordinates by not allowing them to undertake opportunities where they might fail. However, not allowing subordinate leaders opportunities to push limits, make mistakes, and learn by the results, stunts junior leader growth and inhibits experience necessary to accomplish missions in future environments.[160] Instead of developing leaders who identify opportunities, weigh and accept risk, achieve advantages, and learn and recover from honest mistakes, the Army could create leaders who find success by seeking to avoid all risk. These leaders may be forced later to make difficult decisions in unfavorable circumstances. Lacking experiential judgment often born of the lessons from failure in training and lower-risk operations, they may make poor decisions and fail to recover from mistakes when the stakes are much higher. What might only be a temporary setback for a trained, experienced, and resilient risk-taker could become a permanent mission failure for the risk-averse.[161] The end result of a pervasive risk-averse environment is forfeiture of decision advantage, surrender of the initiative, and potential defeat.

    (2) To diminish the potential for regression to a risk-averse environment, senior leaders exercise moral courage and underwrite honest mistakes made as subordinates exercise initiative, using these mistakes made within the commander's intent as opportunities for learning.[162] Senior leaders understand that the climate and ability to exercise disciplined initiative is perishable and no more enduring than the physical conditioning that keeps their Soldiers fit. Consequently, they remain proactively involved in leader development (including the establishment of a rigorous unit

professional development program); monitoring, assessing, and improving command climates; and assigning and positioning personnel appropriately.[163] Commanders make full use of organizational climate surveys, routine exit interviews, and multi-source evaluation and assessment tools to assist in maintaining a culture and command climate that promotes disciplined initiative and risk acceptance.[164] Additionally, a comprehensive, meaningful, and individualized counseling program is established to drive self-development and improve performance. Improved performance raises subordinates' trustworthiness and leaders trust in them. Future leaders must be assessed and rewarded, in large measure, by their ability to empower subordinates to take disciplined initiative. They must develop, encourage, and reward innovative leaders of character who thrive in ambiguity and fast-paced, data-driven operations.

Appendix F
The C2 System's People

F-1. Introduction
Key people within the Army C2 system are commanders, seconds-in-command, subordinate commanders (including unified action partners), senior noncommissioned officers and enlisted advisors, staffs, liaison officers (to and from partners), and those who build, operate, maintain, and protect the communications network and command nodes. The C2 system centers on commanders. Commanders make decisions, clearly convey intent to provide purpose, direct action, and motivate and empower subordinates for success. As an extension of their commanders, other members of their C2 systems assist commanders in creating shared understanding, making quality decisions, and rapidly distributing mission orders and directives in an understandable and useable format. When addressing the system's people component, commanders and capability developers must also consider how individuals come together and operate as competent, cohesive, and well-trained headquarters and human-networked unified-action-partner teams. Given equal access to technological tools, decision advantages will fall to the side whose decision makers are more adaptable problem solvers, who have the most robust access to actionable information and intelligence, and who are more empowered through decentralized authorities and capabilities.

F-2. Bold, agile, adaptive, and competent leaders of character who thrive in ambiguity and fast-paced, data-driven operations.

a. The MC approach to command remains wholly applicable to the future. It is founded on well-developed leaders—enabled by state-of-the-art equipment (including AI-enabled decision support and battle management), streamlined procedures, and common, standardized, shareable, and secure data—that simplify complex activities and extend capabilities and authorities to the lowest practical level. The MC approach is based on the belief that commanders and subordinate leaders are most effective when they articulate a clear intent to empowered Soldiers and Army Civilians who share a common appreciation of the environment, problems, potential solutions to those problems, and risks involved. Commanders' make quality decisions, integrated through an efficient, effective, and domain-comprehensive operations process and communicated within a framework of accurate battlespace visualization and overall shared understanding. Bold, agile, adaptive, and competent Soldiers and Army Civilians that thrive in ambiguity and fast-paced, data-driven operations rapidly turn commander's decisions into decisive action.

b. The real power of the MC approach rests with people. The best way to counter highly adaptive threats is to enhance the expertise and abilities of people so they are more creative, agile, adaptive, and capable.

(1) To effectively command in the future, Army leaders must be grounded in the science and sociopolitical dynamics of warfare; committed to the moral, ethical, and legal application of force; and dedicated to applying the MC principles. They must also be sufficiently knowledgeable of other Services' and partners' capabilities in all of the domains and highly proficient at employing the C2 system during routine garrison activities and training, as well as actual operations.

(2) Future Army leaders must develop a full understanding of the relationships among the physical, cognitive, temporal, and virtual aspects of the battlespace. In particular, leaders must develop in-depth understanding the battlespace to include environments they cannot see such as the space domain, cyberspace, the EMS, and the IE—and have the necessary tools to visualize, describe, and display this non-physical battlespace to create shared understanding and identify decisive spaces. Commanders and staffs must also have a full understanding of the other Services' and unified action partners' capabilities and limitations.[165] They must also possess the appropriate security training and clearances with which to effectively converge effects in all of the domains.

(3) Future Army leaders must be comfortable conducting detailed analytical planning before and after operations; more systemic, conceptual planning; and switching between or blending the two approaches based on time available, level of training and experience, echelon, and the degree of complexity. They must be experts at conducting the detailed planning necessary to understand a specific situation and mission, develop a multi-domain course of action, and produce a timely operation plan or order that adheres to the principles of MC.[166] At the same time, commanders and staffs—particularly at EAB—must be equally proficient at applying (or eliciting) creative thinking to understand, visualize, and describe complex, ill-structured problems and conceptual approaches to solving them as they are at applying critical thinking and detailed planning to more straightforward problem sets.[167] To do so, commanders at all levels must develop a climate conducive to stimulating novel ideas.

(4) Future commanders and staffs will also need to develop expertise and judgment in teaming with AI, autonomous systems, and robotics to process data and information to gain improved understanding of operational and mission variables, develop courses of action, and speed decision making (including target identification, selection, and shooter designation). Network managers and defenders will need to skillfully apply and cooperate with AI to manage and protect the communications network and allow critical data and information to get to key decision makers quickly, and the locations and descriptions of high-value targets to the best shooters to achieve desired effects, even while under degraded communications conditions.[168] Likewise, Army cyberspace operators and others will need to employ AI technologies and other lethal and nonlethal means to attack threat information-centric strategies and capabilities.[169]

c. This first conceptual solution recognizes that the most vital component of any organization's C2 system is the quality, talents, and cognitive abilities of its people—the human aspect of combat power.[170] Consequently, leader development, organizational training, and a trusted and disciplined

force must remain enduring investment areas. Overall, the Army must aggressively pursue the optimization of human physical and cognitive performance, including widespread human-machine teaming, as its key competitive advantage for creating overmatch against future threats and winning in multi-domain competition, crisis response, and armed conflict.[171]

d. For MC to flourish, all Army capabilities, processes, and policies must complement and reinforce the MC approach; at a minimum, they must not contradict.[172] They must create a natural bias toward decentralization, initiative, and freedom to seek and exploit opportunity. While maintaining technological superiority is critically important, it is the courage, tactical and technical competence, creativity, and ethically-guided commitment of Soldiers and Army Civilians that will have the greatest impact on the outcome of future conflict. Future capabilities, processes, and policies must intentionally support the development of teamwork, mutual trust, shared understanding, decentralization, disciplined initiative, and risk acceptance. Without constant attention and continuous senior leader emphasis on the development of Army leaders who are culturally biased to the MC approach; can tolerate ambiguity; are willing to entertain diverse perspectives and novel ideas; and can underwrite honest mistakes, the Army is likely to slowly drift toward a culture of micromanagement and risk aversion.[173] (See appendix E for risks.)

F-3. Globally-networked, interoperable, agile, and all-domain teams of unified action partners.

a. The Army provides globally-networked (socially and technologically), interoperable, and agile teams of active and reserve component Army forces and other unified action partners that are rapidly deployable, mission-tailorable, and responsive to combatant commander needs and the Army's enduring requirements across the competition continuum. Future Army forces rapidly form cohesive, multifunctional teams while combining their diverse knowledge, expertise, and capabilities across all of the domains to create physical, cognitive, temporal, and virtual overmatch. Through flexible command relationships and agile, adaptable formations, future Army forces achieve advantages by swiftly configuring, adapting, and reconfiguring as needed to bring a different set of forces and capabilities to bear against any problem. While maintaining preeminence in the application of landpower, future Army forces adjust, adapt, and transform land-centric thinking, processes, and capabilities to support future MDO and a whole-of-government approach to campaigns and operations.

b. MDO is the application of landpower in an inherently joint way.[174] While future Army forces possess greater organic capabilities and capacities to conduct large-scale operations (including tactical air defense and increased electromagnetic warfare capabilities), they embrace and evolve the organization of Army formations to support an unprecedented degree of Service interoperability and interdependence where each force element provides domain capabilities that can be rapidly converged in decisive spaces to create windows of superiority in which to conduct cross-domain maneuver and lethal and nonlethal all-domain fires.[175] The future security environment and the broad range of potential missions combine to present a multitude of emergent threat situations requiring uniquely tailored joint task forces (JTFs). In uncertain, highly-competitive, and hyperactive environments, JTFs will likely be established with short notice under crisis-action planning conditions. While purposefully built and often temporary in nature, JTFs must not be completely ad hoc, forming only as crises emerge. Instead, the Army organizes, mans,

and trains its senior EAB formations to quickly form JTFs that can meet national and combatant commander requirements and timelines. Due to its operational and tactical versatility and generally higher experience levels of its commanders and staff leaders, a regionally-aligned corps headquarters is the Army's principal organization to transition to an all-domain-capable warfighting JTF when the preponderance of operations are centered in the land domain.

c. The capability to rapidly transition to an all-domain-capable JTF headquarters is achieved through an adequately resourced and continuous joint manning, equipping, education, and training program. All-domain competence can be achieved through organizations with the right mixture of domain-specific experts, various types of multi-domain integration generalists, and leaders with the ability to forge all-domain teams. A sustained training program includes the routine integration of senior Army headquarters into their aligned combatant command's planning efforts and joint, special operations, and multinational exercises; a greater number of EAB-level headquarters training opportunities; and extensive participation in joint and combined leader exchange programs.[176] Transitioning away from "Army-only" exercises and combat training center (CTC) rotations, senior headquarters regularly request joint, special operations forces, interorganizational, and multinational partners' participation.[177] Each training event then becomes an opportunity to receive and integrate partners; develop or refine common coordinating procedures, interoperability standards, and agreements; cultivate mutual understanding of each other's domain or functional area capabilities and organizational cultures; and identify other cultural and technological barriers and adapt the C2 system to overcome them.

d. To win in multi-domain competition and facilitate transition to warfighting, senior Army headquarters should organize and employ their staffs at home station much as they do for actual operations including the habitual use of joint and Army information systems and applications, and the routine employment of centers, groups, cells, offices, elements, boards, working groups, and operational planning teams, conducted physically or virtually. Senior Army headquarters are prepared to begin crisis-action planning using the joint planning process even while in transition to an all-domain-capable JTF headquarters.[178] As necessary, senior Army headquarters send and accept network-enabled liaison elements to facilitate shared understanding, collaboration, and coordination, and build teamwork and unity of effort among unified action partners.[179] Critically, the future Army C2 system must operate as part of a joint all-domain C2 ecosystem, whether in competition, crisis response, or armed conflict. Interoperability with, access to, and availability of—or outright adoption of—joint systems and applications is essential to forming a well-trained and prepared all-domain-capable JTF rapidly. Expeditionary Army forces deploying into a theater of operations must be trained and organized to rapidly integrate and immediately interoperate with forward-presence forces (forward-deployed and rotational) and their unified action partners.

e. The Army resources division, corps, and army-level positions with joint professional military educated and trained personnel. Other staff personnel participate in individual and group classroom and distributed learning as part of a sustained training program.[180] These efforts are integral to the Army's overall professional development program. To make quality decisions and gain decision advantages, all Army leaders must be progressively educated and trained to think, plan, and operate simultaneously across all of the domains; with ample understanding of the human aspects of military operations; and as full contributing members of joint, multinational, and interorganizational teams.[181] Again, while future technological advancements are crucial, the

necessary leap from current combined arms operations to future MDO will not occur without Army leaders who are capable of solving complex problems using capabilities from all available domains.

f. Army forces integrate with partners early in mission planning, training, and rehearsals; thoroughly understand joint, special operations forces, and other partner capabilities; and encourage unified action partners to advocate for their competencies and capabilities where they best serve the mission. Recognition of partner organizational cultures, capabilities, and limitations is vital to the MC approach and maximizing the contribution of partner capabilities. (Misapplication of the MC approach is discussed in appendix E.) Similarly, Army forces, operating in a supporting role, are proactive in determining how to adapt warfighting capabilities to the unique stability or civil support situation they may face. Army forces take the lead in developing effective partner relationships and procedures before the onset of operations.[182] This enables Soldiers and coalition counterparts to make rapid decisions when under fire. Global networking and interoperability expand the people component of the C2 system, taking full advantage of, and contributing to, joint, multinational, and interorganizational capabilities, knowledge, and expertise. Interoperability and a well-coordinated, synchronized, and mutually-reinforcing civil-military effort are essential to winning in multi-domain competition, crisis response, and armed conflict, and making hard-fought gains enduring.

Appendix G
C2 Processes

G-1. Introduction

a. The Army's overarching framework for making decisions, organizing forces and capabilities, and putting decisions into action is the operations process: planning, preparing, executing, monitoring, and continuously assessing operations. Each warfighting function has one or more functional integrating processes that support the overall operations process. And like the overall operations process, each supporting process must consider how it contributes to supporting a whole-of-government approach to winning. Two key supporting processes that cut across warfighting functions are knowledge management (which includes information and data management) and airspace management. Knowledge management is the process that optimizes the arrangement of the C2 system's people, process, and tools to enable knowledge to flow and commanders to make rapid, quality decisions. Airspace management is the process used to coordinate, integrate, and regulate the use of airspace of defined dimensions.

b. Currently, the Army uses two key methodologies or sub-processes for planning campaigns and operations—the Army design methodology and the military decision-making process—to enable Army forces to understand the OE and problems, determine an appropriate end state, and visualize the conceptual and detailed approaches to attain that end state.[183]

c. Knowledge management is an essential process as it enables the generation and flow of knowledge to enhance all-domain battlespace visualization, overall shared understanding, continuous learning, and rapid, quality decision making. Knowledge management is also applied

to continuously assess CP configurations to determine the best number, distribution, and alignment of the C2 and other warfighting functions' people and tasks both within and among various command nodes. Knowledge management ensures the integration and distribution of knowledge and capabilities throughout an organization.

d.   Airspace management ensures the safe, flexible, efficient, and effective use of assigned airspace and the Army's organic and supported aerial capabilities. The proliferation of unmanned aircraft systems and the employment of directed-energy and long-range precision fires capabilities result in contested and congested airspace requiring dynamic and flexible Army and joint airspace planning, management, and coordinating measures.

e.   Other warfighting functions' integration processes, such as intelligence preparation of the battlefield, information collection, targeting, air and missile defense control, risk management, protection assessment, movement control, supply distribution management, and other sustainment processes, support the overarching operations process and are equally critical to supporting MDO and a whole-of-government approach, improving agility, and overall, achieving decision advantages and combat power overmatch.[184]

f.   While this concept takes the approach that many of the Army's current integration processes are, at their base level, sufficiently broad to allow necessary adaptation and modification during the concept's timeframe, it does not rule out that some processes may need to be abandoned altogether and new processes developed and instituted. Wherever possible, the Army and other Services must adopt joint processes outright.[185] Rather than modifying Army-only processes, wholesale adoption of joint processes (and shared terms) gains efficiencies and drives the interoperability required by future MDO.[186] However, any future integration processes—joint or Army-specific—must be comprehensive and habitually consider capabilities from all available domains that can be brought to bear to accomplish assigned missions across the physical, cognitive, temporal, and virtual aspects of the battlespace.

G-2. All-domain operations process

a.   Due to the uncertain future environment and the Army's previous focus on counterinsurgency and other operations dominated by stability tasks, the Army refocused on the conduct of the operations process at all echelons, with unified action partners, and across the full range of military operations. Army training and education reemphasized crisis-action planning and large-scale operations characterized by lethal and destructive offensive and defensive tactical task. For the future, the Army must continue along this path. In addition, it must determinedly broaden its expertise to include the seamless integration of joint, multinational, and interorganizational capabilities to create temporary windows of superiority across multiple domains and throughout the depth of the physical, cognitive, temporal, and virtual battlespace to achieve the operational initiative.

b.   As the Army develops new capabilities, the operations process and supporting integration processes must be updated to ensure these capabilities can be integrated into operations rapidly and fully, and not addressed later as an afterthought. At a minimum, newer capabilities must be carefully incorporated into operations to multiply combat power and create overmatch.

Conversely, newer non-physical capabilities, like offensive cyberspace operations, may be situationally decisive and older, more-conventional physical capabilities employed in a supportive role. New Army formations may be created to add the required physical, cognitive, temporal, and virtual capabilities into the force. These formations will bring the depth of expertise needed for rapid and skilled execution. Nevertheless, the higher headquarters responsible for employing these capabilities must have the requisite knowledge and expertise to understand the capabilities that these new formations bring to multi-domain competition, crisis response, and conflict, and how to continuously converge their lethal and nonlethal effects across multiple domains to enable cross-domain maneuver and all-domain fires.[187] Recognizing that the character of armed conflict is always changing, the Army modifies or creates new planning methodologies and multi-domain control measures, and constantly pursues other innovative tools for commanders to understand, visualize, describe, and direct action rapidly in and across all of the domains.[188]

c. Driving the operations process, commanders identify intelligence and information requirements and determine priorities rapidly to focus intelligence, reconnaissance, and surveillance capabilities to answer priority information requirements and create deeper shared understanding.[189] Army commanders and their staffs are tactical and technical experts, skilled in operational art, capable of framing complex problems, talented at thinking, planning, and operating across multiple domains, and able to adapt quickly to changes in the situation or new information.[190] Army commanders are proficient at formulating and articulating effective planning guidance and preparing a clear mission statement, intent, and concept of operations to guide multi-domain action.[191] Comfortable with ambiguity, Army commanders, staffs, and subordinate leaders balance risk against reward, make timely and quality decisions, and take appropriate action without complete information or perfect synchronization. Recognizing the capabilities of individual team members and demonstrating humility regarding their own strengths and limitations, future Army leaders build cohesive teams with the right mix of capabilities for mission accomplishment.

d. Because the proliferation of technology is an integral part of the future OE, future armed conflict can no longer be considered simply an attritional contest between opposing military forces.[192] It must also include the battle to defeat or protect increasingly complicated and complex operational systems. Consequently, future Army forces must develop the expertise and operational art needed to conduct a systems warfare analysis to defeat near-peer threat systems (notably their air defense and fires complexes).[193] Through systems thinking, friendly forces develop a holistic understanding of threat systems and how they are employed in order to determine the friendly actions necessary to reduce or collapse key threat systems or align friendly systems in a manner that reduces vulnerability and renders the threat system less effective. Underpinned by extensive information collection and analysis, this system-of-systems examination identifies critical system nodes or pathways within combined systems that may be individually exploited to reduce overall system functioning, or detects the multiple interdependent pathways and nodes of composite systems that may be engaged simultaneously, thereby creating a cascading effect that degrades or collapses the larger system as a whole.[194]

e. While rebalancing and improving its expertise to plan, prepare, execute, monitor, and assess large-scale combat, the Army simultaneously ensures that previous lessons learned, particularly its understanding of the criticality of the human aspects of military operations, the proper use of restraint, and special operations and conventional forces interdependence and integration, are

institutionalized in the Army profession.[195] Deliberate integration into the Army's culture and operating capabilities safeguards against individual and organizational memory loss.

G-3. Support to whole-of-government approach

a.   Achieving national aims in future OEs requires the timely integration, dynamic synchronization, and optimal convergence of all instruments of national power as part of a combined, whole-of-government approach that avoids redundant and competing efforts. The military's operational defeat of an enemy is only a part of the larger campaign. The overall objective is to create a secure environment to facilitate a better political, social, or economic outcome. Future multi-domain competition, crisis response, and armed conflict require the timely integration, dynamic synchronization, and optimal convergence of the activities and capabilities of civilian partners with military operations. Accordingly, the Army organizes in a manner that facilitates an integrated whole-of-government approach, making it easier to generate the breadth and depth of knowledge and capabilities necessary to achieve clearly identified, mutual objectives. As the central process of the C2 system, commanders and their staffs employ the operations process to integrate available elements of national and coalition power in time, space, and purpose. They achieve this by integrating unified action partners into the process, and applying their knowledge and capabilities into making quality decisions.

b. In both defense support of civil authorities (DSCA) and defense support to stabilization, the Army joins with and supports other federal agencies to confront domestic emergencies and promote stability in designated fragile and conflict-affected areas outside the U.S. Future Army forces contribute to joint interoperability across all warfighting functions, form habitual partner relationships, and seamlessly combine, coordinate, synchronize, and integrate with partners, either as the lead or in active support, to promote unity of effort and the qualitative advantage needed for the Army and the nation to succeed. Without a whole-of-government approach, future Army forces may win every battle and engagement, but the nation fail to secure its overall objectives and protect its vital interests. Consequently, the Army makes the internal changes necessary to become a valued and capable supporter of this holistic, winning approach.[196]

c.   Significant civilian populations and dual-use nature of considerable amount of communications, transportation, and sustainment infrastructure mean that many military operational decisions will have to be made in close concert with host-nation governments. Future Army forces must understand, visualize, and leverage or shape the functions, capabilities, vulnerabilities, and influences of populations, government institutions, and other interorganizational partners that reside or operate in and around an area of operations. These efforts support information collection and expand situational understanding, inform targeting and decision-making cycles, mitigate civilian interference, maintain operational tempo, and prevent the loss of combat power required to support host-nation security issues.

d. Across the competition continuum and at all echelons, civil affairs forces are commanders' subject matter experts and facilitators for military-to-civil engagements and transitional governance operations. Civil affairs forces' well-developed expertise is applied to ensure shared understanding and visualization of the civil component of the OE, a coordinated whole-of-government action, and overall unity of effort. Civil affairs forces are key to planning,

coordinating, and conducting defense support to stabilization and the governance efforts abroad that help consolidate gains and lead to the transfer of responsibility for civilians to other legitimate authorities.

e. Army contracting specialists overseeing execution of contracts can provide invaluable information on the state of host-nation economy, labor relations (to include their attitudes towards U.S. and coalition forces), and other economic insights to their commanders and unified action partners. Similarly, Army financial intelligence and counter-threat finance personnel interact with host nation and regional banking and finance and can provide more insights into a region's economy. This type of whole-of government support will be crucial in MDO as adversaries will leverage economic power to gain advantage.

f. Finally, future Army commanders and staffs achieve greater understanding of the differences between domestic and overseas operations based on applicable laws and DOD policies. This includes the distinctions between Army components (authorities, domestic support capabilities, requirements, and restrictions) as they task organize and establish flexible command and support relationships to accomplish assigned missions.[197]

G-4. Pervasive knowledge management to generate shared understanding, speed decision making, and create cognitive overmatch.

a. Future knowledge management streamlines the flow of information and intelligence and ensures commanders, staffs, and subordinates are not overwhelmed by the volume and availability of information but, instead are provided or can derive the required knowledge when they need it to make sound, ethical decisions and solve problems. Knowledge management is applied continuously to optimize how information is collected, developed, and shared throughout the operations process (and supporting processes, activities, and procedures), within and among their distributed command nodes, across echelons, and with unified action partners. Knowledge management is also employed to organize, adapt, and reorganize staffs as needed to generate and exploit knowledge rapidly, and streamline an organization's battle rhythm and decision cycles across time zones, planning and event horizons, and with partners. Knowledge management aids in developing and balancing efficiency with the adaptability needed to be effective. It is crucial to creating decision advantages against near-peer threats.

b. The routine application of knowledge management ensures that required information is validated, assimilated, organized, and shared by leaders, Soldiers, Army Civilians, and other unified action partners, so that it is easily discovered, accessed, and applied when and where needed. Further, the disciplined employment of knowledge management improves an organization's ability to understand the operational and mission variables within a given environment (and the relationship among the variables), and enables commanders to rapidly visualize and apply an operational approach and end state under any conditions. This requires knowledge management experts to have the capability to access and pull data from databases, manipulate the data (transforming data into relevant information), and design easy-to-understand display presentations (charts and models) that reduce the cognitive load on users.[198] Knowledge management facilitates collaboration and learning, encourages subordinates to act within their commander's intent, and fosters unity of effort among dispersed partnered organizations.

c. Comprehensive knowledge management is embedded into all underlying operational and institutional Army functions and activities. Knowledge management generates and enhances shared understanding and all-domain battlespace visualization, increases collaboration, accelerates learning, and improves and speeds decision making. In so doing, knowledge management improves agility and operational effectiveness across and among all echelons and unified action partners.[199]

d. Knowledge management enables future Army formations and organizations to become true learning organizations. Active knowledge management helps leaders cultivate mental agility, make quality decisions, and develop an overall cognitive edge against highly-competitive threats.[200] Critical to achieving decision advantage and staying inside the enemy's decision-making cycle, Army forces skillfully employ information management to systematically build, structure, and integrate data to distill information and constantly create knowledge.[201] Future Army forces must continuously assess their knowledge management capability, as well as the degree to which they are encouraging individual and organizational learning and establishing an Army culture of learning and innovation.

G-5. Responsive airspace management to facilitate cross-domain maneuver and all-domain fires.

a. Future airspace management enables the safe, efficient, effective, and flexible use of assigned airspace among Army forces and their unified action partners for greatest operational effect. Future Army forces exploit the benefits of increased interoperability as part of joint all-domain C2 to create seamless airspace coordination, integration, and regulation at echelon between Army and joint airspace users and other unified action partners. With advancements in technology, Army forces conduct real-time airspace management to deconflict flight paths and trajectories, make maximum use of its assigned airspace use while preventing fratricide, optimize aerial capabilities and effects, and enable MDO.

b. Future airspace management enables Army forces and other unified action partners (including federal agencies as needed) to make optimal use of airspace allowing greater density of munitions, directed energy, and aircraft over an operations area. Future AI systems—powered by common, standardized, shareable, and secure data and self-reporting platforms— rapidly synchronize and deconflict improved precision and loitering munitions; high-altitude long-endurance communications and surveillance platforms; large numbers of manned military (including coalition and special operations forces), civilian, and other government agency aircraft; myriad unmanned aircraft systems distributed across virtually every echelon; and air and missile defense engagements.[202]

c. Future airspace management, enabled by an all-domain capable, tailorable battlespace visualization that includes display of relevant airspace information, facilitates dynamic adjustments to airspace plans and rapid dissemination of those changes to all affected users. Future airspace battle management systems are capable of the real-time detection and tracking of all friendly, enemy, and civilian aerial platforms within assigned airspace to facilitate the timely integration, dynamic synchronization, and optimal convergence of effects from and through the

air into other domains, as well as effects in the air domain itself.[203] Future airspace management supports the joint force's ability to use any sensor for target identification (and later battle-damage assessment), and quickly and seamlessly access and transfer that sensor's data through any command node to the best shooter for timely prosecution. Overall, future airspace management contributes to the Army's ability to operate effectively and efficiently in highly-contested and heavily-congested airspace and gain, maintain, and exploit the operational initiative.

Appendix H
The Army's Future Communications Network

H-1. Introduction

a. The Army's future communications network encompasses all communications capabilities and associated procedures for collecting, processing, storing, displaying, disseminating, and managing information. It is the Army's interoperable contribution to the larger Department of Defense (DOD) communications network. Like the holistic nature of the C2 system of which it is a part, the Army's communications network is the totality of enterprise and deployed networks operating seamlessly as a unified whole. The communications network consists of—
- Network transport
- Information, information-management, and battle-management systems (including a tailorable battlespace visualization capability)
- Warfighting and business applications
- Network services
- Sensors and other network points of presence
- Data

> **Note:** *The AFCC-C2 describes the future communications network. For actions taken on the communications network, refer to the Army Futures Concept for Cyberspace and Electromagnetic Warfare Operations.*

b. The Army's future communications network links leaders, Soldiers, Army Civilians, and other unified action partners; command nodes; ground, aerial, waterborne, and space-based platforms; and sensors to help create a synergistic, globally-connected total Army force and allow Army forces and their unified action partners to seamlessly interoperate in the expanded competitive space.[204]

c. The communications network is simple for operators to establish and maintain, reliable, intuitive to the user, mission-tailorable, and allows commanders to expand the people component of their C2 system as required. The future communications network allows commanders to connect unified action partners over greater distances and in urban and other complex terrain, within and between the operating force and the strategic sustainment base, during all phases of an operation, and, based on need-to-know, across all security enclaves. It enables Army forces and unified action partners to collaborate, create all-domain battlespace visualization and overall shared understanding, and continually increase the depth of their organizations' knowledge and

expertise. Shared understanding includes clear visualization and understanding of the organization's communications network and current levels of connectivity among partners

d. With primacy to facilitating C2, the communications network links all sensors to the right command node and the best shooter in real time and in any domain to improve situational understanding, the speed and quality of decisions, and achieve timely, all-domain convergence.[205] It also provides the warfighting platform from which to conduct cyberspace operations and other network-based activities. While an essential combat multiplier, overreliance on technical capabilities provided by the communications network may lead to unacceptable atrophy of the traditional skills necessary to continue to operate under degraded network conditions. (See appendix E for risks.)

H-2. Operational imperatives for the future communications network

a. The Army's communications network is designed and built holistically to operate with MC principles, supporting warfighting processes, and business procedures. The communications network provides the warfighting platforms for cyberspace operations and other network-based activities. The communications network enables future Army forces to out-think, out-maneuver, and out-fight adversaries physically, temporally, cognitively, and virtually through extension of combined arms across all of the domains. To enable decision advantages, the future communications network facilitates the following operational imperatives.

(1) *Continuity of command*. The communications network facilitates the ability for commanders, staffs, and subordinate leaders to continuously communicate together and with other unified action partners. It allows them to tailor, monitor, and in real time, refresh or update their tailorable battlespace visualization to enhance and maintain continuous shared understanding. The communications network facilitates these abilities during daily home station activities, training, and operational deployments; from the continental U.S.; to and throughout the area of operations; and across warfighting functions. It supports Army leaders and Soldiers while moving on the ground (dismounted or mounted and in all types of terrain), in the air, or on the water.[206] The communications network allows globally-responsive Army forces to C2 anytime, anywhere, against any enemy. Achieving continuity of command includes the ability to plan without major interruption and in parallel among globally-dispersed command nodes and forces, and throughout the competition continuum and all phases of preparation, deployment, entry, and follow-on MDO.

(a) Regardless of the mode of intertheater or intratheater maneuver (ground, air, or sea), achieving continuity of command requires an enroute C2 capability, with access to real-time, all-source intelligence to support joint-expeditionary and multiple, simultaneous, and dispersed entry operations (forcible or permissive) into remote areas.[207] Enroute or on-the-move C2 capabilities include integrated maneuver (ground and air), fires, and intelligence collaboration and planning applications, the capacity to view real-time, full-motion video gathered from any collection platform, and the ability to provide updates to unit mobile devices.

(b) Realizing continuity of command is essential to the rapid deployment and employment of combat-ready forces directly into noncontiguous areas of operations and the unity of effort between early-entry, follow-on, and rotational forces. It also supports cross-domain maneuver and

lethal and nonlethal all-domain fires by allowing the commander to exercise authority, direct action toward accomplishment of intent (including during planning and rehearsals), monitor operations, assess effects, and make timely and informed decisions in response to changing conditions.[208] Continuity of command across the competition continuum and range of military operations is achieved by integrating mobility platforms, computing environments, supporting infrastructure, and other ancillary equipment carefully; a robust network transport that can leverage what is commercially available securely to augment organic Army assets; and proactive network management.

(2) *Expeditionary, dispersed, and decentralized operations.*[209] The communications network has ample capacity and robustness to support expeditionary, dispersed, and decentralized MDO in remote, austere environments, dense urban areas, and other complex terrain. The communications network connects air and ground maneuver, intelligence, fires, protection, and sustainment elements; adjacent, subordinate, and higher echelons; and relevant unified action partners.[210]

(a) The communications network provides a converged network transport configuration, voice, data, imagery, and video. This network transport configuration consists of a balanced continuum of line-of-sight and beyond-line-of-sight means that are layered on the land and sea, in the air and space (including high-altitude), and undersea. This layered network transport must be defended in cyberspace and the EMS, as well as the physical domains in which they exist. The communications network provides multiple paths for information to take. When one path is disrupted, critical data or communications is automatically re-routed through another path or transport mechanism to the intended recipient.

(b) The Army's future network transport is resilient and self-healing, and provides automatic, uniform, and location-agnostic access to information, applications, and services. However, when the communications network is severely disrupted, units and individuals can disconnect information systems, continue to conduct operations on individual systems or as part of smaller closed networks, and reconnect and resynchronize later within the communications network when connectivity is restored. In this manner, the communications network supports the MC approach by allowing subordinate organizations and individuals some level of functionality within which to exercise disciplined initiative.

(c) The Army leverages existing technologies to achieve required imperatives while reducing the Army's communications architecture footprint and reliance on fixed infrastructure. A robust, resilient, layered, and multi-path network transport is critical to the extension of a commander's reach, the conduct of dispersed operations at maximum supporting ranges and extended supporting distances (including the ability to sense across the depth of the expanded battlespace), and the overwhelming synergy that can be created through shared understanding and synchronized warfighting capabilities extended to the lowest tactical echelons.[211] It enables leaders to have the right information, at the right time, and in a useable format to make the right decisions. It also enables the Army's physical and synthetic future training environments; supports continuous learning and adaptation by providing all Army leaders, Soldiers, Army Civilians, and organizations access to knowledge and educational opportunities (including the ability to create and participate in learning networks); and facilitates the ability to train and exercise command regardless of physical location or phase within the Army's future sustainable readiness process.

(3) *Interoperability with unified action partners.*[212] The Army's communications network supports dynamic and rapid forming and reforming of human and organizational networks among unified action partners. It creates the potential for other joint, multinational, and interorganizational elements previously separated by geographic and organizational barriers to fight cooperatively. It enables coordination, cooperation, and the secure exchange of real-time intelligence and relevant information to achieve unity of command or unity of effort with partners not under a commander's direct authority. Improving systems interoperability and creating an inclusive mission partner environment have priority over improving individual systems capabilities.[213]

(a) Interoperability enables the timely integration, dynamic synchronization, and optimal convergence of joint and coalition partners' lethal and nonlethal activities and capabilities through sharing and exchanging data and information and collaboratively creating, communicating, and rehearsing plans and orders.[214] Army C2 information, information-management, and battle-management systems enable senior Army headquarters to work, operate, and plan easily within a joint and coalition environment and transition rapidly to or join a JTF or joint force land component command.[215] The communications network allows Army forces to establish or integrate into joint and combined all-domain fires and airspace control networks easily, greatly expanding munition, aerial, and sensor capabilities. The future communications network enable the sharing of sustainment data and information among unified action partners to allow total-asset visibility and optimize resource utilization.

(b) Technical interoperability with unified action partners (and the Army's own information systems) is attained through shared network services, infrastructure, and security architecture; establishing and following requirements for data to be common, standardized, shareable, and secure; and strict adherence to a joint common operating environment—a universal set of computing technologies and standards.[216] Computing standards adhere to industry best practices to facilitate the integration and adaptation of future technology. As systems and applications are upgraded, they remain backwards compatible between versions or improvements. To support agility and adaptability, the communications network allows Army forces to share data and information rapidly, collaborate, and establish a secure-but-unclassified battlefield visualization with unified action partners that do not have security clearances but are critical to accomplishment of the mission or in the lead (for example, interorganizational partners during a natural disaster or other DSCA or stability missions).[217]

(4) *Convergence of capabilities from all of the domains.* To effectively support convergence of capabilities in all of the domains, the communications network must support deep sensing and human-machine cooperation, collaborative decision making, and battle management.

(a) The future communications network enables seamless access to information from joint, Service, and other unified action partners' information systems and sensors throughout the extended battlespace to enable commanders to understand, visualize, describe, and assess complex problems rapidly. It facilitates commander's visualization of a diverse set of people, objects, activities, and capabilities in time and space which in turn, enables understanding of the current situation and future opportunities. An accurate understanding of the battlespace enables

commanders to conceptualize, plan, and execute optimal combinations of sequential and simultaneous operations organized across multiple domains to create windows of superiority.

(b) To support the convergence of capabilities from all of the domains, the future communications network embraces human-machine cooperation, collaborative decision making, and battle management. Supported by AI, ML, and big data analysis, the Army's future communications network allows commanders and staffs to plan, monitor, and assess MDO to rapidly identify weaknesses and opportunities in planning and execution, and make the necessary adjustments at speed that outpace adversaries. AI-enabled decision-support and battle-management systems promptly recommend action when friendly force strengths, paired against enemy vulnerabilities, create overmatch and similarly, provide alerts and recommend action when the situation is reversed. As such, the future communications network must leverage AI, ML, big data analysis, enhanced automation, and quantum computing technologies as they become available to address key requirements identified in experimentation and ongoing real-world operations.

(5) *Rapid force tailoring, dynamic task organization, and support of commander's priorities*. The communications network is configured and reconfigured easily, secured, operated, maintained, and sustained to increase agility, enable freedom of action, and support the exercise of disciplined initiative on land and in and through the other domains as required.

(a) As bandwidth is critical, the communications network facilitates the visualization and responsive data-informed management of its transport resources to scale and align rapidly with the commander's changing intent and priorities, dynamic modifications to task organization and scheme of maneuver, and other changing mission requirements.[218] Along with a robust network capacity, dynamic network management contributes to the establishment and sustainment of reliable and ultra-low-latency communications to support all-domain sensor-to-shooter links, airspace management, medical, and other selected mission requirements where extreme accuracy and timeliness are essential.

(b) Dynamic network management also includes signature awareness, management, and control aspects to understand and reduce susceptibility to signals intercept and enemy countermeasures. As part of DSCA or stability operations, the Army extends its network resources to other interorganizational partners when needed. Semiautonomous network management optimizes applications, service levels, and system performance to meet the commander's intent under all network conditions, across computing environments, and throughout the operation.[219] Overall, these imperatives support the development of the agility and versatility necessary to form, dissolve, and reform teams rapidly to allow the Army and the joint force to succeed throughout the entire competition continuum.

(6) *Leverage of data and information*. As data and information are critical to quality decisions and future MDO, the communications network enables protection and visibility of, and ready access to, data and information for all Soldiers, Army Civilians, and authorized unified action partners appropriate to their security clearance and need to know.

(a) Soldiers and Army Civilians can find and access non-sensitive, distributed learning content anywhere and on any device. The communications network automatically allows visibility across security levels. However, the communications network automatically blocks sensitive data, information, or network access to unauthorized individuals, processes, or devices, and detects and protects against modifications or destruction of data and information. This includes the capability to self-destruct, thereby preventing data and system capture by potentially successful attackers. It must also include the capability to back-up data and allow remote locations to operate from back-ups to maintain continuity of command.[220] Cybersecurity for the communications network keeps pace with evolving threats and the ever-increasing number of attack surfaces created with the addition of more and newer network points of presence.

(b) Following threat attacks, debilitating environmental effects, or other operational hazards, the communications network facilitates restoration of data, information, and information systems lost, damaged, or destroyed. In an IE characterized by competing demands for limited network resources and combinations of space, cyberspace, and EW attacks, clear visibility and assessment of the status and functionality of the communications network, coupled with agile network management, facilitate the shareability, protection, and integrity of critical data and information to support mission requirements.

(7) *Collaborative development of shared understanding*. While a tailorable battlespace visualization capability is essential to generating shared understanding and visualization of the battlespace, screen icons, charts, and tabulated data, no matter how accurate, cannot describe a vision or idea, communicate intent and purpose, articulate acceptable risk, and build consensus among a diverse range of unified action partners.[221] Achieving shared understanding and solving complex problems requires dialogue and collaboration. Collaborative capabilities support decision making and the sharing of the resulting decisions and the relevant information that informed those decisions among staff and subordinates as rapidly as possible to speed action. Future collaborative capabilities help to distribute decisions and relevant information in a useable and sharable format and minimize unnecessary interruptions to staff and subordinate leaders.

(a) The communications network includes a common suite of tools and processes that allow multi-form collaboration internally and externally to enable and speed shared understanding, cultivating trust and encouraging disciplined initiative. This imperative includes sharing ideas and developing understanding between superiors, subordinates, peers, and other unified action partners in the form of sketching, highlighting, talking, listening, and gesturing through voice and voice-recognition, text, chat, video, white boarding, map boarding, messages, three-dimensional representations, file sharing, virtualization, and other common applications. The right mixture of collaborative applications and devices allows unified action partners to train and master these collaborative capabilities and find the nexus where they can communicate and describe their ideas best, and others can best receive, understand, and contribute to their development or refinement.[222]

(b) Advances in computing power and technologies allow Army forces to collate, sort, cross-reference, and analyze huge volumes of data to glean relevant information to inform understanding and decision making. Commanders, staffs, subordinate leaders, and other unified action partners operating from widely dispersed and constantly changing geographic locations gather relevant information, plan, collaborate, and learn from each other as effectively as if they were co-located

and stationary. Effective collaboration generates the solutions to unfamiliar and emergent mission situations that no single individual or organization could independently develop.

(c)   The communications network enables the receipt and dissemination of relevant information for synthesis and display or overlay on a tailorable battlespace visualization based on common, standardized, shareable, and secure data from all of the domains and warfighting functions that is refreshed simultaneously as data is updated. This tailorable battlespace visualization is available and pushed as needed to the mounted or dismounted commander, leader, and Soldier; all higher-echelon commands; and appropriate unified action partners.[223] This imperative supports all-domain battlespace visualization; enhanced collaboration and shared understanding; effective coordination; synchronized and timely action; and the establishment and sustainment of ready and globally-responsive units.[224]

(d) To support a real-time tailorable battlespace visualization, C2 information, information-management, and battle-management systems utilize and employ common, standardized, sharable, and secure data that enables all elements of the Army and joint force (and other ground, supporting forces, and national agencies) to reference the same information no matter the device or application used. A single, standard data input into a unified database is accessed and shared among all sensors, Army information systems (stand-alone or integrated into weapons platform), and applications at all echelons and across all functional formations, and is directly attributable to the reporting organization for rapid verification in case of a perceived discrepancy. This facilitates coordination, integration, shared understanding, interoperability, maneuver, targeting, and reporting.[225]

(8) *Parallel planning and rapid order development and dissemination.* The communications network allows Soldiers and Army Civilians to solve problems and make good decisions rapidly, and create, change, and distribute plans and orders (voice, written, and graphical) between command nodes; ground, air, and waterborne platforms; dismounted formations; and unified action partners, collaboratively and dynamically.

(a)   During rapidly-changing, decentralized, and dispersed operations, this imperative promotes parallel planning, teamwork, and unity of effort, and provides the means to communicate the commander's intent (purpose, key tasks, and end state) to the lowest tactical levels clearly and accurately. During more centralized operations requiring greater massing of effects and precision (high-intensity, large-scale combat against large enemy formations, for example), this imperative includes the ability to rapidly convey greater levels of detail when needed to simultaneously integrate, synchronize, and converge domain capabilities, warfighting functions, and the activities of all subordinate forces. To support a rapidly-responsive, expeditionary Army, this imperative also includes an enroute mission planning capability.

(b) The communications network links and enables all aspects of the operations process, and supports its various planning methodologies, such as troop leading procedures, the military decision-making process, and Army design methodology.[226] Rapid, quality decisions, disseminated quickly, accurately, and in a form that is easily understood, creates a decision advantage that enables Army forces to act decisively, outpace, and outmatch adversaries and enemies anywhere along the competition continuum.

(9) *Fusion of operational, sustainment, and civil information with intelligence.* The communications network enables the commander and staff to gather, track, analyze, and fuse operational, sustainment, and civil information with intelligence to generate shared understanding of the situation, environment, assumptions, constraints, limitations, problems, multi-domain operational approaches, risks, gains, and desired end state. This fusion also contributes to effective and continuous assessment of the operation's progress, effectiveness, and sustainability, and the overall quality of shared understanding. Future assessments determine if needed intelligence, operational, sustainment, and civil information was available when and where it was needed to make a decision and if not, why. Critically, future operational and training assessments must routinely include determination of network connectivity, knowledge flow, shared understanding, battlespace visualization, and interoperability.

(10) *Training, wargaming, rehearsals, and in-stride decision making.* C2 warfighting applications contain embedded training, wargaming, rehearsal, and in-stride decision-making functions that support live and synthetic constructs for unit (individual and collective) and institutional training and education, and real-world MDO.[227]

(a) These warfighting applications include reconfigurable, globally-available, and mobile 2D and 3D simulation and stimulation tools.[228] These tools model and replicate the threats, terrain and other environmental conditions, sustainment complexities, and current technological capabilities and limitations in, through, and from space, cyberspace, the EMS, the IE, and other domains that Army forces will encounter. Future simulation and modeling tools expand to replicate the effects of Army operations on influential leaders, audiences, and other stakeholders, and the effects of these individuals and groups on Army operations. These future simulation, modeling, and stimulation tools enable geographically-dispersed, multifunctional teams to train, rehearse, and operate together.

(b) In addition to the requirement for backwards compatibility between system and application versions or improvements, all applications are simple, intuitive, and standardized with a common look and feel across all systems and warfighting functions. This minimizes training requirements, frees up time for scenario based training, sustains perishable skills, and facilitates command node operations and C2 functions. This imperative supports development of an immersive synthetic training environment that can approximate the future OE in all of the domains to create realism and facilitate mastery of the MC principles and C2 tasks, processes, procedures, and applications required to succeed in MDO.[229]

b. As a final point, the Army's communications network is an integral component of the all-domain-capable C2 system. However, even under denied communications conditions, future Army leaders can take disciplined initiative and act in the absence of orders, when existing orders no longer fit the situation, or when unforeseen opportunities or threats arise. Training always incorporates simulated command node attacks and communications disruptions for significant periods of time to allow formations to practice and stress their contingency communications plans (primary, alternate, contingency, and emergency), command succession plans, and other tactics, techniques, and procedures that allow Army forces to continue to operate under degraded network conditions.[230]

H-3. Common, standardized, shareable, and secure data

a. All future technology intended to connect to the Army's communications network must be designed to organically interoperate as part of a joint common operating environment, and send and receive common, standardized, shareable, and secure data among all components and—to the greatest extent possible—unified action partners. *Common data* is data that is synchronized to ensure that all users see the same representation of reality. Common data is authoritative and available to all users at the speed available through the communications network. *Standardized data* is a data storage schema that includes data form, format, structure, tagging, domain values, and semantics. *Shareable data* is data that can be discovered, accessed, understood, and transformed into a digestible format to internal and external users without changing the intent of the representation, including any mission partner or legacy system not compliant with standardized data models. *Secure data* is data that is protected against unauthorized use and manipulation.

b. Common, standardized, shareable, and secure data is critical to the AI, ML, and big data analysis that supports decision making and to linking all sensors to the right command nodes and the best shooters. Without common, standardized, shareable, and secure data, the necessary improvements in the speed and quality of decision making, the ability to converge capabilities across all of the domains to create windows of superiority, and the capability to seamlessly interoperate technically with partners will not be possible. Common, standardized, shareable, and secure data is at the heart of the Army's and the joint force's ability to out-think, out-maneuver, and outpace any competitor, deter aggression, and win in multi-domain competition, crisis response, and armed conflict with the lowest costs to the Army and the nation. These required data qualities are achieved through two primary methods. First, *new* data can be created at the outset to be common, standardized, shareable, and secure. Second, *existing* data can be analyzed in whatever location and format that it is found in, and the results translated or converted to take on these qualities sufficiently to be widely, rapidly, and securely distributed and used among unified action partners. Both approaches are required for the future timeframe of this concept.

(1) Common, standardized, shareable, and secure data encompasses the DOD data strategy goals to make data visible, accessible, understandable, linked, trustworthy, interoperable, and secure, as the DOD strives to become data-centric. This concept is aligned with the DOD data strategy vision to leverage data at speed and scale for increased efficiency and to gain, maintain, and exploit the operational initiative.[231]

(2) To achieve the speed and quality of decisions required in future MDO (including targeting decisions), Army and joint sensors; information, information-management, and battle-management systems; logistics systems, and weapon systems must rapidly exchange data, see or interpret it the same, speedily process it, and trust in its accuracy and provenance. Common, standardized, shareable, and secure data includes 2D and 3D terrain data to create an accurate, high-resolution geospatial foundation that enhances intelligence analysis and shared understanding, speeds decision making, and supports precision targeting. This data also includes friendly Soldier, vehicle, and weapons sensor data that can be used for any number of things such as health status monitoring, predictive logistics, airspace deconfliction, and friendly combat power assessment. Finally, this data includes ground, maritime (surface and subsurface), aerial, space,

cyberspace, EMS, and sensor data and human reports that can be analyzed with AI to allow for the detection, identification, and location of threats and their weapon systems. No data can be guaranteed to be perfect. However, decision makers can more readily rely on data that is born common, standard, shareable, and secure to create decision advantages.

(3) While data that is created by Army and joint forces to a standard criteria is more reliable and trustworthy, the Army and the joint force as a whole cannot regulate data outside their control. Future Army and joint forces require data from as many applicable sources as possible to gain an understanding of political, economic, financial, social, infrastructure, informational, and other civil aspects of the OE. Consequently, future Army forces require an automated capability to analyze data as it is found and translate and manage the resulting data and information into a common, standardized, shareable, and secure format. This comes with the real risks, however, that threats may create false data and manipulate existing data to confuse and disrupt operations, and that an automated tool may replace data field gaps with incorrect information. Both risks reduce the overall trustworthiness of the end results. To mitigate unintended outcomes, technological data analyzers must come with the ability to determine data accuracy and provide quality estimations to enable commanders to understand the risks they are accepting by using external data sources.

c. Common, standardized, shareable, and secure data is necessary, feasible, and achievable in the timeframe of this concept. Senior leaders must view data as a strategic asset that must be operationalized. As such, they must aggressively pursue and ruthlessly enforce Service adherence to established data criteria. While standardizing data, applications, and information systems to develop interoperability and a common user experience, the communications network maintains the flexibility to incorporate emergent technology quickly. The Army's future communications network must be linked and allow users to access and pull data or have relevant data pushed to them. Linked and accessible data allows users to manipulate and analyze that data, and create new, intuitive presentations to help commanders and staffs develop a shared understanding of operational and mission variables and the cause-and-effect relationships among them

H-4. Tailorable battlespace visualization
A tailorable battlespace visualization capability enables a shareable display of relevant information tailored to the user's requirements and based on common data and information from across one or more domains, the EMS, the IE, and warfighting functions. It allows for continuous shared situational understanding among all unified action partners. This future visualization capability can be easily filtered to each individual's security clearance and need to know.

Appendix I
The Command Post Constellation

I-1. Introduction
The future CPC is the variable arrangement of multiple, distributed, and meshed command nodes cross-functionally organized from home station to the close area. The multiple command nodes that form the future CPC are connected by the communications network. These command nodes provide the physical locations from where the C2 system's people meet (in person or virtually) to perform the functions, activities, processes, and procedures (see appendix K) that enable command

and control and the timely integration, dynamic synchronization, and optimal convergence of capabilities from all-domains with other elements of national power to accomplish mission objectives. All command nodes are able to seamlessly link to each other to form one cohesively-functioning CPC—though each node and the people within are designed and prepared to operate under the MC approach should communications be disrupted.

I-2. Functional characteristics of the future CPC

a. The future Army CPC is designed and engineered as a fully-integrated sociotechnical system of communications network capabilities, vehicles, shelters and workspace, information systems, power generation and distribution, and other ancillary equipment and supporting infrastructure capable of dividing into multiple command nodes dispersed around the extended battlespace but connected and operating as a unified whole. The future Army CPC is fielded as a comprehensive package that is formation and echelon appropriate and includes long-term education, training, and life-cycle sustainment strategies. To generate agility, support expeditionary Army forces, and realize the Army's MC approach, and enable C2, the Army's future command nodes are smaller, reduce physical and technical complexity, automate routine staff functions, decrease the cognitive burden on commanders and staffs, optimize human interaction and collaboration, and support self-forming teams. In future MDO, the CPC must be rapidly deployable, tactically mobile, tailorable, scalable, and survivable. To enable decision advantages, the future CPC facilitates the following functional characteristics.

b. *Rapidly deployable and tactically mobile*. The command nodes that comprise the future Army CPC are untethered from a fixed operating base. They are rapidly deployable, highly mobile, allowing quick set-up and tear-down in minutes rather than hours, and are vehicle-based or fully integrated at echelon into each formation's organic transportation to enhance mobility, deployability, survivability, and overall agility.[232] When needed, command nodes integrate easily into existing urban infrastructure or other fixed facilities. The future Army CPC is Soldier-operated and maintained with organic unit assets. Contractors or field service representatives are not required for installation and operation, including training and maintenance.[233] As part of the Army's continuing modernization and investment strategy, the future Army CPC minimizes size, weight, and power requirements and continuously takes advantage of advancements in miniaturization, cellular and wireless technologies, cloud-computing and data storage, mobile or wearable devices, lightweight protective materials, adaptive camouflage, and energy efficiencies and breakthroughs in sources, production, distribution, management, and storage.[234]

c. *Tailorable*. The future Army CPC is designed with common, standardized, and interchangeable components to support scalability (next imperative below), cross-leveling, minimizing supply-chain requirements, and training. These tailorable components contribute to agility. These uniform components can be added or removed to support combinations of decisive action from peacetime engagement to large-scale combat, rapid changes in task organization, and reconstitution. Tailorability supports the formation of a single, cohesive headquarters and staff from active and reserve component elements. While standardized, the future Army CPC maintains an open system architecture to allow rapid insertion of future technology innovations.

d. *Scalable*. The future Army CPC is composed of a flexible suite of systems tailored and configured to minimize the physical footprint and decrease threat detection while meeting enduring C2 functions and other demands driven by echelon, type of unit, task organization, specific mission requirements, and commanders' preferences.[235] Scalability includes a feature for ease of installation and employment on strategic and operational deployment platforms (air and sea), and immediate transition to or supplementation of an assault or early-entry command node to enable expeditionary maneuver and continuity of command. Tailorable components, a multi-path network transport layered within and among all of the domains, enhanced collaborative capabilities, and scalability allow commanders to tailor, echelon, and distribute their CPCs into appropriate command nodes positioned at multiple locations from home station to intermediate staging bases or other sanctuary locations, and throughout the area of operations to enable maneuver, increase protection, manage transitions between phases, sustain high-tempo operations, maintain continuity of command, and adapt to meet changing missions and situational demands.[236]

e. *Survivable*. Command nodes remain high-payoff targets for enemy forces particularly those possessing advanced intelligence, surveillance, reconnaissance, long-range fires, and offensive cyberspace and EW capabilities.[237] Ensuring the continuity and survivability of critical C2 functions and capabilities is obtained by balancing multiple materiel and non-materiel considerations. In turn, CPC survivability considerations must be balanced with maintaining effectiveness in performing essential C2 functions (see appendix K).

(1) To remain physically and functionally survivable, future command nodes must be able to—
- Avoid being detected and targeted.
- Work through and survive attacks.
- Rapidly recover from losses.

(2) Overlapping considerations that support CPC survivability include:
- Leaner and simpler design. Smaller components and infrastructure contribute to the mobility imperative discussed above. Leaner designs allow the establishment of the minimum footprint closest to the threat. Simplicity aids in command node construction and deconstruction (see next) and eases training.
- The ability to rapidly set up, tear down, and displace in minutes rather than days and hours. This contributes to overall mobility and dispersion.
- Hardening and protection from enemy and weather effects (the communications network and CPC infrastructure).[238]
- Camouflage and concealment. This includes reducing, obscuring, concealing, or otherwise managing or controlling the visual, thermal, radio frequency, acoustic, and seismic signatures. This requires commanders to be aware of their own signatures—observe, characterize, understand, and assess—as well as those of future threats.
- Tactical deception capabilities. This includes command nodes that can mimic other formations' signatures that may be of lesser value to the threat or blend into the surrounding environment. This may include coopting or sharing the use of civilian infrastructure. Remoting emitters deceives the threat as to the precise command node location. Tactical deception capabilities also include sacrificial decoys that mimic

command nodes and attract threat sensors, waste their time and other resources in locating and engaging them, and reduce their confidence in their own targeting ability.

- Intentional capability duplication and diversification among command nodes.[239]
- A resilient, multi-path network transport layered throughout all of the domains.
- The dispersion of the entire CPC into multiple nodes across the extended battlespace, the dispersion of the command nodes themselves within an area of operations, and other innovative employment tactics and techniques.[240]
- Routinely training command post operations under tough, realistic conditions of a near-peer threat to discover unit-specific strengths and weaknesses.

Appendix J
The Army C2 System Operating Across the Competition Continuum

J-1. Introduction

a. The Army's primary responsibility is to prepare future forces to fight and win the nation's wars in any environment, against any threat, and achieve decisive results across multiple domains and the entire competition continuum: competition, crisis response, armed conflict, and the return to competition. Successful future MDO require the application of the MC principles and the knowledgeable employment of the C2 system to achieve decision advantage. This includes a communications network that is simple for operators to establish and maintain, reliable, intuitive to the user, secure, and defended in all of the domains (including the EMS); that facilitates interoperability; and that ensures continuity of command. Similarly, it requires agile, expeditionary, and distributed locations—the command nodes that operate together as a unified CPC—from which to plan, prepare, execute, monitor, and assess MDO.

b. The future Army all-domain-capable C2 system allows commanders and staffs to frame and understand each mission, apply critical and creative thinking to developing a multi-domain operational approach, rapidly make sound, ethical decisions, and direct timely action to gain, maintain, and exploit the operational initiative. The future all-domain-capable C2 system allows commanders and staffs to continuously monitor operations; accurately assess effects and progress; and continuously adapt military action to changing circumstances quicker than opponents. As the primary engine of the C2 system, a new or modified operations process allows commanders and staffs—in cooperation with AI—to fully consider all of the domains, innovatively converge joint, multinational, and interorganizational capabilities to create windows of superiority in which to conduct cross-domain maneuver and employ lethal and nonlethal all-domain fires, and win decisively. Most importantly, the ability to develop and leverage the talents, abilities, and imaginations of every Soldier, Army Civilian, and mission partner allows future Army forces to out-think, out-maneuver, and out-fight any adversary on the complex, highly-competitive, and hyperactive physical and non-physical battlespace of the future.

J-2. Competition and crisis response

a. The Army succeeds in competition and crisis response by gaining, maintaining, and exploiting the operational initiative throughout the battlespace.[241] This is achieved in large measure

by maintaining sufficient capacity, capability, and readiness to win in MDO.[242] As a predominantly continental U.S.-based and expeditionary force, developing regionally-engaged, globally-responsive, and mission-tailorable units manned by competent leaders and Soldiers prepared to win any fight minimizes miscalculations by opportunistic threats who might otherwise choose to engage unprepared Army forces in a lethal contest of wills.

(1) While well-equipped units with significant technological overmatch are essential to preventing and deterring would-be opponents from engaging in conflict, future deterrence requires capable organizations manned by morally, intellectually, and physically strong leaders and Soldiers empowered with appropriate authorities and permissions and able to apply the MC approach.[243] Whether through the media or by personal observation, partners and threats recognize and respect the ability of Soldiers to act ethically and independently, take immediate action, and expertly employ the tools of warfare.

(2) Putting Soldiers in harm's way remains the greatest symbol of the nation's resolve and commitment. To maintain this military credibility, the Army trains and develops leaders who, with the appropriate authorities, think and operate across all of the domains, exercise disciplined initiative to develop the situation through action, adapt, and act decisively in uncertain and chaotic situations. The ability to easily converge landpower with other domain capabilities and other elements of national power rapidly delays, impedes, or halts the enemy's initial aggression, denies initial objectives, and ends crises earlier and on terms acceptable to U.S. authorities—often before any Soldiers' lives are lost.[244]

b. Partners are an integral factor in a properly calibrated force posture and the battlespace calculus that determines the appropriate capacity, capability, and readiness to confront future adversaries and gain, maintain, and exploit the operational initiative. As part of a whole-of-government approach to achieving national and theater objectives, the Army, working as interdependent, multifunctional teams of conventional and special operations forces, shapes OEs by establishing and sustaining strong alliances and partnerships with other militaries and supports their efforts to build the capacity necessary to protect and govern.[245] Developing partner capacity and interoperability during competition allows partners to compete on their own, serves as a deterrence, enables effective crisis response, and facilitates rapid transition to armed conflict if necessary.[246]

(1) As part of a long-term security investment strategy, sustained cooperative efforts with allies and other partners serve to gain, maintain, and exploit the operational initiative and provide early warning of developing crises (reducing the prospect of strategic surprise). Cooperative efforts also help deepen the Army's and joint force's overall situational understanding of the operational variables that, should prevention and deterrence fail, guide decision making and the development of operational approaches that lead to rapid, decisive victory.

(2) The careful integration of advanced communications capabilities allows Army forces to establish a virtual presence and virtual partnerships to build relationships well in advance of deployments, to maintain relationships between deployments, and, in some cases, to provide non-physical capabilities forward as a substitute for physical deployments. When conflict arises, strong, capable partners may preclude the employment of U.S. forces to key regions affecting

national interests and, if not, these partners may help facilitate operational access or share the responsibility and burden for creating a mutually beneficial outcome, or both.

c. Credible and timely public affairs coupled with sustained and persistent operations in the information environment, physical and virtual, communicate the reasons for U.S. involvement in a region and establish the long-term dialogue to develop and sustain partner relationships, win the battle for the information narrative, and consolidate gains. To be effective, Army leaders develop cultural acuity and strong interpersonal, communications, collaboration, and negotiation skills. Army forces apply knowledge management to harness information to create all-domain battlespace visualization; a tailorable battlespace visualization based on common, standardized, shareable, and secure data; and an overall shared understanding with and among unified action partners. Pervasive knowledge management helps build agile learning organizations, facilitates innovation and adaptation, and creates the unity of effort that leads to success.

J-3. Armed conflict

a. If unsuccessful in achieving strategic objectives in competition and crisis response, future Army commanders and their staffs employ the future C2 system to converge capabilities from all of the domains to fight and win on land and the airspace above; in and through space, cyberspace, the EMS, and the IE; and as part of cohesive joint, multinational, and interorganizational teams. Future Army forces project power outward from land in and through all of the domains and contested spaces to support joint force freedom of maneuver and action. Through effective employment of their C2 system, commanders create shared understanding of the environment, problems, and approaches to solving them. With the support of their staff, they employ their C2 system to rapidly produce, rehearse, and distribute mission orders with associated graphics between command nodes (ground, aerial, and waterborne platforms as well as dismounted leaders), and direct decisive action to break an enemy's will to continue the fight.

b. Army leaders, Soldiers, and organizations are grounded in military tactical and technical competencies and skilled in exercising MC to ensure decisive victory in armed conflict against any enemy. MC empowers subordinates to make rapid decisions to seize, retain, and exploit the operational initiative and succeed in sustained, high-tempo combat operations. Exercising MC, Army forces are able to continue to operate even under degraded space and network conditions and when geographically separated.

c. In future MDO, the joint force leverages Army expertise to attack and defeat threat systems and protect forces, weapon systems, logistics nodes (surface and air), and other critical infrastructure through expert system warfare analysis and the convergence of capabilities across all of the domains to create and exploit windows of superiority. Together with space, cyberspace, and EW operations to destroy, disrupt, degrade, deny, deceive, manipulate, and exploit in the IE, Army forces conduct sustained information warfare, including the skillful integration of operations security and effective military deception, to create disparity between the information quality available to friendly forces and that available to threats. At times during the campaign, future Army leaders conduct deliberate operations to restore information connectivity as the decisive operation.

d. Commanders and staffs apply knowledge management to tailor and organize their C2 system to generate cognitive synergy and an intellectual edge against future opponents. Army commanders and staffs use the future operations process to drive the conceptual and detailed planning necessary to integrate and synchronize capabilities from all of the domains and the Army's decisive action tasks as part of interoperable joint, multinational, and interorganizational teams. The future AI-enabled C2 system allows commanders and staff to better predict changing conditions and adapt to outpace and out-maneuver threats.[247] The future all-domain-capable C2 system also enables Army forces to dynamically task organize, shift capabilities, and direct action across the battlespace in response to changes in mission. When necessary, senior Army headquarters can seamlessly transition to a joint land force or a larger joint task force and immediately begin conducting joint all-domain operations.

e. The communications network enables the information sharing required for converging capabilities across all of the domains. It overcomes the enemy's ability to isolate nodes by maximizing all transport infrastructure available including U.S. military, unified action partner, civilian, and even enemy controlled network transport routes. To reduce the burden on available communications network resources, all capabilities dependent on the communications network are developed to use the minimal amount of data possible. In the event of unforeseen bandwidth bottlenecks, critical information automatically takes transmission priority during limited bandwidth situations.

f. A rapidly configurable, deployable, mobile, scalable, and survivable CPC, with capabilities that facilitate interoperability and sustain continuity of command, supports joint entry operations and echeloned maneuver. As command nodes will be high-payoff targets for the enemy, scalable and tailorable CPCs are able to be dispersed into smaller, more mobile command nodes while still operating together as a whole. Command nodes are distributed in the battlespace from home station to the forward edge of the battle area with the minimal footprint forward. In addition to the protection afforded by being more mobile, future command nodes are physically and electronically less visible to threat sensors making them more survivable. Essential C2 capabilities are appropriately redundant among the multiple command nodes to ensure continuity of command should one node be discovered and targeted. The mobile command group allows the commander to move about and see the battlespace to gain a personal understanding of the situation and lead forces, while maintaining connectivity with other command nodes. If needed, the mobile command group can "dock" with any other command node (or even subordinate command nodes) when commanders require greater C2 capability than they have while on the move.

J-4. Return to competition

a. Commanders and staffs, in coordination with unified action partners and other key organizations operating in the battlespace, begin planning for return to competition coincident with planning for armed conflict. Many of the activities required for successful transition back to competition from a position of advantage occur in consolidation areas during armed conflict where future Army forces first began to maintain or reestablish a safe and secure environment to allow the restoration, development, or provision of essential governmental services, humanitarian relief, and emergency infrastructure reconstruction.

b. The Department of State is the overall lead federal agency for U.S. stabilization efforts and the DOD is a critical supporting element. Cohesive civil-military operations are essential to these efforts during MDO across the competition continuum. Army and joint force commanders—executing transitional military authority with civil affairs forces and other enablers in liberated or occupied areas during and immediately following large-scale combat—take steps to set conditions for transfer of governance responsibilities to a transitional civil authority or other authority as early as possible. Steps to transfer authority include civil affairs forces and engineers conducting detailed civil infrastructure assessments and, based on those assessments and in conjunction with unified action partners, developing, synchronizing, and executing appropriate remediation. Transfer of authority measures also include governance and rule of law tasks to support the establishment or reestablishment of a stable, credible, and legitimate host-nation government. In the return to competition, civil-military operations are key to making previously hard-fought gains more enduring.

Appendix K
Common C2 Functions, Activities, and Tasks

K-1. Introduction
Command and control is the lawful exercise of authority derived from rank or assignment to direct the efforts of assigned and attached forces and utilize resources to accomplish tasks. Command and control includes the responsibility for planning the employment of, organizing, directing, coordinating, controlling, and leading forces for the accomplishment of assigned missions. It also includes the responsibility for subordinates' health, welfare, morale, and discipline. The procedural engine that powers every organization is the overall operations process: plan, prepare, execute, monitor, and assess.[248] Commanders drive the operations process through their personal command activities of understanding, visualizing, describing, directing, leading, and assessing. To this end, the future Army CPC enables a set of general, often overlapping, functions, activities and supporting tasks common to any operation across the competition continuum.[249]

K-2. General functions, activities, and supporting tasks

a. *Creating comprehensive shared understanding with higher, lower, adjacent, supporting, and supported units, and other unified action partners*.

(1) Generating, distributing, or sharing information and knowledge products including reports required by higher headquarters.

(2) Collecting and receiving data and information from humans and technological sensors, including the information and reports from subordinate units.

(3) Analyzing data and information to produce actionable information and intelligence.

(4) Establishing a comprehensive, tailored battlespace visualization based on common, standardized, shareable, and secure data from across all of the domains and warfighting functions.

(5) Building, operating, and defending the Army's communications network.

(6) Ensuring a thorough understanding of the commander's intent and concept of operations.

(7) Conducting updates and informing the organization on critical issues so they may adjust plans as required.

(8) Informing the public and responding to specific requests for information.

b. *Planning operations (long- and short-range).*[250]

(1) Planning branches and sequels.

(2) Integrating intelligence and critical sustainment considerations into current operations and future plans.

(3) Planning, prioritizing, and sequencing targets and determining appropriate method(s) of engagement.

(4) Avoiding unnecessary conflict and duplication of effort among units and unified action partners.

(5) Planning and managing sustainment.

(6) Determining protection priorities.

(7) Determining and managing risk.

c. *Integrating and synchronizing resources and capabilities across multiple domains.*

(1) Resourcing subordinates with the combat power—all constructive, destruction and information capabilities—needed to accomplish assigned missions.

(2) Prioritizing support and weighting the decisive action or main effort.

(3) Obtaining and providing appropriate decision-making authorities and permissions to allow disciplined initiative.

(4) Integrating and synchronizing all available intelligence, surveillance, reconnaissance, and security for information collection.

(5) Synchronizing airspace management and area air defense plans and orders with the joint force air component commander and other partner airspace users.

(6) Creating unity of effort among unified action partners and interorganizational organizations operating in the area of operation not under military command.

d. *Orchestrating and controlling operations*.

(1) Establishing appropriate command and support relationships with necessary authorities and permissions among subordinate commanders. This includes establishing the chain of command.

(2) Providing timely adjustments to the current operation in response to immediate changes in the OE and fleeting opportunities.

(3) Providing responsive airspace management.

(4) Providing clear rules of engagement.

(5) Orchestrating the convergence of capabilities from all of the domains to achieve physical, cognitive, temporal, and virtual windows of superiority in decisive spaces.[251]

e. *Monitoring and assessing operations and effects in all of the domains and warfighting functions, and their impact on future operations*.

(1) Conducting running estimates and after action reviews.

(2) Tracking the battle and conducting battle damage assessments.[252]

(3) Conducting protection assessments.

(4) Making anticipatory and proactive recommendations to the commander.

Glossary

The glossary contains acronyms and terms with Army or joint definitions. Terms unique to or modified by this concept are marked with an asterisk (*).

Section I
Abbreviations and acronyms

ADP	U.S. Army doctrine publication
AFC	U.S. Army Futures Command
AFCC-C2	Army Futures Command Concept for Command and Control
AI	artificial intelligence
AP	U.S. Army Futures Command pamphlet
AR	Army regulation
ASA(ALT)	U.S. Assistant Secretary of the Army for Acquisition, Logistics, and Technology
ATP	U.S. Army techniques publication
BCT	brigade combat team
BCT-CDM	Army Futures Command Concept for Brigade Combat Team Cross-Domain Maneuver
CAC	U.S. Army Combined Arms Center
CCDC	U.S. Army Combat Capability Development Command
CoE	center of excellence
CP	command post
CPC	command post constellation
CTC	combat training center
DA	Department of the Army
DOD	Department of Defense
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
DSCA	defense support of civil authorities
EAB	echelons above brigade
EMS	electromagnetic spectrum
EW	electromagnetic warfare
FCC	U.S. Army Futures and Concepts Center
FM	U.S. Army field manual
G-6	assistant chief of staff, signal
IE	information environment
ISR	intelligence, surveillance, and reconnaissance
JADC2	joint all-domain command and control
JP	joint publication
JTF	joint task force
Li-Fi	light fidelity
LOE	line of effort
MC	mission command
MCCoE	U.S. Army Mission Command Center of Excellence
MDO	U.S. Army Concept for Multi-Domain Operations 2028
ML	machine learning

MMDO	Army Futures Command Concept for Maneuver in Multi-Domain Operations 2028
OE	operational environment
RC	required capability
S&T	science and technology
TP	U.S. Army Training and Doctrine Command pamphlet
TRADOC	U.S. Army Training and Doctrine Command
U.S.	United States

Section II
Terms

adversary
A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

*agility
Flexibility of mind and an ability to anticipate and adapt to uncertain or changing situations.

airspace control
Capabilities and procedures used to increase operational effectiveness by promoting the safe, efficient, and flexible use of airspace. (JP 3-52)

airspace control system
An arrangement of those organizations, personnel, policies, procedures, and facilities required to perform airspace control functions. (JP 3-52)

airspace coordinating measures
Measures employed to facilitate the efficient use of airspace to accomplish missions and simultaneously provide safeguards for friendly forces. (JP 3-52)

airspace management
The coordination, integration, and regulation of the use of airspace of defined dimensions. (JP 3-52)

*all-domain fires
The ability to integrate and deliver lethal and nonlethal fires in and across all five domains (land, maritime, air, space, and cyberspace), the electromagnetic spectrum, and the information environment to create windows of superiority (Adapted from MDO Concept's cross-domain fires definition)

*Army's communications network
The Army's interoperable contribution to the Department of Defense communications network encompassing all Army communications capabilities and associated procedures for collecting, processing, storing, displaying, disseminating, managing, and protecting data and information worldwide. (Adapted from ATP 6-02.71)

*artificial intelligence
An artificial creation of human-like intelligence that can learn, reason, plan, perceive, or process natural language.

*battlespace
The physical and non-physical spaces where military operations are conducted to achieve military goals consisting of all of the domains (air, land, maritime, space, and cyberspace), the electromagnetic spectrum, and the information environment (including human cognitive aspects). It includes factors and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission, including enemy and friendly armed forces, infrastructure, weather, terrain, and civilian populations within the operational areas and areas of interest. (Modified from the MDO Concept's definition for battlefield)

*big data
Extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions.

*cognition
The mental action or process of acquiring knowledge and understanding through, thought, experience, and the senses.

cognitive dimension
Dimension of the information environment within the minds of those who are affected by and act upon information. (Maneuver in Multi-Domain Operations Concept)

*cohesion
The bonding together of members of an organization through shared experiences in such a way as to sustain their will and commitment to each other, their unit, and the mission.

*collaborative planning
Commanders, subordinate leaders, staffs, and other trusted partners vertically and horizontally planning together in real time, sharing data, information, knowledge, perceptions, and ideas, regardless of physical location, to develop their respective plans simultaneously.

combat power
The total means of destructive, constructive, and information capabilities that a military unit or formation can apply at a given time. (ADP 3-0)

*combined arms
The synchronized and simultaneous application of all elements of combat power to achieve an effect greater than if each element was used separately or sequentially. (Adapted from ADP 3-0 definition)

*command and control (v)

Lawfully exercising authority derived from rank or assignment, directing the efforts of assigned and attached forces, and utilizing resources to accomplish tasks. Command and control includes the responsibility for planning the employment of, organizing, directing, coordinating, regulating, and leading forces and applying combat power for the accomplishment of assigned missions. It also includes responsibility for subordinates' health, welfare, morale, and discipline. (Created from JP 1 definitions for command and command and control)

*command and control system
The arrangement of people, the operations and associated integrating processes, the communications network, and a command post constellation, optimally organized through knowledge management into appropriate command node configurations for a specific organization and mission, which enables the exercise of command and control. (Adapted from ADP 6-0 definition)

*command and control warfighting function
The system and related tasks that enable commanders to understand, visualize, and describe the OE, problems, and approaches to solving them; make and articulate rapid, quality decisions; direct and lead forces; and monitor and assess operations. The command and control warfighting function aids commanders in regulating and converging all elements of combat power across all of the domains, the electromagnetic spectrum, and the information environment and with all instruments of national power to accomplish assigned missions and achieve objectives. (Adapted from ADP 3-0 definition)

*commander's intent
A clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus for the staff, and helps subordinates and supporting commanders act to achieve the commander's desired results without further orders, even when communications are degraded and the operation does not unfold as planned. (Adapted from JP 3-0 definition)

commander's visualization
The mental process of developing situational understanding, determining a desired end state, and envisioning an operational approach by which the organization will achieve that end state. (ADP 6-0)

*command post constellation
The variable arrangement of multiple, distributed, and meshed command nodes cross-functionally organized from home station to the close area from which commanders and their staffs perform their command and control functions, activities, processes, and procedures. Based on the situation, commanders determine the number of physical and virtual dispersed command nodes acting with unity of command and effort. (Adapted from FM 6-0 definition)

common operating environment
Approved set of computing technologies and standards that enable secure and interoperable applications to be developed rapidly and executed across a variety of computing environments.

(U.S. Army Chief Information Officer/G-6 Annex B to LandWarNet 2020 and Beyond Enterprise Architecture Version 2.0: Definitions and Guidance for the Common Operating Environment)

*common, standardized, shareable, and secure data
Common data is data that is synchronized to ensure that all users see the same representation of reality. Common data is authoritative and available to all users at the speed available through the communications network. *Standardized data* is a data storage schema that includes data form, format, structure, tagging, domain values, and semantics. *Shareable data* is data that can be discovered, accessed, understood, and transformed into a digestible format to internal and external users without changing the intent of the representation, including any mission partner or legacy system not compliant with standardized data models. *Secure data* is data that is protected against unauthorized use and manipulation.

competition continuum
Enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict. (Joint Doctrine Note 1-19)

computing environment
Logical grouping of systems with similar characteristics used to organize the [common operating environment] (deployment, echelonment, environmental, transport dependencies, form factors, and others.) A computing environment comprises the necessary hardware, operating system, libraries, and software required to run applications within the [common operating environment]. (U.S. Army Chief Information Officer/G-6 Annex B to LandWarNet 2020 and Beyond Enterprise Architecture Version 2.0: Definitions and Guidance for the Common Operating Environment)

control
The regulation of forces and warfighting functions to accomplish the mission in accordance with the commander's intent. (ADP 6-0)

control measure
A means of regulating forces or warfighting functions. (ADP 6-0)

*convergence
Rapid and continuous integration of capabilities in all domains, the electromagnetic spectrum, and information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative. (Adapted from MDO Concept definition)

cross-domain
Having an effect from one domain into another. (MDO Concept)

cross-domain maneuver
The synchronization and employment of forces and capabilities through movement in combination with converged lethal and nonlethal capabilities across multiple domains, the electromagnetic spectrum, and the information environment. Cross-domain maneuver creates synergistic effects in the physical, cognitive, temporal, and virtual realms that increase relative combat power and

provides the overmatch necessary to destroy or defeat enemy forces, control land areas and resources, and protect populations. (U.S. Army Concept for Brigade Combat Team Cross-Domain Maneuver)

*decentralized
The delegation of authority, information, warfighting capabilities, and other resources to subordinates at the lowest practical level which enables aggressive, independent, and disciplined initiative to develop the situation; seize, retain, and exploit the initiative; and cope with uncertainty to accomplish the mission within Army professional ethics and the commander's intent.

*decision advantage
Acquiring timely and accurate information to gain accurate situational understanding, translating that understanding into quality decisions, and disseminating those decisions rapidly in a useable and shareable format thereby allowing subordinates to take action at a speed and scale that adversaries are unable to match and achieve the operational initiative. (Adapted from Decision Advantage Discussion in Draft DOD Joint All-Domain Command and Control Vision)

decision dominance
A desired state in which commanders sense, understand, decide, act, and assess faster and more effectively than their adversaries. (CSA Paper #1)

decision point
A point in space and time when the commander or staff anticipates making a key decision concerning a specific course of action. (JP 5-0)

decisive action
The continuous, simultaneous execution of offensive, defensive, and stability operations or defense of civil authorities tasks. (ADP 3-0)

*decisive space
Conceptual geographic and temporal location where the full optimization of the employment of capabilities from all of the domains generates a marked advantage over an enemy and greatly influences the outcome of an operation. (Adapted from MDO Concept)

*Department of Defense communications network
The set of communications capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (Modified from Department of Defense information network definition in JP 6-0)

*disciplined initiative
The duty and willingness to act in accordance with Army professional ethics and the commander's intent without orders, when existing orders no longer fit the situation, or when unforeseen opportunities or threats arise.

dis-integrate
Break the coherence of the enemy's system by destroying or disrupting its subcomponents (such as command and control means, information collection, critical nodes, etc.) degrading its ability to conduct operations while leading to a rapid collapse of the enemy's capabilities or will to fight. (MDO Concept)

*dispersion
Deliberate or accidental reaction to adversary capabilities to spread out or break up forces, reduce the targetable mass of friendly forces, more effectively cover terrain in an area of operations, and gain operational and tactical flexibility.

domain
Area of activity within the operating environment (land, air, maritime, space, and cyberspace) in which operations are organized and conducted. (MDO Concept)

*early-entry command node
Lead element of a headquarters designed to control operations until the remaining portion of the deployed headquarters arrives and becomes operational. The early-entry command node could be the only portion of the headquarters command post that is deployed. (Adapted from FM 6-0 definition)

echeloned maneuver
Army air-ground movement in depth supported by ground fires along with air, maritime, space and cyberspace generated effects to gain positions of advantage, penetrate adversary defenses, and conduct exploitation. (Maneuver in Multi-Domain Operations Concept)

electromagnetic spectrum
The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 3-85)

electromagnetic warfare
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-85)

enclave
A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (National Security Agency Committee on National Security Systems Instruction [CNSSI] 4009)

enemy
A party identified as hostile against which the use of force is authorized. (ADP 3-0)

*emotional intelligence

Capacity to be aware of, control, and express emotions, and handle interpersonal relationships judiciously and empathetically; a component of social intelligence. (Adapted from Merriam-Webster Online Dictionary definition)

*expeditionary maneuver
The rapid deployment of task-organized multi-domain forces able to transition quickly to conduct operations of sufficient scale and ample duration to achieve strategic objectives. (Adapted from MDO Concept)

force tailoring
The process of determining the right mix of forces and the sequence of their deployment in support of a joint force commander. (ADP 3-0)

flexibility
The employment of a versatile mix of capabilities, formations, and equipment for conducting operations. (ADP 3-0)

function
A practical grouping of tasks and systems (people, organizations, information, and processes) united by a common purpose. (ADP 1-01)

globally-integrated operations
Operations arranged as cohesive military actions in time, space, and purpose, executed as a whole to address transregional, all domain, and multi-functional challenges. (MDO Concept)

hyperactive
More active than usual or desirable; hyper-competitive during competition and hyper-violent in armed conflict. (MDO Concept)

information
In the context of decision making, data that has been organized and processed in order to provide context for further analysis. (ADP 6-0)

information advantage
The application of information capabilities, including space, cyberspace, EMS, and influence, resulting in comparative advantage to support all-domain operations. It includes intense targeting of adversary command and control, intelligence, surveillance, reconnaissance, and targeting. In the decision cycle, information advantage provides the ability to acquire, process, and present contextually relevant information from across all domains for action faster than an opponent. (AFC Concept for Operations in the Information Space: Cyber and Electronic Warfare)

information environment
The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information management

The science of using procedures and information systems to collect, process, store, display, and protect data, information, and knowledge products. (ADP 6-0)

*information warfare
The integrated employment of information activities and capabilities along with other lines of operation to coerce, disrupt, corrupt, or usurp threat decision making while protecting U.S. capabilities. (Adapted from JP 3-13 definition of information operations)

*institutionalize
To deliberately translate an organization's code of conduct, mission, policies, vision, and strategic plans into guidelines and practices applicable to the daily activities of its leaders and subordinates; integrate fundamental values and objectives into the organization's culture, structure, and operating capabilities. (Adapted from Merriam-Webster Online Dictionary definition)

integration
The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 1)

interoperability
The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (AR 34-1)

interorganizational
Includes U.S. government departments and agencies; state, territorial, local, and tribal government agencies; foreign military forces and government agencies; international organizations; nongovernmental organizations; and the private sector. (Maneuver in Multi-Domain Operations Concept)

joint all-domain command and control
Secure environment, composed of shared [information technology] infrastructure, enterprise services, and a single security architecture, to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize [information technology] efficiencies. (Deputy Secretary of Defense Joint All-Domain Command and Control Cross Functional Team Establishment Memorandum, Jan 31, 2020)

joint information environment
Secure environment, composed of shared [information technology] infrastructure, enterprise services, and a single security architecture, to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize [information technology] efficiencies. (DOD Instruction 8320.02)

knowledge
In the context of decision making, information that has been analyzed and evaluated for operational implications. (ADP 6-0)

knowledge management

The process of enabling knowledge flow to enhance shared understanding, learning, and decision making. (ADP 6-0)

leader development
Deliberate, continuous, sequential, progressive process—founded in Army values—that grows Soldiers and Army Civilians into competent and confident leaders capable of decisive action, and achieved through the life-long synthesis of the knowledge, skills, and experiences gained through the training and educational opportunities in the institutional, operational, and self-development domains. (AR 350-1)

*machine learning
Machine learning is a field of computer science that aims to teach computers how to learn and act without being explicitly programmed for a specific result. Specifically, machine learning is an approach to data analysis that involves building and adapting models and algorithms that are able to improve prediction or conclusion accuracy as they process more datasets. Although seen as a subset of artificial intelligence, machine learning has a larger application outside of the strict definition of artificial intelligence.

maneuver
The employment of forces through movement in combination with lethal and nonlethal effects across multiple domains, the electromagnetic spectrum, and the information environment to destroy or defeat enemy forces, control land areas and resources, and protect populations. (Maneuver in Multi-Domain Operations Concept)

*mesh
To connect nodes or devices directly, dynamically, and non-hierarchically to as many other nodes or devices as possible allowing them to relay critical data without interruption and cooperate, self-organize, and self-configure to accomplish tasks collectively despite individual node or device degradation or destruction. (Modified from the definition in the EAB Concept)

military deception
Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 3-13.4)

mission command
The Army's approach to command and control that empowers subordinate decision making and decentralized execution appropriate to the situation. (ADP 6-0)

mission orders
Directives that emphasize to subordinates the results to be attained, not how they are to achieve them. (ADP 6-0)

mission partner environment
Capability framework in which combatant command partners plan, prepare and execute operations at an appropriate, single security classification level, with a common language. It provides

strategic, operational, and tactical flexibility for all commanders to execute C2 by providing the means to clearly communicate the commander's intent to achieve maximized operational effects with all mission partners. (AR 34-1)

mission variables
Categories of specific information needed to conduct operations. (ADP 1-01)

*mobile command group
The commander and selected staff members who assist the commander in controlling operations away from other, relatively-stationary, command nodes. (Adapted from FM 6-0 definition)

multi-domain formations
Army organizations possessing the combination of capacity, capability, and endurance necessary to operate across multiple domains in contested spaces against a near-peer adversary. (MDO Concept)

multi-domain operations (MDO)
Operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture; employment of multi-domain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives. (MDO Concept)

*multi-form collaboration
Sharing thoughts and thought processes between superiors, subordinates, and peers in the form of sketching, highlighting, talking, listening and gesturing through voice and voice recognition, text, chat, data, video, white boarding, map boarding, messages, and other shared applications.

multinational
Between two or more forces or agencies of two or more nations or coalition partners. (JP 5-0)

*national power
All resources available to a nation in the pursuit of national objectives, including diplomatic, informational, military, economic, financial, intelligence, and law enforcement elements. (Adapted from JP 1 definition)

*network operations
Activities conducted to operate and defend the DOD communication network. (Adapted from JP 6-0 definition)

*node
An element of a system that represents a person, place, or physical thing. (Adapted from JP 3-0)

network transport
The processes, equipment, and transmission media that provide connectivity and move data between networking devices and facilities. (FM 6-02)

operational environment
A composite of conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

operational initiative
Setting the tempo and terms of action throughput an operation. (ADP 3-0)

operational variables
Comprehensive set of information categories used to define an operational environment. (ADP 1-01)

*operations in the information environment
Actions taken to generate, preserve, and apply informational power toward a relevant actor in order to inform or influence that actor and increase or protect a competitive advantage or combat power potential within the operating environment. (Modified from DRAFT DepSecDef Memo, IE and OIE, 29 Jan 20)

*operations process
The major command and control activities performed during operations: planning, preparing, executing, and continuously monitoring and assessing the operation. (ADP 5-0)

overmatch
Application of capabilities or unique tactics either directly or indirectly, with the intent to prevent or mitigate opposing forces from using their current or projected equipment or tactics. (MDO Concept)

parallel planning
Two or more echelons planning for the same operations nearly simultaneously facilitated by the use of warning orders by the higher headquarters. (ADP 5-0)

planning
The art and science of understanding a situation, envisioning a desired future, and determining effective ways to bring that future about. (ADP 5-0)

planning horizon
A point in time commanders use to focus the organization's planning efforts to shape future events. (ADP 5-0)

position of relative advantage
A location or the establishment of a favorable condition within the area of operations that provides the commander with temporary freedom of action to enhance combat power over an enemy or influence the enemy to accept risk and move to a position of disadvantage. (ADP 3-0)

preparation

Those activities performed by units and Soldiers to improve their ability to execute an operation. (ADP 5-0)

principle
A comprehensive and fundamental rule or an assumption of central importance that guides how an organization or function approaches and thinks about the conduct of operations. (ADP 1-01)

*protection assessment
An assessment that provides the commander an understanding of threat activities; what capabilities, assets, and activities are critical and likely targeted by the threat; and what actions and resources are required to counter and preserve combat power.

public affairs
Those public information, command information, and community engagement activities directed toward both the external and internal publics with interest in the Department of Defense. (JP 3-61)

range of military operations
Activities, tasks, missions, and operations along the competition continuum from peace to war that vary in purpose, scale, risk, and combat intensity and which can be grouped into military engagement, security cooperation, and deterrence; crisis response and limited contingency operations; and large-scale combat operations. (EAB Concept)

reach
Collaboration, information sharing, and capability integration with any organization and/or individuals, regardless of location, echelon, or affiliation. (CAC & ARCIC The Mission Command Network: Vision & Narrative.)

reachback
Process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 3-30)

regionally-aligned forces
Army units assigned to combatant commands, allocated to a combatant command, and those capabilities service retained, combatant command aligned, and prepared by the Army for combatant command missions. (MDO Concept)

relevant information
All information of importance to the commander and staff in the exercise of command and control. (ADP 6-0)

*resiliency
The ability of an architecture to support the functions necessary for mission success in spite of hostile action or adverse conditions. An architecture is considered "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, or across a wider range of scenarios, conditions, and threats.

*shared understanding
A collaboratively-developed and shared mental model of the environment, problems, and approaches to solving them. (Adapted from ADP 6-0 discussion)

situational understanding
The product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables. (ADP 6-0)

*social intelligence
Ability to effectively negotiate complex social environments and form rewarding relationships with others. (Adapted from Merriam-Webster Online Dictionary definition)

*sociotechnical
The careful and thoughtful integration of humans and technology so that technology compliments human attributes—cognitive and physical—for greatest benefit.

stand-off
The physical, cognitive, and informational separation that enables freedom of action in any, some, or all domains, the electromagnetic spectrum, and information environment to achieve strategic and/or operational objectives before an adversary can adequately respond. It is achieved with both political and military capabilities. (MDO Concept)

survivability
Quality or capability of military forces which permits them to avoid or withstand hostile actions or environmental conditions while retaining the ability to fulfill primary mission. (ATP 3-37.34)

synchronization
The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. (JP 2-0)

*synthetic training environment
Convergence of virtual, constructive, gaming, and augmented reality training environments into a single training environment capable of interacting and augmenting live training to provide a cognitive, collective, multi-echelon training and mission rehearsal capability for the operational, institutional, and self-development training domains.

*system
A group of interacting, interrelated, and interdependent components or subsystems (people. processes, and tools) that form a complex and unified whole. Systems have a purpose with their parts arranged in a way (structure) to carry out their purpose.

tailor
To provide the warfighting capabilities required for the situation and mission. (EAB Concept)

*tailorable battlespace visualization

A shareable display of relevant information tailored to the user's requirements and based on common data and information from across one or more domains, the EMS, the IE, and warfighting functions. (Adapted from the definition of common operational picture in ADP 6-0)

*talent management
Deliberate and coordinated process to optimize leader development practices and align talent with current and future requirements to improve the individual, the organization, and the Army as a whole. Talent management is informed by the mission command approach and is complementary to leader development.

*task organization
A temporary grouping of unified action partners designed to accomplish a particular mission or pursue a mutual line of effort. (Adapted from ADP 5-0 definition)

*task-organizing
The act of designing a force or organization, support staff, or sustainment package of specific size and composition to meet a unique task, mission, or line of effort. (Adapted from ADP 3-0)

tempo
The relative speed and rhythm of military operations over time with respect to the enemy. (ADP 3-0)

*threat
Any combination of environmental factor, actors, entities, or forces that could harm United States forces, United States national interests, or the homeland. (Adapted from ADP 3-0 definition)

unified action
The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1)

unified action partners
Those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations. (ADP 3-0)

*warfighting function
A group of tasks united by a common purpose and a supporting system (people, processes, and tools) that commanders use to accomplish missions and training objectives. (Adapted from ADP 3-0 definition)

windows of superiority
Converging capabilities in time and space in selected domains and environments to enable commanders to gain localized control or physical, virtual, and/or cognitive influence over a specified area to prevent its use by an enemy or to create conditions necessary for successful friendly operations. (MDO Concept)

Endnotes

[1] The *Army Futures Command Concept for Command and Control 2028: Pursuing Decision Dominance*, hereafter referred to as the AFCC-C2, approaches command and control as a series of commander-related activities and responsibilities and defines it as lawfully exercising authority derived from rank or assignment, directing the efforts of assigned and attached forces, and utilizing resources to accomplish tasks. Command and control includes the responsibility for planning the employment of, organizing, directing, coordinating, regulating, and leading forces and applying combat power for the accomplishment of assigned missions. It also includes responsibility for subordinates' health, welfare, morale, and discipline. Multi-Domain Operations (MDO) are "operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture; employment of multi-domain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives." TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, p. GL-7, hereafter referred to as the MDO Concept.

[2] "The *U.S. Army Concept for Multi-Domain Combined Arms at Echelons Above Brigade, 2025-2045* calls for formations able to integrate, synchronize, and converge all elements of combat power across all the domains, the EMS, and the IE to execute cross-domain maneuver; provide essential linkage to the expanded instruments of national power; and operate ubiquitously with joint, interagency, and multinational partners to overmatch any threat in any future environment." MDO Concept, p. x, footnote 8. The MDO Concept defines convergence as the rapid and continuous integration of capabilities in all domains, the electromagnetic spectrum, and information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative.

[3] Joint Doctrine Note 1-19 defines competition continuum as "enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict."

[4] "The intellectual foundation for building tomorrow's military force rests on the unfounded assumption that technologies emerging from the 'information revolution' will lift the fog of war and permit U.S. forces to achieve a very high degree of certainty in future military operations….The first step is to abandon explicitly the assumptions that future war will lie mainly in the realm of certainty and that American forces will be able to achieve and maintain information dominance during combat operations." McMaster, H. (2003, April 7). *Crack in the Foundation: Defense Transformation and Underlying Assumption of Dominant Knowledge in Future War*. U.S. Army War College Strategy Research Project. Carlisle Barracks, PA, pp 1-2. "Fog of war" is a term used to describe ambiguity experienced by participants in military operations. It is ascribed to the Prussian military theorist Carl von Clausewitz, who wrote: "The great uncertainty of all data in war is a peculiar difficulty, because all action must, to a certain extent, be planned in a mere twilight, which in addition not infrequently—like the effect of fog or moonshine—gives to things exaggerated dimensions and unnatural appearance." von Clausewitz, C. (1975). *On War*. (Ed. and trans. Michael Howard and Peter Paret). NJ: Princeton University Press. Book 2, chapter 2, para 24.

[5] ADP 3-0 defines operational initiative as "setting the tempo and terms of action throughout an operation" and tempo as "the relative speed and rhythm of military operations over time and with respect to the enemy." Operational initiative encompasses all levels of warfare: tactical, operational, and strategic.

[6] Quality decisions are logical, pragmatic, and justified by the information and intelligence available at the time of decision. Quality decisions are based on a combination of analysis and intuition. However, intuitive aspects are not based in emotions but grounded in doctrinal theory, relevant experience, ethical principles, and consideration of intangibles such as subordinate leadership and unit morale. Quality decisions reflect an understanding of all available capabilities in all the domains and dimensions from both a friendly and enemy perspective. Quality decisions account for risk and allow for recovery from failure. Quality decisions do not create new, unapproved risk to higher commanders' plans. Quality decisions facilitate effective action even in the face of unforeseen events. Quality decisions are easier to understand and explain in terms of how they accomplish the higher commanders' intent and assigned mission or, more generally, how they lead to solving problems.

[7] See Ancker, C. (2013, March-April). The evolution of mission command in U. S. Army doctrine, 1905 to the present. Military *Review,* pp. 42-52.

[8] See ADP 6-0, p. vii. "Clarifying command is more than just nitpicking. Clarity about what kind of command is in use—or should be used—can inform better decisions about force modernization, training, what kind of technology to acquire, personnel management, and what changes are needed to implement mission command." Friedman, B. & Garard, A. (2020, April 7). Clarifying command: Keeping up with the (John Paul) Joneses. *War On the Rocks*.

[9] The AFCC-C2 later modifies the labels and descriptions of two of these components (networks to communications network and command posts to the command post constellation).

[10] The AFCC-C2 defines the C2 system as the arrangement of people, the operations and associated integrating processes, the communications network, and a command post constellation, optimally organized through knowledge management into appropriate command node configurations for a specific organization and mission, which enables the exercise of command and control.

[11] Commander's intent and a concept of operations are forms of control.

[12] See DA. (2020, November 6). *U.S. Army Mission Command Network Implementation Plan Volume 1—Framework*.

[13] MDO Concept, p. A-1 and EAB Concept, pp. 6-8.

[14] The MDO Concept defines calibrated force posture as "the combination of position and ability to maneuver across strategic distances. It includes, but is not limited to, basing and facilities, formations and equipment readiness, the distribution of capabilities across components, strategic transport availability, interoperability, access, and authorities." MDO Concept, p. GL-2. The MDO Concept defines expeditionary maneuver as "the rapid deployment of task-organized combined arms forces able to transition quickly to conduct operations of sufficient scale and ample duration to achieve strategic objectives." MDO Concept, p. GL-5.

[15] "While the Army fights alongside the Navy, Air Force, Marines, Coast Guard, and our allies, the Nation also relies on a ready Army to provide unique capabilities for the Nation's defense. Unique to the Army is the ability to conduct sustained land campaigns in order to destroy or defeat an enemy, defend critical assets, protect populations, and seize positions of strategic advantage. Additionally, as the foundation of the Joint Force, the Army provides critical capabilities—command and control, communications, intelligence, logistics, and special operations—in support of Joint operations." Murphy, P. & Milley, M. (2016, April 7). [Record Version]. Statement by the Honorable Patrick J. Murphy, Acting Secretary of the Army and General Mark A. Milley, Chief of Staff United States Army before the Committee on Armed Services United Sates Senate. Washington, DC, p. 5.

[16] "From its global perspective, the [National Military Strategy] premises an adaptive and innovative Joint Force capable of employing its capabilities seamlessly across multiple regions and all domains—continuing the transition from a regional to a global mindset and approach." DOD, The Joint Staff. (2018). Description of the National Military Strategy 2018 (hereafter referred to as 2018 NMS Description), p. 2.

[17] The MDO Concept defines overmatch as "the application of capabilities or unique tactics either directly or indirectly, with the intent to prevent or mitigate opposing forces from using their current or projected equipment or tactics." MDO Concept, p. GL-7.

[18] The MDO and other concepts use the term *cross-domain fires*. While the ability to shoot or employ capabilities across domains is essential, the AFCC-C2 seeks to emphasize that Army forces need to be able to employ capabilities from *all available domains* to create windows of superiority. Hence, the AFCC-C2 uses *all-domain fires* and defines it as the ability to integrate and deliver lethal and nonlethal fires in and across all five domains (land, maritime, air, space, and cyberspace), the electromagnetic spectrum, and the information environment to create windows of superiority

[19] "Defining convergence is critical: it is the ability to enable any shooter, with any sensor, through any headquarters with the right authorities, in near real time. It has two essential characteristics: 1) recognizing that it is cost-prohibitive to invest enough money in individual domains to dominate in each independently, it relies on the idea of integrating all five domains in decisive space such that the "total effect is greater than the sum of the parts," thus creating overmatch; 2) because the U.S. Army will be challenged in all domains and exquisite linear kill chains will be defeated, convergence must exhibit resilience and have the ability to leverage alternate or multiple pathways to achieve the same effect. Both of these must be achieved rapidly and continuously in order to enable convergence." Wesley, E. & Simpson, R. (2020, April). Expanding the battlefield: An important fundamental of multi-domain operations. *Land Warfare Paper*, (131). Arlington, VA: Association of the United States Army, p. 5.

[20] See MDO Concept, p. 21.

[21] "It is said that mission command is the art and science of decision making. In the case of MDO, more science will demand more art. Dispersed operations with contested networks and communications will demand intimate understanding of intent throughout formations so that intent can be carried out in the absence of definitive direction." Wallace, W. (2011, August). Multi-domain operations in context. *The Landpower Essay Series*, (20-4). Arlington, VA: Association of the United States Army, p. 4.

[22] Multiple intent-aligned decisions at lower echelons contributes to creating a decision advantage as subordinates do not need to wait for permission to act. This is what the MDO Concept refers to as *intent-based synergy*. See MDO Concept, p. 21. "The commander's intent provides a unifying idea that allows decentralized execution within an overarching framework. It provides guidance within which individuals may exercise initiative to accomplish the desired end state. Understanding the commander's intent two echelons up further enhances unity of effort while providing the basis for decentralized decision making and execution throughout the depth of a formation." ADP 6-0, p. 1-5.

[23] Currently, a decisive point is defined as "a geographic place, specific key event, critical factor, or function that, when acted upon, allows commanders to gain a marked advantage over an enemy or contribute materially to achieving success." JP 5-0. The AFCC-C2 defines a decisive space as a conceptual geographic and temporal location where the full optimization of the employment of capabilities from all the domains generates a marked advantage over an enemy and greatly influences the outcome of an operation. "The Army must move beyond 'decisive points' because they artificially imply discrete physical characteristics of a battlefield that no longer exists. Decisive space implies that there are in fact particular synergistic opportunities where domains overlap, but acknowledges that there will be ill-defined bleedover." Wesley, E. & Simpson, R. (2020, April). Expanding the battlefield: An important fundamental of multi-domain operations. *Land Warfare Paper*, (131). Arlington, VA: Association of the United States Army, endnote 7, p. 11.

[24] See EAB Concept, pp. 27-28.

[25] "Commanders today are disadvantaged in many ways. We have large staffs and refined processes. Our communications methods create opportunities for over-communicating and are bereft of the right information at the right time for the right decision. Doubling down on putting the commanders back [into writing their own clear and concise] intent, providing them with the skills necessary to create time and space for thinking and reflection, and deepening our investment in their development will help lay the foundation for successful mission command." Shafley, B. (2020, May 13). Put the commander back in commander's intent. *Center for International Maritime Security*.

[26] The MDO Concept defines hyperactive as "more active than usual or desirable; hyper-competitive during competition and hyper-violent in armed conflict." MDO Concept, p. GL-5.

[27] "Adversaries will challenge U.S. interests by means and with ways below the threshold of armed conflict and short of what the United States considers war." MDO Concept, p. A-1.

[28] In military operations, asymmetric is defined as the application of dissimilar strategies, tactics, capabilities, and methods to circumvent or negate an opponent's strengths while exploiting his weaknesses. (JP 3-15.1)

[29] The AFCC-C2 defines information warfare as the integrated employment of information activities and capabilities along with other lines of operation to coerce, disrupt, corrupt, or usurp threat decision making while protecting U.S. capabilities.

[30] Russian actions in Ukraine and Crimea provide a prime example.

[31] As a case in point, the growing use of tunnels and underground facilities by military and irregular forces to gain a tactical advantage is becoming more sophisticated and increasingly effective, making the likelihood of U.S. forces encountering military-purposed subterranean structures on future battlefields very high.

[32] See Bērziņš, J. (2014, April). *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Center for Security and Strategic Research, National Defence Academy of Latvia, p. 5. Information warfare will be a combination of general and more personalized attacks against specific populations and leaders.

[33] "Indeed, in a 2018 Gallup Poll of American confidence in societal institutions, the military came out on top. This is a long-standing position that our military has assiduously strived to protect. The poll results are more than mere platitudes—they speak to the military's legitimacy within the American system. I believe there are three key reasons our military enjoys this reputation: it respects civilian control of the military; it represents the people it serves; and it remains apolitical. When the military's nonpartisan nature is called into question, it challenges those reasons, skews the constitutional balance among America's fundamental institutions, and threatens our democratic governance." Votel, J. (2020, June 8), An apolitical military is essential to maintaining balance among American institutions. *Air Force Times*.

[34] Super-empowered individuals and small groups are "wild cards" that may be leveraged by a near-peer adversary, act independently on behalf of a near-peer adversary, or work to their own separate goals.

[35] Weapon and explosive fabrication instructions, as well as necessary raw materials, are only a mouse click away.

[36] A computer or internet bot is short for "robot." It is a computer program that operates as an agent for a user or other program, or to simulate a human activity. Bots are normally used to automate repetitive tasks and run without specific instructions from humans. Bots can be used for good or malicious purposes. They can be used for good purposes such as to crawl the web and gather information or provide automatic interaction with instant messaging. Malicious bots are self-propagating malware that can infect their hosts and connect back to a central server. Among their many

malicious uses, bots can gather passwords, log keystrokes, obtain banking information, relay spam, launch denial-of-service attacks, and open back doors on infected computers.

[37] "In competition, [China and Russia] seek to fracture U.S. alliances and partnerships…. By generating instability within countries and alliances, they create political separation that results in strategic ambiguity, *reducing the speed of friendly recognition, decision, and* reaction." [Emphasis added.] MDO Concept, p. 7. Army forces must seek to improve partners' ability for self-defense. Thoughtful and sustained security cooperation sets conditions for access, improves partner interoperability and resiliency to crisis response events, contributes to understanding and the development of appropriate operational approaches, and supports expeditionary maneuver. (See EAB Concept, pp. 38-40 & 50.)

[38] The Maneuver in Multi-Domain Operations Concept 2028 (hereafter referred to as the MMDO)) defines information narrative as the "commander's visualization of outcomes in the information environment achieved through the combination of actions in the physical, virtual, and cognitive domains." MMDO, p. 85.

[39] See MDO Concept, p. 8 and EAB Concept, p. 14.

[40] "Across these battlefields, rival powers made investments and developed doctrine, providing ample evidence that future wars promise extreme lethality not seen since World War II." Brown, R. & Perkins, D. (2017, August 18). Multi-domain battle: Tonight, tomorrow, and the future fight. *War on the Rocks*.

[41] "We ignore the ethical implications of [human enhancement (HE)] technology use for soldier resilience at our own peril. Without proper *a priori* ethical considerations, the adoption of HE technologies could stall at the regulatory policy development stage, hindering the deployment of HE solutions for more resilient soldiers. Perhaps even more grave, if ethics is not considered prior to the adoption of HE technologies, unanticipated and potentially catastrophic unethical situations on the battlefield could ensue. Neither of these outcomes is desirable for military dominance in the [future operational environment]." Thorpe, J., Girling, K., & Auger, A. (2017, July 13). Maintaining military dominance in the future operating environment: A case for emerging human enhancement technologies that contribute to soldier resilience. *Small Wars Journal*.

[42] "Since the enemy will disrupt friendly communications and plans, mission command must expand to enable initiative and dynamic cooperation across Service and other partner lines—at some risk—to allow the Joint Force to preserve the ability to continuously and rapidly integrate multi-domain capabilities despite disrupted communications." MDO Concept, p. 21.

[43] Enemies and adversaries will use urban areas for camouflage, concealment, and protection from advanced U.S. technology. They will routinely position CPs and other military targets in dense urban environments and deliberately endanger civilians to create international sympathy and support.

[44] "The physical and demographic density in this environment creates distinct physical, cognitive, and operational characteristics. The cumulative effect of these factors compounds the friction of war by increasing the number of tasks required within a given physical or temporal space while multiplying the tactical, operational, and strategic variables that commanders and staffs must take into account." MDO Concept, p. 6. See also MDO, pp. D-1 through D-6 and ATP 3-06.

[45] This second method has been dubbed "lawfare." See Dunlap, C. (2017, May-June). Lawfare 101: A primer. *Military Review*.

[46] "[General Martin E. Dempsey] said he believes in the whole-of-government approach with economic, diplomatic, law enforcement, energy and the military instruments of power working together to confront problems and issues, and he's pushed for that approach many times during his tenure." Garamone, J. (2015, September 22). Dempsey talks caution, whole-of government approach. *DoD News*.

[47] "When establishing their operational framework, commanders and staffs consider the physical, temporal, virtual, and cognitive aspects of their own AO, their higher echelon's AO, and subordinate AOs. The physical, temporal, virtual, and cognitive aspects of an operational framework vary in terms of focus and priority depending upon the echelon, force capabilities, and the OE." FM 3-0, p. 1-26. Note that combat power is defined as "the total means of destructive, constructive, and information capabilities that a military unit or formation can apply at a given time." ADP 3-0, p. 5-1.

[48] "There is no 'default' military-centric response in a true whole-of-government conflict resolution strategy. The primary objective of a comprehensive approach is to achieve multidimensional and system-wide effects in multinational and interagency operations. When a new national security strategy is developed, or when an existing strategy—such as the coalition's strategy to address transnational threats across all the areas of operation outlined above—is refined, it is vital that every appropriate lever available to the government can, and should, be part of the planning process as well as the implementation process." Blannin, P. (2018, May 4). The good operations: Notes on a whole-of-government approach to national security. Modern War Institute.

[49] ADP 3-0 defines operational initiative as "setting the tempo and terms of action throughout an operation" and tempo as "the relative speed and rhythm of military operations over time with respect to the enemy." The Chief of Staff's Paper #1 defines decision dominance as "a desired state in which commanders sense, understand, decide, act, and assess faster and more effectively than their adversaries." McConville, J. (2021, March 16). *Army Multi-Domain Transformation: Ready to Win in Competition and Conflict, Chief of Staff Paper #1*, p. 30. "And then we come to decision dominance. 'This is a developing definition,' [General John Murray, Commanding General of Army Futures Command] cautioned. 'But right now, [decision dominance] is the ability for a commander to sense, understand, decide, act, and assess faster and more effectively than any adversary.'" Freedberg, S. (2021, March 17). Army's new aim is decision dominance. Breaking Defense.

[50] "First, the [Department of Defense] should ramp up its efforts to develop joint operational concepts to drive more rapid fielding of game-changing technologies. Greater alignment between the services on concepts, planning and budgeting will give Congress greater confidence and clarity about the DoD's commitment to this new strategic direction." Flournoy, M. & Chefitz, G. (2020, April 1). Breaking the logjam: How the Pentagon can build trust with Congress. *Defense News*.

[51] DOD. (2020). Joint All-Domain Command and Control Vision (draft version 0.6), p. 3.

[52] This does not mean that the solutions and required capabilities described within the AFCC-C2 cannot be later modified during subsequent experimentation, analysis, and research. It does mean, however, that the entire concept should be understood as a baseline before deviations are made based on new information and insights obtained during later capability development efforts. The campaign of learning for command and control is continuous; it does not end upon publication of this document.

[53] The AFCC-C2 defines a system as a group of interacting, interrelated, and interdependent components or subsystems that form a complex and unified whole. Systems have a purpose with their parts arranged in a way (structure) to carry out their purpose.

[54] For example, the technological changes and advancements necessary to link any sensor to any command echelon or node and the best shooter across the Services and with coalition partners is critical to future targeting and the ability to rapidly converge effects against fleeting targets and assess results. Future multi-domain operations as envisioned in the MDO and EAB concepts will not be possible without this transformation. However, effective convergence will also not be possible without the concomitant changes necessary in people—considering both individual and organizational aspects—and other processes to which targeting supports or is supported.

[55] "The future strategic environment will require leaders who have the cognitive complexity to understand, decide and act while leading large military organizations in complex, chaotic, multidimensional environments. Increasing this complexity will be the incorporation of future

technologies that are exponentially increasing the velocity of war. The time and space available for national security decision-making, potentially existential in nature, will shrink." Schmidt, T. (2020, November). Developing officers with a higher degree of brain power. *Army Magazine, 70 (11)*, p. 10.

[56] "We will enhance the development and education of our leadership at all levels to produce adaptive, agile, innovative and flexible leaders of character and competency. And we will do so as a total force to win anywhere, anytime, against any enemy." Milley, M. (2015, October). Winning matters: Especially in a complex world. *Army Magazine, 65(10)*, p. 23. The AFCC-C2 defines agility as a *flexibility* of mind and an ability to anticipate and *adapt* to uncertain or changing situations. The attribute of "agile" captures and includes the need for flexibility and adaptability.

[57] "Mission command remains an essential element of Army operations on a contested battlefield against a near-peer enemy." MDO Concept, p. 21.

[58] "In today's era of big data (data that requires high-performance processing and large computational infrastructure, and is characterized by its volume, velocity, and variety at scale), there are tools designed for insight generation from data. What is missing for tactical leaders are soldiers trained to use the tools to exploit today's modern data-rich tactical environment. Unfortunately, even when a battle staff has the right tools (and they do), soldiers do not have the training to use them well, and leaders do not have the background to ensure that the battle staff is focused on the right data to solve the tactical problem at hand." Tunnell, H. (2020, July-August). Tactical data science. *Military Review*. "…the Army will work to build a capable talent pool of data experts and ingrain data-centric behaviors and mindsets across the force….Finally, this [line of effort] will examine the addition or creation of Army skill sets, positions, and organizations that facilitate enduring data competence." DA. (2019, November 15). HQDA EXORD 009-20: Army Data Plan Implementation in Support of Cloud Migration.

[59] There are two aspects to the term "globally-networked." The first is that is that formations, organizations, and the individuals that form them are seamlessly connected (technologically) by the Army's future communications network. The second is that formations, organizations, and the individuals that form them can unite and connect (socially) to establish human networks across echelons, boundaries, and organizations to create deep, shared understanding of complex problems and an accurate visualization of the battlespace, contribute to developing operational solutions, and act with unity of effort to succeed. For example, special operations forces (SOF) describe a global SOF network as a system of personal and professional relationships with other SOF teams, command elements, joint forces, allied and partner forces, and other government agencies and nongovernmental organizations.

[60] "When technical architecture is disrupted, flexible command relationships and multi-domain control measures are the enabling elements of mission command." MDO Concept, p. 24.

[61] Current doctrine specifies only four components to the operations process: planning, preparation, execution, and assessment. Monitoring is considered an integral part of assessment. The AFCC-C2 highlights monitoring as a separate component to ensure that capabilities developers specifically consider capabilities that allow commanders to sense and understand their extended battlespace. Whether or not this change should be included in doctrine will be determined in later DOTMLPF-P analysis.

[62] "Today, most leaders of combat formations have limited experience with combined arms operations against enemy conventional or hybrid forces." Murphy, P. & Milley, M. (2016, April 7). [Record Version]. Statement by the Honorable Patrick J. Murphy, Acting Secretary of the Army and General Mark A. Milley, Chief of Staff United States Army before the Committee on Armed Services United Sates Senate. Washington, DC, p. 5.

[63] "Our approach to readiness recognizes that after a decade of focus on counter-insurgency operations, the U.S. armed forces must re-hone other capabilities needed for a wider spectrum of missions and [threats]." DOD. (2012, January). *Defense Budget Priorities and Choices*, p. 2.

[64] "In large-scale combat operations against a peer threat, commanders conduct decisive action to seize, retain, and exploit the initiative. This involves the orchestration of many simultaneous unit actions in the most demanding of operational environments. Large-scale combat operations introduce level of complexity, lethality, ambiguity, and speed to military activities not common in other operations. Large-scale combat operations require the execution of multiple tasks synchronized and converged across multiple domains to create opportunities to destroy, dislocate, disintegrate, and isolate enemy forces." ADP 3-0, p. 5-3.

[65] "Accelerate the Department's activities to contribute to our whole-of-government efforts to combat transnational threats." Miller, C. (2020, November 16). [Memorandum]. *Message to the Department—Acting Secretary Miller's Goals*.

[66] "Operational success…relies upon the performance of ground forces enabled by robust and Joint-Interagency efforts to affect activities occurring in finite amounts of time and discrete amounts of space." DA, Chief of Staff of the Army Strategic Studies Group-I. (2013, July). *Testing Assumptions about the Role of Land Power in 2030 Final Report*, p. 15.

[67] "While the need is clear, efforts to implement a "whole-of-government" approach to national security have been episodic and ultimately unsuccessful. Although there has been much discussion, frustration, and angst about the lack of cooperation and coordination between and among U.S. government agencies and departments, there has been very little progress in establishing mechanisms to coordinate disparate and diverse organizations, each with their own leadership, culture, and authorities. The result is a disjointed and often ineffective foreign policy. While it will take national leadership to change this at the strategic level, there are measures that can be taken to mitigate challenges at the operational and tactical levels." Derleth, J. (2018, February 28). Fostering a whole-of-government approach to national security from the bottom up. *Military Review*, p. 1.

[68] "There is more to sustaining a competitive advantage than acquiring hardware; we must gain and sustain an intellectual overmatch as well." Milley, M., et al. (2020, May 01). *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education & Talent Management*, p. 2.

[69] "Knowledge management is supported by four tasks that bring an organization closer to situational and shared understanding. The four knowledge management tasks are creating knowledge, organizing knowledge, applying knowledge, and transferring knowledge." ADP 6-0, p. 3-8.

[70] As each echelon's future command post constellation and their associated command nodes become widely distributed over greater and greater distances, knowledge management becomes even more critical to the development of accurate battlespace visualization and overall shared understanding.

[71] The integration and management of other domain, EMS, and IE capabilities is equally important but left to other Army functional and supporting concepts to discuss.

[72] "Second, the Army must maintain a robust *Network* that is not vulnerable to cyber-attacks. This network provides the ability for the Joint Force to assess reliable information on adversaries, the terrain, and friendly forces. This information provides a decisive advantage by enabling the Joint Force commander to make accurate and timely decisions, ultimately, hastening the defeat of an adversary." Murphy, P. & Milley, M. (2016, April 7). [Record Version]. Statement by the Honorable Patrick J. Murphy, Acting Secretary of the Army and General Mark A. Milley, Chief of Staff United States Army before the Committee on Armed Services United Sates Senate. Washington, DC, p. 9.

[73] "Fundamentally, mission resilience is built on three pillars: robustness, the ability of a system to resist or negate the impact of disruption; responsiveness, the ability of a system to provide feedback on and incorporate changes in response to the impact of disruption; and adaptability, the ability of a system to change itself to continue operating amid disruption over its full life cycle, even when those changes dictate an adjustment of the system's objectives." Herr, T., et al. (2020, December). *How Do You Fix a Flying Computer? Seeking Resilience in Software-Intensive Mission Systems*. Atlantic Council. Washington, DC, p. 5.

[74] Resiliency is the ability of an architecture to support the functions necessary for mission success in spite of hostile action or adverse conditions. An architecture is considered "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, or across a wider range of scenarios, conditions, and threats. Resilience may leverage cross-domain or alternative interagency, commercial, or international capabilities. DOD. (2016, September 15). DOD Instruction 8420.02: DoD Satellite Communications (SATCOM), p. 34.

[75] While allowing for a rapid and responsive acquisition process, the Army must establish unity of effort in materiel development for the communications network to enable integrated and synchronized research, development, and acquisition efforts within the Army, across the Department of Defense, and in conjunction with partners in industry and academia.

[76] "Plans to increase technical training are in place, [General David Perkins, head of Army Training and Doctrine Command], said, but it's not enough to keep up with the speed of technology. 'You have to realize that the Army is going to field new systems before we get [warrant officers] back into the school system again,' he said. 'We just can't bring you back every time a new system comes in.' One solution: Increased efforts to push updated maintenance tutorials and requirements into the field alongside the new gear. "Lilley, K. (2016, February 16), Warrant officer forecast: What's in store for the Army's technical experts. *Army Times.*

[77] "To solve problems with agility in a complex, uncertain environment, the Army must leverage information and data—at scale—more quickly and effectively than our adversaries." McConville, J. & McCarthy, R. (2020). *Project Convergence.*

[78] "DoD data will be: **Visible**–Consumers can locate the needed data. **Accessible**–Consumers can retrieve the data. **Understandable**–Consumers can find descriptions of data to recognize the content, context, and applicability. **Linked**–Consumers can exploit complementary data elements through innate relationships. **Trustworthy**–Consumers can be confident in all aspects of data for decision-making. **Interoperable**–Consumers and producers have a common representation and comprehension of data. **Secure**–Consumers know that data is protected from unauthorized use and manipulation. [VAULTIS]" DOD. (2020, October 08). DoD Data Strategy, p. 6.

[79] "Improving data management will enhance the Department's ability to fight and win wars in an era of great power competition, and it will enable operators and military decision-makers to harness data to capitalize on strategic and tactical opportunities that are currently unavailable." DOD. (2020, October 08). DoD Data Strategy. p. i.

[80] "Pentagon leadership and the heads of each of the military service branches have all come to the same conclusion: Data is the principal currency of future warfare. And the military that is able to collect, process and share data faster than opponents will hold a huge advantage…. The Pentagon will need help *from* Congress and private industry to see this through…. None of this comes without a cost and without some levels of risk. But history suggests dramatic progress is possible. Indeed, the military history of the last century shows that success on the battlefield goes to those willing to make a break from the familiar conventions and invest their resources and reputations in the future." Goldfein, D. & Raymond, J. (2020, February 27). America's future battle network is key to multidomain defense. *Defense News.*

[81] "There is a sea of data outside the Defense Department's networks that can be brought to bear on defense problems. Datasets that are external to the U.S. military and from commercial providers, academia, non-governmental organizations, other federal departments, and even local governments provide a diverse view of global markets. They can help the Defense Department stay abreast of technological developments, industrial base dynamics, and supply chain risk—they are pieces of information critical to strategy development and execution. External data, including canonical data models, can also serve as a 'Rosetta Stone' that translates between disparate datasets so that they can 'speak' with one another, increasing the quality and utility of internal datasets. Furthermore, the Defense Department should access external data simply to keep pace with China, which is aggressively collecting and utilizing data available in commercial markets." Work, R. & Dougherty, T. (2020, October 6). It's time for the Pentagon to take data principles more seriously. *War on the Rocks.*

[82] "[Line of Effort] 1 also includes senior leader and commander emphasis on task execution and on the importance of data as a strategic asset." DA. (2019, November 15). HQDA EXORD 009-20: Army Data Plan Implementation in Support of Cloud Migration. "To support the National Defense Strategy objective to provide combat-capable military forces needed to deter war and protect the security of our Nation, we must turn data into a strategic asset. In this time of rapid technological change with challenges from adversaries in every operating domain, our data and data sets are the digital ammunition of the future. We must be able to see, understand, and leverage the data in our platforms, systems, applications, and networks in an integrated and consistent manner to improve our operational decision-making and outcomes. These rules apply to all Mission Areas. In particular, these are critical for Army contributions to Joint All-Domain Operations and Joint All-Domain Command and Control." McConville, J. & McCarthy, R. (2020, April 10). DA Memorandum: *Mandatory Implementation of Army Data Services Requirements.*

[83] The AFCC-C2 defines *mesh* as: to connect nodes or devices directly, dynamically, and non-hierarchically to as many other nodes or devices as possible allowing them to relay critical data without interruption and cooperate, self-organize, and self-configure to accomplish tasks collectively despite individual node or device degradation or destruction.

[84] The AFCC-C2 defines sociotechnical as "the careful and thoughtful integration of humans and technology so that technology compliments human attributes—cognitive and physical—for greatest benefit." CP infrastructure includes the environmentally controlled workspace and lighting necessary to house and protect Soldiers and systems from the environment; the visualization and collaboration devices that allow the commander and staff to view a tailorable battlespace visualization based on common, standardized, shareable, and secure data and communicate internally and externally (large-scale displays and intercom). It also includes the necessary power generation and distribution equipment to establish and manage the power grid to enable continued, sustained operations.

[85] "[Controlling or managing electronic emissions to reduce signature detection can degrade one's own communications capabilities] is driving separate work in the U.S. military, among others, on electronic systems, especially sensors, such as radars and communications systems, that can work effectively in passive modes or otherwise have a low probability of intercept, making them more difficult to detect and more resilient against jamming or spoofing" Trevithick, J. (2020, May 11). This is what ground forces look like to an electronic warfare system and why it's a big deal." *The Drive.*

[86] Leader development is a combination of training, education, and experience.

[87] "Leader development is the fundamental basis for a U.S. Army that practices mission command in everything it does. Mission command and leader development are interdependent. Mission command is how we fight, and leader development is part of how we prepare to fight. Leader development that excludes the principles of mission command, or worse, that preaches mission command without putting it into practice, is missing out on the exploitation of human potential, knowledge, and experience that mission command allows. However, a U.S. Army that operates according to the principles of mission command does not just happen naturally, especially in peacetime. How effectively the Army

applies the principles of mission command will be the product of leader development in a peacetime environment." Whitford, A. (2015, May-June). The path to Mission Command. *Military Review, XCV (3)*, p. 40.

[88] "A further issue is the need to sustain the human quality of our armed forces….If we are to retain high-caliber people capable of thinking and acting quickly and effectively under stress, we need to retain a doctrine or philosophy (such as Mission Command) that supports those characteristics. If we do not, the good will leave and only the obedient, subservient and unimaginative will stay." Storr, J. (2003, Autumn). A command philosophy for the information age: The continuing relevance of mission command. *Defence Studies*, (3) 3, p. 126.

[89] "We will spend billions of dollars researching how to improve the network, but it will mean little if we don't focus our energies on command climates and environments—trust, initiative, dialogue and freedom of action within intent—that will allow mission command to thrive throughout our Army and our institutions to become as agile as our operating force." Guthrie, T. (2012, June). Mission command: Do we have the stomach for what is really required? *Army Magazine, 62(6)*, p. 28

[90] The AFCC-C2 defines institutionalize as the deliberate translation an organization's code of conduct, mission, policies, vision, and strategic plans into guidelines and practices applicable to the daily activities of its leaders and subordinates; integrate fundamental values and objectives into the organization's culture, structure, and operating capabilities.

[91] "'Expecting audacity among junior leaders in combat while micromanaging them in peacetime garrisons is a recipe for battlefield failure,' a leader told [Rand] researchers. 'The Army must restore its commitment to decentralized leadership and frontline leaders' authority, and practice what it preaches in garrison as well as during operations.'" Tan, M. (2020, March). Under pressure: Overtasked commanders need time management help. *Army Magazine, 70(3)*, p. 44.

[92] "Achieving our leader development aim requires a new trajectory for our professional military education (PME) that must include associated talent management systems. Our vision is for a fully aligned PME and talent management system that identifies, develops, and utilizes strategically minded, critically thinking, and creative joint warfighters skilled in the art of war and the practical and ethical application of lethal military power." Milley, M., et al. (2020, May 01). *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education & Talent Management*, p. 2.

[93] "Although a whole-of-government approach may seem a daunting task, one of the most effective ways to encourage coordination and collaboration is to bring representatives from interagency entities together for realistic training with their military counterparts *before* they are forced to work together in a crisis. Recognizing the importance of "training as you fight," the Army's Joint Multinational Readiness Center (JMRC) in Hohenfels, Germany, integrates interagency personnel into its exercises. They include mission rehearsal exercises, noncombatant evacuation operations, and brigade readiness exercises with North Atlantic Treaty Organization allies and multinational partners. This experience provides soldiers and other interagency participants the opportunity to work with, and learn from, the other entities they may encounter during a deployment. Integrated training also helps build the relationships and develop the trust required to effectively implement national security policy." Derleth, J. (2018, February 28). Fostering a whole-of-government approach to national security from the bottom up. *Military Review*, p. 1.

[94] "Unfortunately, in survey after survey, Army officers report that their leaders' greatest shortcoming is the failure to develop subordinates." Pryer, D. (2013, November-December). Growing leaders who practice mission command and win the peace. *Military Review, XCIII(6)*, p. 36.

[95] "What I'm suggesting here, however, is that our leader-development programs must also produce and reward leaders who are inquisitive, creative and adaptable." Dempsey, M. (2011, February). Leader development. *Army Magazine, 61(2)*, p. 26.

[96] "As critical thinkers, staff members discern truth in situations where direct observation is insufficient, impossible, or impractical. They determine whether adequate justification exists to accept conclusions as true, based on a given inference or argument. As creative thinkers, staff members look at different options to solve problems. They use proven approaches (drawing from previous similar circumstances) or innovative approaches (coming up with completely new ideas). In both instances, staff members use creative thinking to apply imagination and depart from the old way of doing things." ADP 6-0, p. 4-5.

[97] "The primary conclusion of this paper is that the Army's current laissez-faire approach is insufficient to effectively meet the challenges posed by implementation of either mission command or the principles…." Michelson, B. (2013, September-October). Character development of U.S. Army leaders: The laissez-faire approach. *Military Review, XCIII (5)*, p. 37.

[98] "…but it will be our commanders who will execute these mission command principles each day and who will continue to shape the Army we build for the future." Perkins, D. (2012, June). Mission command: Reflections from the combined arms center commander. *Army Magazine, 62(6)*, p. 34. "Its senior officers need to take on this challenge directly. They must embrace and protect a leadership philosophy anchored in trust—one that imbues the Army's peacetime operations with wartime precepts of Mission Command." Barno, D. (2014, July 10). The Army's next enemy? Peace. *The Washington Post*.

[99] "For leaders who are accustomed to tackling performance problems by telling people what to do, a coaching approach often feels too 'soft.' What's more, it can make them psychologically uncomfortable, because it deprives them of their most familiar management tool: asserting their authority. So they resist coaching—and left to their own devices, they may not even give it a try." Ibarra, H. & Scoular, A. (2020, November-December). The leader as coach. *Harvard Business Review*.

[100] "Formal counseling and informal mentoring are clearly Army weaknesses that limit the ability of Army leaders to reach their full potential in all areas, to include their personal character." Michelson, B. (2013, September-October). Character development of U.S. Army leaders: The laissez-faire approach. *Military Review, XCIII (5)*, p. 36.

[101] "Moving the Department to a data-centric organization requires a cultural transformation with the DoD workforce at its heart. DoD will continue to evolve its decision-making culture to one soundly based upon data and analytics enabled by technology. A modern, agile, information-advantaged DoD workforce (leaders, service members, civilians, and contractors) will be increasingly empowered to work with data, make data-informed decisions, create evidence-based policies, and implement effectual processes. We must carefully cultivate our data talent to create and sustain these capabilities. We must provide data skill training, establish centers for data engineering excellence, and foster a supportive ecosystem for collaboration among data experts." DOD. (2020, October 08). DoD Data Strategy, p. 6.

[102] "As we look to reinvigorate wargaming across the defense enterprise, there is another lesson from the inter-war period that we would do well to heed. In the years leading up to the Second World War, we energized our war colleges and schools to think about how we would fight differently in future conflicts, and wargaming was central to this effort. All students and officers returning as instructors were taught how to run a wargame. The constant cycling of officers from the schoolhouse to the operating forces not only created great wargames, but great wargamers—many of whom turned out to be great wartime commanders." Work, B. & Selva, P. (2015, December 8). Revitalizing wargaming is necessary to be prepared for future wars. *War on the Rocks*, p. 5. Faculties must include the correct balance of military and civilian instructors, curriculum developers, and researchers.

[103] "A world-class educational program is not an accident, nor does it come cheap; it is the product of deliberate design, founded upon a top-notch faculty. Every PME institution must make sure its military and civilian faculty are qualified instructors and current in the fields they are

teaching." Milley, M., et al. (2020, May 01). *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education & Talent Management*, p. 7.

[104] See U.S. Army Combined Arms Center. (2015, September). *Talent Management Concept of Operations for Force 2025 and Beyond*. Fort Leavenworth, KS. Appendix A to this Concept of Operations (CONCOPS) covers these issues under its problem area discussions of talent requirements; talent inventory; evaluations, promotions, and succession planning; and assignments, development, and career management, pp. 23-25.

[105] "This legacy [personnel management] system is woefully archaic in the 21st century—and far removed from the best talent-management practices of the private sector. It may well be the last untransformed segment of an otherwise modern, flexible, and adaptable U.S. military. Yet the personnel system touches every single person in the military every single day of their career—and determines how much they are paid, where they live, what kind of jobs they perform, and how often they move or get promoted. Neither officers nor enlisted troops have any substantial input in how they fit into this system—nor how to maximize their talents for the greater good." Barno, D. & Bensahel, N. (2015, November 5). Can the U.S. military halt its brain drain? *The Atlantic*. "In the command processes and professional structures that create generation after generation of warriors that tacitly reinforce and defend the centralized hierarchy, this sort of change will be near impossible. It requires the awakening of a senior level of defense leadership at the right moment, with the strength and agility to purge what will inevitably be multiple generations of those still shackled to the centralized hierarchical form. Those that prosper under the traditional form will find it most hard to abandon, as change ushers in uncertainty and the greater potential for loss of power and prosperity for those expecting it under the current form." Zweibelson, B. (2016, January 12). US, allies must 'stop fixating' on ISIL & friends; 'frankly, we are losing.' *Breaking Defense*.

[106] "While new capabilities will be essential, many of our most important advancements will come through innovations in training, education, personnel management, and leadership development." CCJO, p. iii.

[107] AR 34-1 defines interoperability as the ability to act together coherently, effectively and efficiently to achieve tactical, operational, and strategic objectives. AR 34-1, p. 30. "Interoperability across Service, interagency, and multinational partners is a key element to executing MDO. Multi-domain command and control is the combination of joint and combined materiel, processes, and authorities that underpin convergence, multi-domain formations, and mission command designed to enable and exploit interoperability." MDO Concept, p. 23.

[108] "The 2018 NMS acknowledges the unique contributions of allies and partners, a strategic source of strength for the Joint Force. Building a strong, agile, and resilient force requires better interoperability and enhancing the combat lethality and survivability of our allies and partners. The NMS also informs engagement with interagency partners, both abroad and domestically, to enable the Joint Force to best support the application of all instruments of national power throughout the continuum of conflict." 2018 NMS Description, pp. 3-4.

[109] "As the foundation upon which other U.S., allied and multinational capabilities will operate, the Army of 2025 must be interoperable by easily supporting and enabling joint, whole-of-government and multinational land-based operations." DA. (2015). *The Army Vision: Strategic Advantage in a Complex World*, p. 9. "Joint Forces face a rapidly evolving, multi-domain operating environment in which highly adaptive and innovative adversaries create resilient formations, forces, and systems to support their strategies. Adversaries employ systems to achieve their strategic ends over time to avoid war and negate the traditional operating methods of the Joint Force. It is in this context that the Army, as the primary land force of the U.S. military, must partner with [unified action partner] forces to organize, practice, and employ capabilities and methods across domains, environments, and functions to contest these adversaries in competition below armed conflict and, when required, defeat them in armed conflict. The capabilities that [unified action partners] provide are critical to the success of any such campaign and act as a military force multiplier for the Coalition Forces." AR 34-1, p. 2.

[110] The Army has already instituted a measurement process to assess progress and identify and mitigate interoperability gap, The army measure interoperability in terms of four levels: Level 0, Not Interoperable; Level 1, De-Conflicted; Level 2, Compatible; and. the highest. Level 3, Integrated. See DA, U.S. Army Center for Lessons Learned. (2020, April 08). *New From the Front: The Army Interoperability Measurement Systems AIMS*, p. 2.

[111] See Mission Command Center of Excellence, Army Capability Manager for Mission Command / Command Posts. (2018, May 09). *Army Mission Command Interoperability White Paper*. Fort Leavenworth, Kansas, forward & p. 5.

[112] Of course, this may first require careful review to make any modifications—agreed to by all Services—to account for any critical Service- or domain-specific equities that have not already been considered.

[113] However to ensure the greatest understanding of the concept's ideas within the Army, this concept uses approved Army doctrinal terminology unless it does not adequately describe the future subject matter area.

[114] "*The U.S. Army in Multi-Domain Operations* concept requires the Army to develop or improve capabilities to contribute cross-domain options within the Joint Force by:… Establishing necessary authorities and permissions normally reserved for conflict or to higher echelons to operate in competition and rapidly transition to conflict effectively." MDO Concept, pp. x and xi. This may require policy changes at the national level and in and among each of the Services.

[115] See MDO Concept, p. 13.

[116] "The main consideration in exercising initiative is the urgency of the situation. If time permits, subordinates attempt to communicate their new situation and recommended course of action to their commander. When subordinates communicate their intentions to their commander, their commander can assess the implications for the overall force, and for other operations, and set in motion supporting actions. However, subordinates must depart from their orders when they are unable to contact their commander or when there is a limited amount of time to seize a fleeting opportunity. If doubt exists about whether to contact their commander or depart from orders and act to seize a fleeting opportunity, subordinates should act, if they can do so within their commander's intent." ADP 6-0, p. 1-12.

[117] "Fostering a command climate that encourages initiative requires commanders to accept risk and underwrite the good faith mistakes of subordinates in training, before the unit is committed to combat. Commanders set conditions for subordinates to learn and gain the experience they need to operate on their own. Subordinates learn to trust that they have the authority and responsibility to act, knowing their commander will back their decisions. Because mutual trust and shared understanding constitute the foundation of subordinate initiative, commanders train subordinates to act within the commander's intent in uncertain situations." ADP 6-0, p. 1-12.

[118] Machine-machine cooperation, collaborative decision making, and battle management will also be important as the future will likely have multiple, smaller, and specific AI applications rather than larger, general, all-encompassing AI. Smaller AI must be able to work together to accomplish larger complex tasks. Drone swarms are one example.

[119] Although machines will have an ability to consolidate and process massive amounts of data, decision making in modern war will still depend on human judgment to integrate tactical, operational, and strategic context into decisions. This unique strength of the human brain, combined with the speed and capacity of computers, will create a symbiotic relationship that enhances the speed, responsiveness, and quality of decisions.

[120] "Finally, in looking toward the future, having tactical leaders who understand data science can alleviate challenges in emerging artificial intelligence programs, such as bias in machine learning models. For example, factors that contribute to model bias are selecting the wrong data to

train the model and building models that do not reflect environmental realities as they are based upon incorrect assumptions. To mitigate this, some researchers are creating audit systems to scrutinize predictive models before they are deployed." Tunnell, H. (2020, July-August). Tactical data science. *Military Review*.

[121] The AFCC-C2 defines big data as extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions.

[122] Take cybersecurity, for example. "We must always test and measure cyber controls, resilience techniques and procedures, in realistic complex environments and against a broad range of sophisticated threats. That is the only way to make sure we are prepared for a cyberattack." Kott, A. & Delano, K. (2020, November). Cyber resiliency through the lens of COVID-19. *Army Magazine, 70 (11)*, p.48.

[123] See, for example, Covey, S.M.R. (2006). *The Speed of Trust: The One Thing That Changes Everything*. New York, NY: Free Press.

[124] "Breaking this logjam to ensure the United States has the capabilities it needs in an operationally relevant time frame will require building greater transparency and trust between the [Department of Defense] and Congress." Flournoy, M. & Chefitz, G. (2020, April 1). Breaking the logjam: How the Pentagon can build trust with Congress. *Defense News*. "[The Defense Department] should, for example, explore setting different standards for data transparency depending on the level of trust it has with certain companies and academic centers through mechanisms such as a trusted data consortium." Work, R. & Dougherty, T. (2020, October 6). It's time for the Pentagon to take data principles more seriously. *War on the Rocks*.

[125] "DoD data requires trust to deliver the needed value to its Service members, civilians, and stakeholders. Lacking confidence in the data may result in less timely decision-making or, consequently, no decision when one is warranted. DoD will know it has made progress toward making data trustworthy when… DoD data has protection, lineage, and pedigree metadata bound throughout its lifecycle." DOD. (2020, October 08). DoD Data Strategy, p. 8.

[126] "[Air Force Chief of Staff General Charles] Brown reiterated that there are tech barriers to data sharing, but said the bottom line challenge is a lack of trust among the services. The services don't trust the validity of the data provided by other services; nor do they trust their sister services to properly protect any data they themselves share. 'At the end of the day, information sharing has a currency: trust,' he said." Hitchens, T. (2020, October 27). Data sharing hurdles stymie JADC2: CSAF Brown. Breaking Defense.

[127] "Autonomy reduces the human workload required to operate systems, enables optimization of the human role in the system, and allows human decision making to focus on points where it is most needed. These benefits can further result in manpower efficiencies and cost saving as well as greater speed in decision-making." DOD, Office of the Undersecretary of Defense for Acquisition, Technology, & Logistics. (2011, October). Unmanned Systems Integrated Roadmap FY2011-2036, p. 45.

[128] "It is not yet clear how or if a commander with responsibility for the multi-domain fight can provide guidance and direction to an artificial intelligence algorithm that is designed to ease his cognitive load." Wallace, W. (2011, August). Multi-domain operations in context. *The Landpower Essay Series*, (20-4). Arlington, VA: Association of the United States Army, p. 4.

[129] In some cases, a decision might not be made even when one is warranted.

[130] The format that AI may be able to use to describe its logic may be natural human language.

[131] See DOD, Defense Innovation Board. (2019, October 31). *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*. "'The United States, together with our allies and partners, must accelerate the adoption of AI and lead in its national security applications to maintain our strategic position, prevail on future battlefields, and safeguard the rules-based international order,' said Secretary [of Defense Mark] Esper. 'AI technology will change much about the battlefield of the future, but nothing will change America's steadfast commitment to responsible and lawful behavior. The adoption of AI ethical principles will enhance the department's commitment to upholding the highest ethical standards as outlined in the DOD AI Strategy, while embracing the U.S. military's strong history of applying rigorous testing and fielding standards for technology innovations.'" Department of Defense. (2020, February 24). *DOD Adopts Ethical Principles for Artificial Intelligence* [Press release]. Retrieved from https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/

[132] "Department of Defense personnel have taken an oath to defend the Constitution of the United States. I myself have taken it many times in my military and civilian careers, and believe strongly in it. As part of that oath, we commit to protecting the American people's right to freedom of speech and to peaceful assembly. I, like you, am steadfast in my belief that Americans who are frustrated, angry, and seeking to be heard must be ensured that opportunity. And like you, I am committed to upholding the rule of law and protecting life and liberty, so that the violent actions of a few do not undermine the rights and freedoms of law-abiding citizens." Esper, M. (2020, June 2). Secretary of Defense Memorandum, Subject: *Message to the Department—Support to Civil Authorities*.

[133] "We will craft and direct coherent communications campaigns to advance American influence and counter challenges from the ideological threats that emanate from radical Islamist groups and competitor nations. These campaigns will adhere to American values and expose adversary propaganda and disinformation." White House (The). (2017, December). *National Security Strategy of the United States of America*. Washington, DC: The White House, p. 35. "As I reminded you in February, I ask that you remember at all times our commitment as a Department and as public servants to stay apolitical in these turbulent days. For well over two centuries, the U.S. military has earned the respect of the American people by being there to protect and serve all Americans. Through your steadfast dedication to the mission and our core values, and your enduring support to your fellow Americans, we will safeguard the hard-earned trust and confidence of the public, as our Nation's most respected institution." Esper, M. (2020, June 2). Secretary of Defense Memorandum, Subject: *Message to the Department—Support to Civil Authorities*.

[134] There is, however, an inviolate moral imperative to be truthful to U.S. citizens and our coalition counterparts and to always "speak truth to power."

[135] Out of operational security concerns, deception operations may require that only a commander and a select few individuals know the deception plan.

[136] "Finally, leaders and soldiers who have met the challenge of conflict in the 21st century, where they served, learned and excelled, will not be satisfied with a return to routine garrison operations. They will demand a training environment that is as complex as the situations they have seen in real life." Wallace, W. (2013, November). Another training revolution coming. *Army Magazine, 63(11)*, p. 40. "Meaningful training needs context." Wallace, p. 42.

[137] "The Army must continue to build trusted teams of professionals that thrive in ambiguity and chaos and who are empowered through a doctrine of mission command to rapidly react to threats and opportunities based on a commander's intent. The MDO concept leverages a critical U.S. military advantage—our people. But the Army does not always design our training programs and exercises in ways that facilitate or require this type of decentralized decision making. More intellectual effort is required to improve training designs that facilitate mission command of MDO given the increased complexity. MDO Concept, p. F-3.

[138] "The approach the Army needs to employ with big data, AI and machine learning is to focus on the force provider functions of training, maintenance, recruiting, garrison support and purchasing to enable greater combat training time at echelons below brigade. Two primary reasons

support this focus: the greater availability of quality data in maintenance and administration to power AI models; and the administratively overburdened nature of leaders at echelons below brigade that detracts from combat-focused and quality training." Storlie, C. (2020, March). Apply artificial intelligence to improve combat training. *Army Magazine,* 70*(3)*, 14-16.

[139] The AFCC-C2 defines national power as all resources available to a nation in the pursuit of national objectives, including diplomatic, informational, military, economic, financial, intelligence, and law enforcement elements

[140] "Opportunities to create a less dangerous world through diplomacy, economic stability, collective security, and national example exist, but military strength is both a complementary and foundational element of National power in a dangerous world. Each element is necessary in combination with the others; however, each alone is insufficient to win a war or maintain a peace." Murphy, P. & Milley, M. (2016, April 7). [Record Version]. Statement by the Honorable Patrick J. Murphy, Acting Secretary of the Army and General Mark A. Milley, Chief of Staff United States Army before the Committee on Armed Services United Sates Senate. Washington, DC, p. 2.

[141] "The foundation of interoperability is broad, spanning all Army [warfighting functions], with human, procedural, and technical domains. Interoperability is often associated with technical issues, however network and [information technology] systems are not the sole components. Human and procedural aspects must also be considered in developing interoperability. The human dimension builds the basis of the mutual understanding and respect that is fundamental to unity of effort and operational success. The procedural dimension ensures that the Army achieves sufficient harmony in policies and doctrine that will enable it to operate effectively with [unified action partners]. AR 34-1.

[142] See the MDO Concept, pages. C-1 through C-4, for a deeper discussion of the MDO operational framework. "Long-range strike systems are a critical component of the Army's contribution to the joint fight. Experimentation has derived what Joint ISR strike needs to be able to do in MDO. The Army must conduct extensive terrain analysis to identify likely positions for threat systems in order to focus multiple layers of ISR over key terrain to identify firing positions. The Army and Joint assets can then que a friendly system to stimulate threat area denial systems for identification. Once adversary systems emit or fire, friendly forces using manned and Robotic and Autonomous Systems to "penetrate" and then "dis-integrate" enemy IADS and fires platforms. In addition to long-range strike capabilities, the range, rate of fire, number of firing systems, and munition effects should be considered in an MDO fight." Identifying Challenges in the Execution of U.S. Army Multi-Domain Operations C2, ISR-Strike, and Sustainment, RAND Arroyo Center Strategy, Doctrine, and Resources Program, PR-4280-A July 2019.

[143] See ADP 6-0, p. 4-1.

[144] See Clarke, S., et al., editors. (2016). *The Ethics of Human Enhancement: Understanding the Debate*. Oxford, UK: Oxford University Press.

[145] [145] "Patrick Lin, lead author of the report, doesn't offer conclusive answers to these and other ethical questions but insists that it's time for an in-depth discussion. 'Given a significant lag time between ethics and technology, it is imperative to start considering their impacts before technologies fully arrive on the scene and in the theater of war,' Lin writes." Matthews, W. (2015, April). Supersoldiers: Can science and technology deliver better performance? *Army Magazine, 65(5)*, p. 41.

[146] "The [Targeted Neuroplasticity Training] (TNT) program seeks to advance the pace and effectiveness of cognitive skills training through the precise activation of peripheral nerves that can in turn promote and strengthen neuronal connections in the brain. TNT will pursue development of a platform technology to enhance learning of a wide range of cognitive skills, with a goal of reducing the cost and duration of the Defense Department's extensive training regimen, while improving outcomes." DOD, Defense Advanced Research Projects Agency. (Undated). *DARPA and the Brain.*

[147] "'The big story here is decoding: We've finally been able to harness the big data of the human brain,' says Dr. Michael Kahana, a professor of psychology at the University of Pennsylvania and the leader of [a second team] team that recently reported memory-boosting success. 'There's a lot of hype in this field, but that's not hype. That's real....We're hoping to develop a fully implantable device and run trials with that device in the next few years,' Kahana says." Powell, C. (2018, April 23). Memory-boosting brain implants are in the works, Would you get one? *NBC MACH.*

[148] See the augmented reality possibilities described at https://www.youtube.com/watch?v=x8p19j8C6VI.

[149] "Reinforcement learning is an AI approach to enable machines to learn from experience; this is distinct from well-known *supervised learning* techniques for AI where researchers provide devices labeled training data in order to learn by example. An essential requirement for applying RL is defining a *reward* structure that captures the designer's intention of what "good" and "bad" behavior is and to what degree. An RL agent interacts with the environment and uses the successes and failures described by this reward to guide its learning and develop a control strategy that will maximize its long-term success. Applications of RL often rely on a simulated environment in order to allow the learning process, which can be very slow to scale and take advantage of computational infrastructure.." U.S. Army FCC and CCDC. (2020, January 9). *Discovery Enabler Concept of Operations—Artificial Intelligence: Reinforcement Learning to Enable Decision Overmatch*. Fort Eustis, VA, p. 3.

[150] DIA's Vision of MARS: Decision advantage for the 21st Century. Defense Intelligence Agency, (May 23, 2019)

[151] "We must create more diverse systems that cannot be compromised all at once, and where different groups of systems can support each other. We must have the capacity to mix and match diverse systems as the situation demands. Diverse systems can work together and operate more resiliently than a collection of homogenous systems. "Kott, A. & Delano, K. (2020, November). Cyber resiliency through the lens of COVID-19. *Army Magazine, 70 (11)*, p. 48.

[152] The U.S. Army Combat Capabilities Development Command's (CCDC) Army Research Laboratory is currently conducting research in the area of flexible antenna radio frequency energy harvesting.

[153] CCDC's Soldier Center is currently researching (Li-Fi) technology.

[154] See EAB Concept, pp. 73-74.

[155] "Similar to other domains, Army leaders and organizations must be capable of employing capabilities in cyberspace, but not to the point of dependency should those capabilities be negated." DA. (2014, Undated). *2014 Army Strategic Planning Guidance*, p. 17.

[156] "Empowering teams to operate more independently may require helping them learn some scientific-thinking skills, which will enable them to make decisions more autonomously and maneuver situationally." Rother, M. & Rosenthal, M. (2018, Summer). An approach to becoming agile in a dynamic world: Helping employees develop scientific thinking empowers them to solve problems and make decisions. *Target*, p. 21.

[157] This is an important consideration as Army forces seek greater authorities and permissions extended to the lowest practical echelons. Greater authorities and permissions are sought for national-level capabilities including intelligence, cyberspace, space, and some physical strike capabilities to allow future Army forces to operate in competition and rapidly transition to conflict effectively. Some allies and other partners may not adequately understand the second and third order effects and the potential for unintended consequences. Forces must have been trained and prepared to employ the capabilities with which they are entrusted.

[158] "Even if the Army is able to implement [mission command] perfectly, it will still need to be able to communicate in a [joint, interagency, intergovernmental, and multinational] environment to successfully complete operations and support national objectives. " DA, Chief of Staff of the Army Strategic Studies Group-I. (2013, July). *Testing Assumptions about the Role of Land Power in 2030 Final Report*, p. 31.

[159] "Culturally, the Army has seen a rise in risk aversion over the course of the last decade that has prompted many leaders to spend considerable time trying to avoid making decisions and pass that responsibility further up the chain of command. The logical outcome is something with which

most soldiers are all too familiar: micromanagement." Doty, J. & Fenalson, J. (2013, July). Mission command and mission accomplishment. *Army Magazine, 59(9)*, p. 16.

[160] Failure should never be viewed as permanent or representative. Instead, it is an opportunity to learn and remediate.

[161] "A further threat to Mission Command lies in the twin areas of blame culture and litigation. Their combined effects are insidious and potentially corrosive. On the one hand, if something goes wrong, somebody is usually blamed. There is a 'fall guy', not least because the Media, with their need for immediate but often simplistic messages, want someone to be seen to be blamed. Mission Command only works in an environment of mutual trust. One important element of that trust is acceptance by the superior of well-intentioned mistake." Storr, J. (2003, Autumn). A command philosophy for the information age: The continuing relevance of mission command. *Defence Studies, 3 (3)*, p. 125. The Army must develop leaders with the moral courage to resist the current culture of blame and litigation.

[162] "Experienced leaders make fewer mistakes; the risk averse will make none. However, the absence of mistakes is a deceptive metric for judging and selecting leaders. What is far more significant is the ability of leaders to learn and adapt from mistakes and discern and avoid the patterns that led to failure. Leaders who have not made mistakes have not demonstrated the ability to recover and adapt. The future leader development process must offer opportunities to refine judgment in the face of risk, with wide potential for failure in training to identify and develop resilient leaders capable of coping with setbacks." Corbett, A. (Undated). *Mission Command*. Norfolk, VA: Naval Warfare Development Command, p. 16.

[163] "Directed reading and study, coupled with the training and education of our leaders in the institutional Army and their self-study, will create the warrior that is needed for the remainder of the 21st century and beyond." Shaw, S. (2013, October-December). Rally point for leaders: Building an organization's mission command culture. *Infantry, 102(4)*, p. 25.

[164] "Although they may seem inconsequential, exit interviews can have a profound impact. Leaders have the rare opportunity to get unfiltered feedback from their soldiers, and soldiers get confirmation that their superiors care enough to ask for their opinion. This small, seemingly simple act can have a great impact on an organization. Machak, J. (2015, June). Better exit interviews: Opportunities for organizational improvement. *Army Magazine, 65(6)*, 56-57.

[165] Unified action is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1)

[166] See ADP 5-0, pp. 2-23 through 2-24 for its discussion of developing simple, flexible plans through mission orders, optimizing available planning time, and focusing on the right planning horizon.

[167] "Noncommissioned officers (NCOs) lead, train, and execute missions in the U.S. Army with skill and precision, yet the education and training of the enlisted force in the operations field is not standardized. To improve mission readiness, the Army would benefit by establishing an enlisted military occupational specialty (MOS) specializing in operations, ensuring a standardized product." Sheets, C. (2020, April 10). Is it Time for an Operations MOS? *NCO Journal.*

[168] "'It's the second oldest challenge for artillery,' [Brig. Gen. John] Rafferty [Long-Range Precision Fires Director at Army Futures Command] told me, ever since 19th century cannon began to shoot over the horizon at targets their gunners couldn't see. 'The oldest challenge is shooting farther, the second challenge is the sensor to shooter part: How do you minimize the time between the observation of the target and the delivery of the effects?'... Rafferty's counterpart for air and missile defense is Brig. Gen. Brian Gibson. 'It's about connections and access to the data,' Gibson told me in a recent interview. 'Sharing the right data with the right user at the right time, along latency timelines that are useful… is really where the trick to this puzzle lies.'" Freedberg, S. (2020, May 18). Project convergence: Linking Army missile defense, offense, & space. *Breaking Defense.*

[169] "AI may allow China to realize its long-standing, information-centric military strategies. The American military tends to focus on how AI can enable lethal attacks against opposing forces. Chinese strategists tend to argue that AI technologies should be used kinetically and non-kinetically to dominate information systems and networks, to effectively paralyze an opponent's joint force. Information warfare and information control are at the heart of the PLA's approach to warfare — and AI. Countering China's strategy will require a defensive and offensive use of new AI technologies. In a future confrontation, the U.S. military will need to employ AI and autonomous capabilities to enable and defend its information system-of-systems while simultaneously using AI technologies to attack China's information-centric strategy and capabilities." Dahm, M. (2020, June 5). Chinese debates on the military utility of artificial intelligence. War on the Rocks.

[170] "Achieving the Joint Chiefs' vision will require people—the Joint Force's primary source of competitive advantage—to continuously adapt and innovate to maintain their competitive edge." 2018 NMS Description, p. 5.

[171] "The minds of our officers are the most lethal weapon in gray zone competitions." Kay, L. (2016, July 27). Managing the Gray Zone is a gray matter challenge. *Small Wars Journal.*

[172] "Commanders must deliberately create and foster conditions favorable to mission command so that ever disparate formations and capabilities are ready to act upon mutual recognition or in response to a battlefield development." MDO Concept, p. 21.

[173] "Now their Army and their lives will be dominated by policies, regulations—and e-mail. Of course, modern communications technology has enabled remarkable connectivity on the battlefield during the past decade's wars, but its unintended and corrosive effects in peacetime will rapidly wear down the initiative required by Mission Command." Barno, D. (2014, July 10). The Army's next enemy? Peace. *The Washington Post.*

[174] "The Multi-Domain Operations concept was conceived by the Army, but it is inherently joint in nature. It goes far beyond AirLand Battle, which combined its two eponymous domains in a defined area of operations. Multi-Domain Operations expands the fight to the sea, into space and beyond, to the synthetic domain of cyberspace. It acknowledges that to achieve dominance on land, the Army must work with the Navy, Air Force, Marine Corps and now, the Space Force, to rapidly converge effects across multiple domains at the decisive place, which might be anywhere on, or off, the planet." MacFarland, S. (2020, March). Joint operations need a guiding hand. *Army Magazine, 70(3)*, p. 8.

[175] "Acting and reacting at the speed of multidomain warfare, executing cross-domain fires and maneuver, will demand an unprecedented degree of integration between services at multiple echelons, and therein lies the problem." MacFarland, S. (2020, March). Joint operations need a guiding hand. *Army Magazine, 70(3)*, p. 8.

[176] "To prepare the Joint Force for employment, exercises build readiness, interoperability, and the mutual trust required for a joint combined arms approach to global campaigning. Those exercises are key to building interoperability, relationships, and capabilities of allies, partner nations, and interagency partners, as well as enabling units and leaders to "punch above weight class" when necessary. Exercises can also facilitate near-term experimentation to rapidly incorporate innovative ideas and disruptive technologies that promote competitive advantage." 2018 NMS Description, p. 4.

[177] "To conduct MDO in a highly contested environment, Army forces require the ability to consolidate gains through clear demonstrations of U.S. security commitments to partners through combined exercises, training, and other presence activities." MDO Concept, p. B-2.

[178] However, as repeatedly suggested, all Services should adopt the same processes for standardization, to contribute to dynamic task organization, and to enable rapid development of cohesive and effective teams.

[179] Well trained, culturally astute, and adequately resourced liaison teams (including skilled linguists when necessary) having and maintaining a clear understanding of their commander's intent will remain critical to unified action partner interoperability.

[180] This should include training and use of the joint operations planning process. "Although exposed to this during Intermediate-Level Education, [ILE] few Army majors know it well." Grigsby, W., Matlock, P., Norrie, C., & Radka, K. (2013, November-December). Mission command in the regionally aligned division headquarters. *Military Review, XCIII (6)*, p. 6. If the joint operations planning process was adopted by the Army outright, this would not be as a great a concern as it would likely be integral to ILE curriculum.

[181] "To preserve its joint advantage, the U.S. military must reverse this trend [diluting joint education and curtailing joint assignments] and recommit to building military leaders who can think jointly, operate jointly, and lead jointly. Without a renewed emphasis on joint officer development, the United States stands to cede competitive space to global adversaries such as China and Russia." Sukman, D. & Davis, C. (2020, March-April). Divided we fall: How the U.S. force is losing its joint advantage over China and Russia. Military Review, p. 50.

[182] "In the current dynamic operating environment, the U.S. Army will have only days, not weeks or months, to integrate with [unified action partners] in key functions and capabilities. Therefore, interoperability must become a fundamental condition of how the Army plans to fight tonight and tomorrow, and prepares to fight in the future. The smaller size of the current Army combined with the nature of Multi-Domain Operations (MDOs) across air, land, maritime, space, and cyberspace requires that the Army train to fight alongside and with [unified action partners]. The Army, as part of a Coalition, must be able to leverage total Army and [unified action partner] capabilities in ways that enhance the accomplishment of U.S. and Coalition objectives." AR 34-1, p.2.

[183] The Army specifies three other methodologies: 1) rapid decision-making and synchronization process, troop leading procedures, and Army problem solving. The rapid decision-making and synchronization process is a decision-making and planning technique that commanders and staffs commonly use during execution when available planning time is limited. The troop leading procedures provides small-unit leaders an eight-step framework for planning and preparing for operations. Where the other four methodologies are designed for planning operations, Army problem solving is a general methodology available for leaders in identifying and solving a variety of problems. ADP 5-0, pp. 2-18 thru 2-19.

[184] MDO Concept's influence on other integrating warfighting processes should be covered in other functional and supporting concepts as part of the Army's entire concept framework.

[185] Of course, this may first require careful review to make any minor modifications—agreed to by all Services—to account for any critical Service- or domain-specific equities that have not already been considered.

[186] However to ensure the greatest understanding of the concept's ideas within the Army, this concept uses approved Army doctrinally terminology unless it does not adequately describe the future subject matter area.

[187] "The military best able to leverage all domains and environments to maneuver will create the synergy needed to improve their correlation of forces and means (inclusive of military and non-military means across the competition continuum). Conversely, preventing adversaries the ability to use several domains and environments simultaneously will put them at a disadvantage." MMDO, p. 14.

[188] "It is unlikely that the mission command tools of today will meet the demands of tomorrow's MDO environment. It would be difficult and perhaps impossible for a single person to understand, visualize, describe and direct across five inter-related domains in real time, but there is also not currently any contemporary tool or technology which would enable one to do so. There are efforts to provide multi-sensor, multi-shooter solutions across services and capabilities; technical solutions that can match sensors to targets to shooters are necessary, but they are insufficient to fully solve a commander's problem of battlefield visualization and anticipation of opportunity….The ability for commanders to visualize and direct cross-domain actions that create opportunities for their subordinate commands is not pre-ordained. The art, science, tools and training of [command and control] must co-evolve with the MDO concept for it to be executed." Wallace, W. (2011, August). Multi-domain operations in context. *The Landpower Essay Series*, (20-4). Arlington, VA: Association of the United States Army, pp. 4 & 5.

[189] Commander's prioritization of his or her information needs provides a critical filter for the information inputs into the future command post constellation and helps reduce the staff's cognitive burden and prevent information overload.

[190] "Physical, virtual, and cognitive capabilities across the domains, environments, and functions often possess substantially different time characteristics that govern how they can be employed. When creating and exploiting windows of superiority, commanders must visualize and execute combined arms maneuver in new ways because the varied characteristics of different capabilities that must be converged at a place or places to achieve a purpose impose unique time considerations to operations." MDO, p. C-7.

[191] "*Prepare a clear mission statement, intent, and concept of operations.* Focus on key tasks for intent. Make the concept of operations - the how, when and where of the plan -the centerpiece of your orders and assure it is understood two levels down. The concept guides your subordinates for as long as the plan holds up. It preempts a lot of questions and uncertainty if it is well done. We have put so much emphasis on commander's intent, and more recently on over-abbreviated mission templates, that our ability to articulate clearly how we will execute operations is diminished. The cost is that we fail to get the most out of our organizations initially and we deviate from our plans prematurely." McMaster, H. (2016, March 31). Lieutenant General Don Holder's free, non-binding advice for battalion and squadron commanders. *The Strategy Bridge*.

[192] "The United States is highly unlikely to regain its competitive advantage through like-for-like replacements of its legacy platforms with incremental improvements while remaining beholden to industrial age notions of warfare focused on individual weapon systems focused on inflicting attrition." Deptula, D. (2020, July 9). Moving further into the information age with joint all-domain command and control. *C4ISRNET*.

[193] "System warfare analysis to defeat threat technological systems is not the 'silver bullet' to winning across the future competition continuum. However, without a systems approach as one of the primary methods focused on achieving one of the four defeat mechanisms (isolation, dislocation, disintegration, or destruction), the probability of achieving the intended purpose of the operation is unlikely." EAB, p. 36.

[194] See EAB Concept, pp. 33-36 for its entire discussion of systems warfare analysis.

[195] See Johnson, D., et al. (2019). *The U.S. Army and the Battle of Baghdad: Lessons Learned—And Still to be Learned*. Rand Corporation. Santa Monica, CA.

[196] Although doctrine may need to be revised to emphasize the point, the operations process itself is sufficiently broad to allow the incorporation of unified action partners into planning, preparation, execution, monitoring, and assessment. Specific methodologies like the military decision making process, on the other hand, may need careful revision to ease and facilitate greater whole-of-government and partner integration.

[197] "Flexible command relationships allow the rapid reallocation of multi-domain capabilities and formations across functional components and echelons to achieve convergence. Flexible command relationships also allow the creation of favorable force ratios through rapid task organization and re-organization of reinforcing fires and capabilities among echelons." MDO, p. 23.

[198] "'What we found, at least in the Army, is putting the developers as integral members of the team...because they see the problem and they understand the sense of urgency for a particular problem, they can develop a solution,' [LTG Steven] Fogarty [Commander, Army Cyber Command] said. 'In a couple of operations that we've conducted over the last 45 days, we've watched a developer come into a problem, break it down very, very rapidly, develop a script, fix the tool, modify a tool...within an instant...[hours] not days or weeks, we're able to create that solution.'" Pomerleau, M. (2019, September 5). The Army wants more coders alongside operators. *Fifth Domain*.

[199] "This [mission] vagueness means that a campaigning military organization must learn and adapt as fast as it can, at multiple levels at once, and it must learn and adapt in ways that are unique to every echelon while drawing on knowledge and support from peers, superiors, and subordinates alike." Wass de Czege, H. (2012, May-June). Difficult missions: What logic to apply and what action to take. *Military Review, XCII(3)*, p. 57.

[200] The AFCC-C2 defines Army learning organizations as Army organizations that cultivate the processes and activities that facilitate the continuous and collective acquisition of skills and knowledge, and that then apply those learning outcomes to achieve a shared vision of the future.

[201] "Achieving cognitive superiority through technological advantage and augmentation translates into being able to gather, decipher, process and understand tremendous amounts of data and information faster than the enemy. Fusing this capability with cloud-enabled computing, robotics, artificial intelligence and virtual reality augments the decision-making process, multidomain operations, and the learning and adaptability of military organizations at the tactical, operational, and strategic levels. Communicating this knowledge internally and externally faster than a competitor is imperative. It provides the ability to get inside an enemy's decision cycle, influence their perceived reality and impose our will." Schmidt, T. (2020, June). Playing head games is more crucial than ever. *Army Magazine, 70 (6)*, p. 15.

[202] Lethal miniature aerial munitions is one example of precision munitions that are complicating airspace management. Future high- and low-altitude, long-endurance surveillance and communications systems and unmanned aircraft used for sustainment also make the management of airspace more complex.

[203] "Accurate, real-time data 'provides decision-makers with timely, accurate information that helps us fight and win wars,' [Army Undersecretary James] McPherson said, especially in a 'complex, data-saturated landscape.'"*Better Data Management Can Win Wars*. (2020, July 16). Association of the United States Army.

[204] Sensors include those that future Army forces use to see (or sense) themselves. For example, this includes sensors used to monitor Soldier health status or the maintenance status of vehicles and equipment.

[205] "Success against a technologically advanced enemy in the future will require us to think much differently—about both the tools we use in war and, more importantly, how they work together. In fact, the most important element of future combat will not necessarily be warships, combat vehicles, aircraft or satellites. It will be a battle network that connects them to work in unprecedented harmony…. The network would leverage data, artificial intelligence and machine learning so that we know the location and movement of both friendly and enemy forces at all times. U.S. forces operating on land, sea, air, and in space and cyberspace—the major 'domains' of modern warfare—will be able to share information continuously and call on each other when needed." Goldfein, D. & Raymond, J. (2020, February 27). America's future battle network is key to multidomain defense. *Defense News*.

[206] Not every Soldier needs the full complement of network capabilities. The communications network must achieve the right balance of voice and data capabilities tailored to each organization and echelon.

[207] "Some portion of the joint force will be able to maneuver directly against key objectives from ports of embarkation, without reliance on fixed intermediate or forward bases, identifying and changing those objectives enroute. This will put a premium on enroute communications for command and control." DOD, Joint Staff. (2012, January 17). *Joint Operational Access Concept, Version 1.0*, p. 31. See also Flynn, C. & Richardson, J. (2013, July-August). Joint operational access and the global response force: Redefining readiness. *Military Review, XCIII (4)*, p. 40.

[208] "The forward presence of the commander on the battlefield remains critical for ensuring mutual trust between commanders and subordinates in executing mission command. While digital technologies enable commanders to attain unprecedented levels of situational awareness, nothing substitutes for the physical and moral presence of the commander on the battlefield." Higginbottom, M., & Adkison, R. (2012, July). At the tip of the spear: Mission command on the move in a networked force. *Army Magazine, 62(7)*, p. 32.

[209] "Expeditionary capability describes the ability to promptly deploy combined arms forces on short notice to any location in the world, capable of conducting operations immediately upon arrival. Expeditionary operations are entirely dependent upon joint air and maritime support." ADP 3-0, p. 1-10. In future operations, physical distances between units, even at lower tactical echelons, will likely increase.

[210] "A significant part of this strategy requires advancing and adopting spectrum-dependent technologies that will lead to more spectrally efficient, flexible, and adaptable [spectrum-dependent system] capabilities." DOD, Chief Information Officer. (2013, September 11). *Electromagnetic Spectrum Strategy 2013: A Call to Action*, p. 6. Greater dispersion may negatively affect ground units' ability to provide mutually supporting direct fires necessitating a greater dependence on the simultaneous employment of ground forces with manned and unmanned, rotary-, and fixed-wing aviation and fires to seize, retain, and exploit the initiative.

[211] *Reach* is the collaboration, information sharing, and capability integration with any organization and/or individuals, regardless of location, echelon, or affiliation. See also the glossary for related definitions of *intelligence reach* and *reachback*.

[212] "Interoperability is and will remain one of the key requirements for the Army. To conduct combined arms maneuver with [unified action partners], the Army must develop and advance a base technological architecture into which the Army and partners can easily 'plug and play.'" AR 34-1, p.2.

[213] Mission partner environment is the "capability framework in which combatant command partners plan, prepare and execute operations at an appropriate, single security classification level, with a common language. It provides strategic, operational, and tactical flexibility for all commanders to execute C2 by providing the means to clearly communicate the commander's intent to achieve maximized operational effects with all mission partners." AR 34-1, p. 30.

[214] "The burden thus falls on the Joint Force to create the information environment that will facilitate partner integration. Any such environment should provide the ability to collaborate across multiple security levels without the need for segregated hardware systems." CCJO, p. 13.

[215] The synchronization of joint and multinational partners' activities with Army operations is important regardless of whether the Army headquarters is operating as a JTF or JFLCC headquarters, or simply a subordinate organization within the JTF or JFLCC.

[216] A common operating environment provides a technical "ecosystem" to allow systems and applications to natively interoperate with each other. Even if the system appears to be unique and stand-alone, this ecosystem will allow the system to easily interoperate with others if the need later emerges. See the Joint Concept for Command and Control for a greater discussion of the ecosystem characterization of the common operating environment.

[217] "…headquarters need a cross-domain architecture that allows for rapid transfer of information. They also need hardware, such as additional server stacks, to establish a partnered mission command network." Grigsby, W., Matlock, P., Norrie, C., & Radka, K. (2013, November-December). Mission command in the regionally aligned division headquarters. *Military Review, XCIII (6)*, p.7.

[218] "DOD will also continue to adopt new tools and techniques to manage the spectrum more effectively, making our spectrum operations more agile. " DOD, Chief Information Officer. (2013, September 11). *Electromagnetic Spectrum Strategy 2013: A Call to Action,* p. 6. This may be achieved through greater automated or autonomous capabilities which can also reduce the network management burden on units.

[219] The delivery of software patches and version updates will be simplified and eased across entire Army.

[220] Department of the Army, Chief Information Officer/G-6. (2016, March). Shaping the Army Network: 2025-2040, p. 12.

[221] A tailorable battlespace visualization based on common, standardized, shareable, and secure data leads to shared *awareness*, while collaboration leads to discernment of the relationships between multiple operational and tactical variables and shared *understanding*.

[222] The right balance and mixture of collaborative capabilities is important. Too many of the same type of applications or devices can overwhelm an individual's and organization's ability to train and master them.

[223] Relevant information is all information of importance to the commander and staff in the exercise of command and control.. See ADP 6-0, p. 3-5. Relevant information includes position location information; symbols; graphic control measures; intelligence, operational, and unit status information; civil considerations; and information on the OE including political, military, economic, social, information, infrastructure, physical environment, time; area, structure, capabilities, organization, people, events; and sewage, water, electricity, academics, trash, medical, security variables from disparate information and intelligence systems. Relevant information must also include those portions of space, cyberspace, the EMS, and the IE that are relevant to all-domain battlespace visualization. overall shared understanding, and rapid, quality decisions.

[224] A tailorable battlespace visualization based on common, standardized, shareable, and secure data will be critical to achieving these operational and readiness qualities. However, a tailorable battlespace visualization based on common, standardized, shareable, and secure data does not equate to an omniscient picture. While everyone may have the same picture and data, the information displayed will never represent all operational and mission variables relevant to decision making and at each echelon. What is relevant to a particular situation may not be common. Hence, decentralized decision making by empowered subordinates with greater situational understanding of their particular area of operation will remain essential to success in future MDO.

[225] Other ground forces include the U.S. Marines Corps and elements of U.S. Special Operations Forces. This can also extend to coalition ground forces.

[226] "All aspects of the operations process" implies that it also supports other supportive warfighting functions' integration processes such as such as intelligence preparation of the battlefield, information collection, targeting, protection assessment, risk management, movement control, supply distribution, and other sustainment processes.

[227] Future decision-support tools will be designed to provide staff-like functions such as resource allocation and positioning, question answering, mission planning, execution monitoring, risk and opportunity recognition, and recommendations allowing commanders to operate above their experience level.

[228] Mobile and personal computing continues to grow. Army applications must embrace this trend.

[229] The synthetic training environment is the convergence of virtual, constructive, gaming, and augmented reality training environments into a single training environment capable of interacting and augmenting live training to provide a cognitive, collective, multi-echelon training and mission rehearsal capability for the operational, institutional, and self-development training domains.

[230] "And what if the enemy hacks and jams your network, taking away all your digital information? 'That's why we plan for the worst,' [Gen. James McConville, Army Chief of Staff] told the Brooking webcast. 'That's why you have highly trained, disciplined, fit…and lethal forces that can operate when these systems do go down. That's all part of the Primary, Alternate, Contingency, Emergency-type plans that you build into your organizations,' McConville continued–a philosophy of quadruple-redundant backups known by the Army acronym PACE. 'So if you have a system where everything is just working perfectly, [then] you've got tremendous overmatch, [but if] someone takes that down…that's where you start to go to your backup plans.'" Freedberg, S. (2021, March 30). Army won't repeat mistakes of FCS: Gen. Murray exclusive. Breaking Defense.

[231] See DOD. (2020, October 08). *DoD Data Strategy*, pp. 6-9.

[232] Vehicle-based command nodes can help eliminate the requirement for transit cases and cabling associated with today's command posts and can help minimize the number of tents, trailers, and supporting environmental control systems.

[233] "'In a decisive-action fight with a peer-level competitor, when we're taking ground and moving, when bullets start flying, how willing will these civilian contractors be able to fix that digital system' as movement into harm's way commences, [Chief Warrant Officer 3 Heath Stamm] asked. 'We haven't fought a frontline fight in a long time,' he pointed out. 'People say we were in Afghanistan, but we were static. When we start moving and taking ground again, that's going to change the dynamics. Everywhere you see a contractor in the field, you should probably look and say where's the warrant officer that needs to replace him,' he continued. Stamm summed up his feelings for warrants taking control: 'I'm the technical expert on that system. One, I'm cheaper; two, when bullets start flying, I'll continue working on that system.'" Vergun, D. (2016, January 19). Solarium: Warrants need training, Army over-relies on contractors. *Army.mil*.

[234] However, size, weight, and power considerations must be balanced against performance requirements and fiscal realities. Critical decisions will need to be made as to what level of performance is "good enough." Energy efficiencies are critical to the establishment of early-entry command nodes in austere environments. Increasing the battery duration for digital systems and developing small, lightweight, and mobile generators (possibly including a solar array) will be key to maintaining continuity of command. Consolidated power solutions may gain tremendous efficiencies but they may serve to limit CP dispersion.

[235] Enduring CP functions include: 1) receiving information, 2) analyzing information, 3) distributing or sharing information, 4) making plans, 5) issuing orders or directives, 4) monitoring and assessing operations, 4) making anticipatory and proactive recommendations, and 5) integrating and synchronizing resources.

[236] In conjunction with a robust, beyond-line-of-sight network transport, this imperative could allow the largest portion of the commander's staff to operate from home station.

[237] The proliferation and use of unmanned aircraft systems to conduct cross-domain reconnaissance, surveillance, and targeting increases the threat to command post survivability.

[238] Commercial off-the-shelf technologies are of particular concern as they as not routinely hardened for military operations.

[239] Some refer to this as "redundancy." However, some understand redundancy to connote "unneeded" duplication. The duplication referred to here is specifically designed into the command post to ensure survivability of critical functions and capabilities.

[240] Robotics and autonomous systems will improve the agility and mobility of command posts and reduce the signatures of command nodes by dispersing the emitters normally associated with them.

[241] "To succeed in competition while maintaining preparedness for combat, Army forces gain and maintain initiative continuously. Across diverse AORs, the Army does this through enabled EAB formations dynamically postured with the necessary capabilities, capacities, and authorities to create windows of superiority and converge multi-domain effects against enemy vulnerabilities." EAB Concept, p. 55.

[242] "The Army's posture, capabilities (to include necessary authorities), and readiness to execute Multi-Domain Operations deter adversaries from escalation, counter their information and irregular warfare, undermine their efforts to coerce U.S. partners with the threat of armed conflict, and set conditions in the event of conflict." MDO Concept, p. viii.

[243] "Although important, it is not just the size of the Army that matters, but rather the right mix of capacity, readiness, skill, superior equipment, and talented Soldiers, which in combination, are the key to ground combat power and decision in warfare." Murphy, P. & Milley, M. (2016, April 7). [Record Version]. Statement by the Honorable Patrick J. Murphy, Acting Secretary of the Army and General Mark A. Milley, Chief of Staff United States Army before the Committee on Armed Services United Sates Senate. Washington, DC, p. 4.

[244] "However, should war occur, we must terminate the conflict on terms favorable to the United States—this requires significant ready forces and the operational use of the Army National Guard and Army Reserve. Only the Army provides the President and the Secretary of Defense the ability to rapidly deploy ground forces, ranging in decisive ground capabilities from Humanitarian Assistance and Countering Terrorism to high-end decisive operations. Moreover, the Army conducts these operations in unilateral, bilateral, or coalition environments across the range of conflict from irregular warfare to major combat operations. In the end, the deployment of the American Army is the ultimate display of American resolve to assure allies and deter enemies." Murphy, P. & Milley, M. (2016, April 7). [Record Version]. Statement by the Honorable Patrick J. Murphy, Acting Secretary of the Army and General Mark A. Milley, Chief of Staff United States Army before the Committee on Armed Services United Sates Senate. Washington, DC, pp. 4-5.

[245] An example of this could be a Joint Interagency Task Force (JIATF) construct to enable the whole-of-government approach during competition.

[246] "Army forces partner with ministries of defense to develop and shape the environment and establish strategic frameworks that employ forces, build professional military institutions, and partner with European Allies to achieve shared strategic objectives." Murphy, P. & Milley, M. (2016, April 7). [Record Version]. Statement by the Honorable Patrick J. Murphy, Acting Secretary of the Army and General Mark A. Milley, Chief of Staff United States Army before the Committee on Armed Services United Sates Senate. Washington, DC, p. 3.

[247] "Future EAB formations *never ceded the initiative* and always seek to be anticipatory versus reactive….EAB formations must persistently *[sense] and understand* the environment across all the domains to identify adversary or enemy influence….Future EAB forces continually compete throughout the extended multi-domain environment to understand all actions that may shape the environment to an adversary's advantage. Seeing where and how an adversary operates allows EAB commanders and staffs to discern hidden intentions and predict possible future actions." EAB, pp. 17-18.

[248] While the military decision-making process may need to change considerably, the operations process (of which planning is part) is sufficiently broad to account for future changes in the character of war.

[249] "Every echelon requires three kinds of specialized capabilities. The first of these is support to the functioning of the commander and staff—to facilitate decision making and other aspects of battle command, and to provide "housekeeping," protection and mobility. The second of these is to support the functioning of the line organizations, providing capabilities that are periodically required and distributed by mission need and to weight the main effort. The third of these specialized capabilities is required to set conditions for the success of the weighted line organizations." Wass de Czege, H. (2002, April). Using information technologies to reduce the Army's echelons. *Army Magazine*, p. 9.

[250] All headquarters are responsible for planning and arranging the actions of subordinate elements in such a way that the combined effects achieve a higher objective. Ultimately, tactical military operations must, collectively, achieve the operational level military objectives. Achievement of military operational objectives should contribute to fulfilling the strategic political objectives. The headquarters at each succeeding echelon of command is responsible for ensuring that the actions of its subordinate formations contribute to the success of the overall operation. As such, long- and short-range plans are relative terms based on the operational framework and the specific echelon's time horizons.

[251] "The Joint Force currently converges capabilities through episodic synchronization of domain-federated solutions. Future operations against a near-peer threat, however, will require the Joint Force to conduct continuous and rapid integration of multi-domain capabilities to gain cross-domain overmatch at decisive spaces. Decisive spaces are locations in time and space (physical, virtual, and cognitive) where the full optimization of the employment of cross-domain capabilities generates a marked advantage over an enemy and greatly influences the outcome of an operation. Convergence has two advantages over single-domain alternatives: the creation of cross-domain synergy and the layering of options to enhance friendly operations and impose complexity on the enemy. Through convergence, multi-domain capabilities are brought together in stimulate-see-strike or see-strike combinations that disrupt, degrade, destroy or dis-integrate enemy systems or create windows of superiority to enable friendly exploitation of the initiative." MDO Concept, p. 20.

[252] Battle damage assessment is "an estimate of damage composed of physical and functional damage assessment, as well as target assessment, resulting from the application of lethal or nonlethal military force." (JP 3-0)