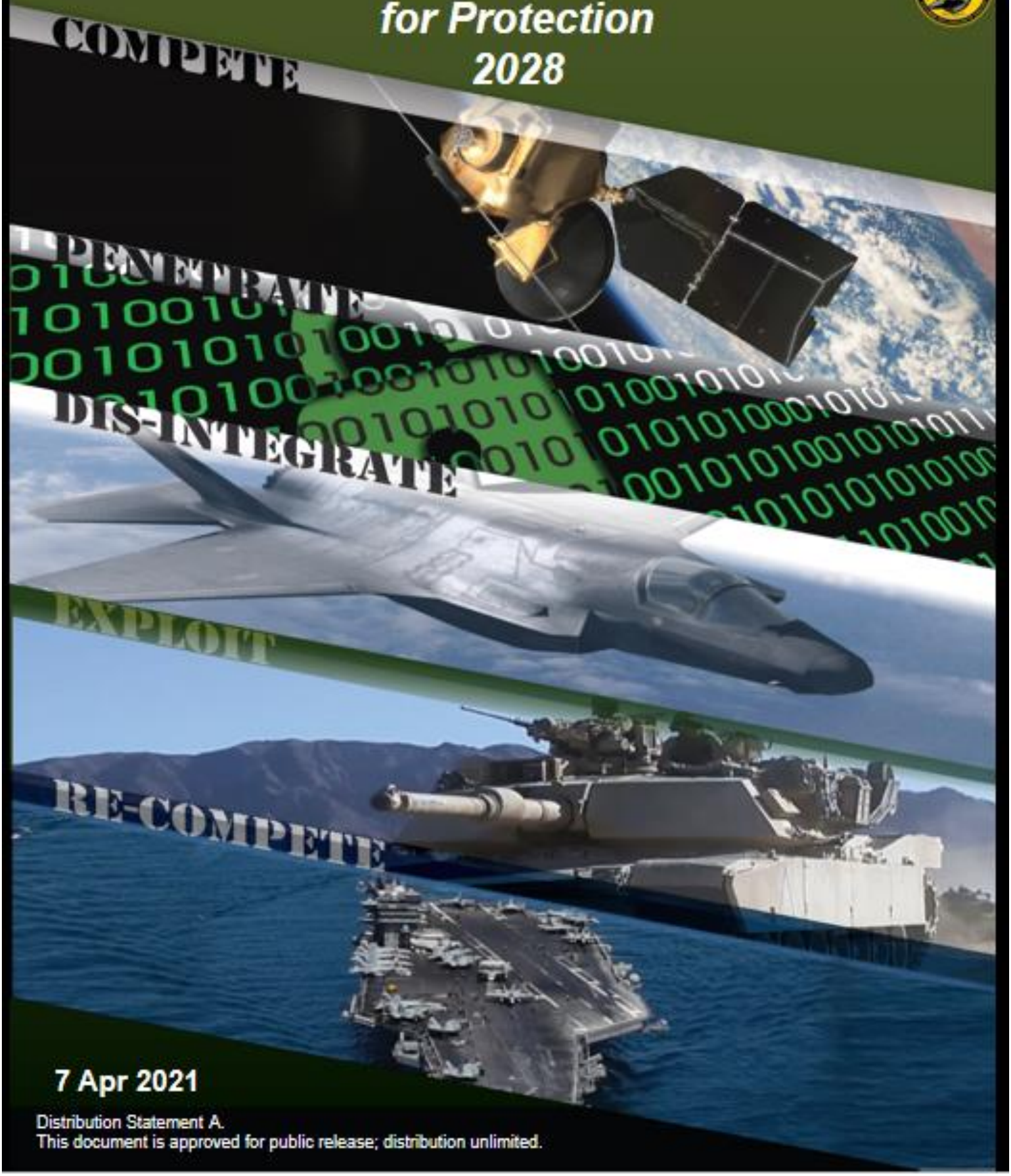
AFC Pamphlet 71-20-7

Army Futures Command Concept for Protection 2028



7 Apr 2021

This page left intentionally blank

Foreword

From the Director
Futures and Concepts Center, Army Futures Command

The Protection warfighting function is essential to preserving future capabilities in multi-domain operations. The future expanded operational environment will be more complex, faster, and lethal. Adversaries will create stand-off in both competition and armed conflict, and will seek to achieve strategic and operational objectives through actions short of armed conflict. Enemies will combine capabilities from all domains, counter friendly force strengths, and create overmatch in many areas. The future force must preserve critical capabilities, assets, and activities against threats in all domains, the electromagnetic spectrum, and the information environment; deny enemy freedom of action; and enable access so that commanders can apply maximum combat power to compete, penetrate, dis-integrate, exploit, achieve our military objectives, and return to competition on more favorable terms.

The *Army Futures Command Concept for Protection* describes the capabilities required for protection in 2028 and how Army forces could perform these tasks to enable multi-domain operations. The protection warfighting function is an integrating function that brings together many entities to collectively solve Army problems. This concept outlines how protection expands beyond passive actions that prevent enemy activities in friendly areas, and is more active across broader spaces. Protection strives to deny, degrade, and disrupt enemy positions of advantage; freedom of action; the ability to destroy friendly critical capabilities, assets, and activities; and enemy influence over third party actors, surrogates, proxies, and irregular criminal threats across the operational environment including force projection and generation platforms in the homeland and abroad. Commanders require the ability to see the adversary, deny them anonymity, counter specific strengths, achieve positions of advantage, and expand and exploit gained areas. Looking forward, the Army must develop capabilities that can support and integrate with our joint, interagency, interorganizational, and multinational partners to expand the protection capability, increase capacity in competition, and operate at scale in armed conflict.

This concept serves as a basis for modernization actions for Army protection warfighting capabilities. It also identifies implications for other warfighting and supporting functions. It will inform experimentation, capability development activities, and other future force modernization efforts to achieve multi-domain operations in the 2028 future force.

D. SCOTT MCKEAN
Lieutenant General, USA
Director, Futures and Concepts
Center

This page left intentionally blank

Executive Summary

1. Purpose.
Army Futures Command Concept for Protection 2028 describes how the Army preserves the force from threats in all domains, generating stand-off so commanders can apply maximum combat power to accomplish the mission. It describes the ever-changing operational environment and provides commanders components of the solution, which include actions those commanders may take and formations available for employment at echelon, throughout the expanded battlefield and across the competition continuum as part of multi-domain operations.

2. The problem.
How do Army forces, as elements of the joint force, achieve all domain protection on the expanded battlefield to preserve combat power, power projection, freedom of action in depth, and access to decisive spaces to create protected windows of superiority while achieving U.S. strategic objectives and deterring adversaries in competition, or when necessary, enabling the rapid transition and ability to prevail in armed conflict, and a return to competition on more favorable terms?

3. Central idea.
Army forces, as part of joint, interagency, intergovernmental and multinational teams, conduct protection activities in all domains, the electromagnetic spectrum and information environment, to preserve commanders' critical capabilities, assets, and activities; deny threat and enemy freedom of action; and enable access to achieve protected windows of superiority.

4. Components of the solution.

a. Preserve critical capabilities, assets, and activities (CCAA). Preserving CCAA is necessary for the future force to survive and win in large-scale combat in multi-domain operations, and is the foundation for resilient and survivable individuals, formations, and operations across the battlefield and the competition continuum. Example CCAAs may include the individual Soldier, mission and objective related readiness, force projection, combat power and formations, access to decisive spaces, decisive points, connections, sustainment assets, facilities, lines of communications, main supply routes, information, understanding, and infrastructure.

b. Deny threat and enemy freedom of action. Passive measures are insufficient to preserve CCAA and prevent threats in all domains, the electromagnetic spectrum, and the information environment, including obstacles and hazards, from degrading mission accomplishment and applying more combat power at sub-optimal times and places. The protection warfighting function serves a role in targeting, all domain command and control, and the operations process. Active protection processes should help characterize the threat and nominate protective denial or defensive countermeasures, thereby expanding the preservation of CCAA throughout all domains, the electromagnetic spectrum, and the information environment. Denying enemy freedom of action is the active approach preventing the enemy's ability to see, understand, and strike friendly force CCAA. Coordinating all domain defense with fires, maneuver, and command and control creates the opportunity to deny enemy antiaccess and area denial, and preserve CCAA.

Commanders can actively deny enemy freedom of action using a host of protective measures that limit enemy access to positions of advantage.

c. Enable access. The future force enables access to denied spaces through projecting power from the strategic support area, penetrating, dis-integrating, and exploiting enemy antiaccess and area denial, and expanding into the enemy's area of stand-off. As friendly forces push forward, security and protection will hold the gained area while creating and exploiting windows of superiority to further pressure enemy defenses. To enable access, future Army forces require access to space, the electromagnetic spectrum, and the information environment through distributed and resilient networks to provide all domain-sensing capabilities to continuously detect and monitor enemy activity across the battlefield and competition continuum. These systems, combined with fires and quick-reaction forces, enable friendly forces to control terrain, thus preventing, disrupting, deterring, and defeating enemy operations anywhere on the battlefield. Ultimately, the objective is to maintain momentum, consolidate gains, and make possible the permanent gain of temporarily-controlled terrain.

5. Summary.

Army Futures Command Concept for Protection 2028 describes how the Army preserves the force from threats in all domains, generating stand-off that enables commanders to apply maximum combat power to accomplish the mission. It describes protection outcomes and requirements integrated across multiple proponents on an expanded battlefield and across the competition continuum as part of multi-domain operations. This concept contributes to experiments, studies, analyses, and continued development of the Army operating concept and the Army concept framework. The required capabilities to achieve the central idea enable modernization.

Figure 1. Logic Chart

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

7 Apr 2021

Force Management

ARMY FUTURES COMMAND CONCEPT FOR PROTECTION 2028

FOR THE COMMANDER:

OFFICIAL:

D. SCOTT MCKEAN
Lieutenant General, USA
DCG, Army Futures Command

JONATHAN PHILLIPS
IT Resources Chief, G6

History. This publication supersedes U.S. Army Training and Doctrine Command Pamphlet (TP) 525-3-5, *The U.S. Army Functional Concept for Maneuver Support (2020-2040)* published on 24 February 2017 as part of the Army concept framework for future forces. This publication provides extensive changes and has shifted from maneuver support as a proposed warfighting function to protection to align with operational demands and modernization requirements to achieve multi-domain operations capabilities within Army functions.

Summary. Army Futures Command (AFC) Pamphlet 71-20-7 describes in depth how future formations perform the protection warfighting function and the conceptual activities required during competition, armed conflict, and the return to competition against near-peer adversaries approaching operational and technical overmatch. This concept supports the operational objectives of compete, penetrate, dis-integrate, exploit and re-compete, and informs methods and means to approach sound modernization decisions associated with calibrating force posture, creating multi-domain formations and convergence of effects. This concept drives further conceptual work, research, experimentation, science and technology. It also guides doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy (DOTMLPF-P) change.

Applicability. This concept applies to all Department of the Army activities that develop DOTMLPF-P capabilities. This concept guides future force development and modernization while informing the Army capabilities integration and development system process. It further supports the Army capabilities development process and serves as a conceptual basis for developing additional supporting or advisory concepts to describe future force capabilities required to inform DOTMLPF-P in 2028 and beyond.

Proponent and supplementation authority. The proponent of this pamphlet is the Army Futures Command Headquarters, Director, Futures and Concepts Center (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. Submit comments and suggested improvements via DA Form 2028 to Director, FCC, Directorate of Concepts (FCFC-CE), 210 West 7th Street, Austin, TX 78701-2982.

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

Summary of Changes.

AFC Pamphlet 71-20-7
Army Futures Command Concept for Protection 2028

This revision:

- This publication supersedes TP 525-3-5, *The U.S. Army Functional Concept for Maneuver Support (2020-2040),* published on 24 February 2017.

- This concept revitalizes the Army protection warfighting function as dynamic, anticipatory, and proactive. The concept describes how the Army achieves all domain protection.

- It is informed by and contributes to experiments, studies, analysis, and continued development of the Army operating concept and the Army concept framework.

- It realigns with the Army function of protection and recognizes the continued operational demand for Army formations to perform related tasks and systems that preserve the force from threats in all domains, generating stand-off so commanders may apply maximum combat power to accomplish missions.

- It describes aspirational protection activities and requirements spanning multiple proponents and organizations to achieve required effects on the expanded battlefield when properly integrated and synchronized at echelon across the competition continuum.

Contents

Foreword ..... **iii**

Executive Summary ..... **v**

Chapter 1 Introduction **5**

1-1. Purpose 5
1-2. References 6
1-3. Explanation of abbreviations and terms 6
1-4. Assumptions 6
1-5. Linkages to other concepts 6
1-6. Protection warfighting function 7

Chapter 2 Operational Environment **9**

2-1. The OE and protection 9
2-2. The adversary challenge to protection 12
2-3. Protection challenges in MDO 14

Chapter 3 Military Problem and Components of the Solution for Protection **16**

3-1. Military problem 16
3-2. Central idea 16
3-3. Solution synopsis 16
3-4. Components of the solution 17
3-5. All domain protection at echelon 30
3-6. Army protection in MDO 34
3-7. Protection across the competition continuum 42
3-8. Supporting ideas 44

Chapter 4 Conclusion **46**

Appendix A References **47**

Section I Required References 47
Section II Related References 47

Appendix B Required Capabilities **49**

B-1. Introduction 49
B-2. Protection warfighting function required capabilities 49

Appendix C Science and Technology **54**

C-1. Introduction 54
C-2. Preserve CCAAs 55
C-3. Deny threat and enemy freedom of action 56
C-4. Enable access 58
C-5. Desired technical and scientific advancements to support required capabilities 58
C-6. Conclusion 83

Appendix D Dependencies **84**

D-1. Introduction 84

D-2. Protection dependencies on other warfighting functions and supporting activities..... 84

Appendix E Protection Across the Competition Continuum 89

E-1. Introduction 89
E-2. Competition 89
E-3. Armed conflict 91
E-4. Return to competition 92

Appendix F Protection Considerations of Unique Environment 93

F-1. Introduction 93
F-2. Dense urban terrain (DUT) 94
F-3. Jungle environments (FM 90-5) 96
F-4. Desert environments (FM 90-3) 97
F-5. Maritime environments 98
F-6. Mountainous and cold weather environments (ATP 3-90.97) 99
F-7. CBRN environments (JP 3-11) 101
F-8. Space and non-terrestrial environments 102

Glossary 102

Section I Abbreviations 102
Section II Terms 105

Figure List

Figure 1 Logic Chart……..……..……vii
Figure 1-1 Army Protection Doctrine and Policy…..…….8

Chapter 1
Introduction

1-1. Purpose

a. The U.S. Army Futures Command Pamphlet 71-20-7, *Army Futures Command Concept for Protection 2028* (AC-P) describes how the Army preserves the force from enemies in all contested domains, the electromagnetic spectrum (EMS), and the information environment (IE), so commanders can apply maximum combat power to accomplish the mission. This functional concept builds on the ideas presented in *U.S. Army Training and Doctrine Command Pamphlet* (TP) 525-3-1 *The U.S. Army in Multi-Domain Operations 2028* (MDO Concept) and TP 525-3-8, *The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045* (EAB Concept), which describe protection outcomes and requirements integrated across multiple proponents on an expanded battlefield and across the competition continuum as part of multi-domain operations (MDO). This concept contributes to experiments, studies, analysis, and continued development of the Army operating concept and the Army concept framework.

b. This concept poses and answers the following questions:

(1) What are the key physical and non-physical aspects of the future operational environment (OE) that influence how Army commanders execute protection?

(2) What are the protection gaps and seams that exist across all domains and the competition continuum?[1]

(3) What capabilities must the Army possess to preserve critical capabilities, assets, and activities (CCAAs); deny threat and enemy freedom of action; and enable access?

(4) What science and technologies must the Army pursue to enable the proposed conceptual solutions and supporting ideas?

(5) How will the Army employ these capabilities and technologies differently from existing protection doctrine to support MDO across the competition continuum?

c. The AC-P consists of four chapters and five supporting appendices.

(1) Chapter one establishes the purpose, underlying assumptions, linkage to the Army concept framework, and a vision of the protection warfighting function (WfF) in 2028. Chapter two provides the operational context that forms the basis for proposed solutions. Chapter three presents the military problem, central idea, components of the solution, and supporting ideas. Chapter four briefly summarizes the pamphlet's main ideas.

[1] Gap - an incomplete or deficient area or a problem caused by some disparity or areas; Seams – touch points between functions where a weak or vulnerable area or gap may exist or be created.

(2) Appendix B reflects required capabilities necessary to conduct operations described in this concept. Appendix C recommends key science and technology capabilities that support the central idea and the three components of the solution. Appendix D discusses contributions to competition, armed conflict and a return to competition. Appendix E discusses considerations of unique operational environments.

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

1-3. Explanation of abbreviations and terms
The glossary explains abbreviations and special terms used in the development of this pamphlet.

1-4. Assumptions
The assumptions from TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028,* and TP 525-3-8, *The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045*, apply to this concept.

1-5. Linkages to other concepts

a. *TP 525-3-1 The U.S. Army in Multi-Domain Operations 2028*. The AC-P recognizes the future OE as contested in all domains, increasingly lethal with an expanded battlefield, and views Russia as the pacing land power threat and China as the emerging pacing adversary. Specifically, the AC-P recognizes cumulative stand-off disrupts power projection from the homeland to decisive spaces, with sanctuary and friendly freedom of action disrupted in depth in all domains. The AC-P military problem poses the question of how to conduct all domain protection in a manner that enables the joint force to prevail in competition and achieve strategic objectives in both competition and armed conflict. The AC-P's central idea of preserving CCAAs, denying threat and enemy freedom of action, and enabling access assists the joint force in achieving convergence at echelon. Achieving multi domain convergence at echelon enables the joint force to compete, penetrate, dis-integrate, exploit, and re-compete on more favorable terms.

b. *TP 525-3-8 The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045*. The AC-P aligns with the same OE described in the EAB concept and assists EAB commanders by seeing and understanding, one key EAB action. The three components of the AC-P solution directly assist EAB formations in all six of the components of the solution outlined in the EAB concept. Deep sensing enables EAB formations to gain and maintain contact, persistently compete, and posture in all domains. The EAB concept supporting idea of establishing protected corridors links directly to enabling access, an AC-P component of the solution. Command posts critically require protection in all domains. These and other linkages enable the EAB commander to compete and when necessary, transition to armed conflict and prevail, consolidating gains to develop and retain enduring outcomes favorable to the U.S.

c. AFC Pam 71-20-1, *Army Future Command* C*oncept for Maneuver in Multi-Domain Operations, 2028*. The maneuver concept and AC-P share linkages in the operational context and OE. The components of the AC-P solution link directly in solving the military problem posed by the maneuver concept, assisting commanders in achieving positions of relative advantage in all

domains. The AC-P components of the solution are critical to the friendly force ability to posture, organize, and equip for decisive campaigns, enabling transition to armed conflict and a return to competition on more favorable terms.

1-6. Protection warfighting function

a. The AC-P describes a different approach to the protection WfF to overcome limitations of current protection efforts. Today, many observe and practice protection as a force protection activity based upon legacy counterinsurgency and base-defense thinking. Commanders often view protection as passive and stationary and fail to incorporate relevant protection information into a common operational picture (COP), or to integrate capabilities such as sensors and shooters. Gaps and seams exist across the many different protection tasks and elements (see Figure 1-1). Gaps and seams exist in air and missile defense (AMD) regarding capacity and capability to defeat rockets, artillery, mortars, unmanned aircraft systems (UAS), and hypersonic weapon systems. Other gaps result from separate or unlinked planning between force health protection (FHP), cyberspace operations, EMS management, and information related capabilities (including public affairs, Soldier leader engagement, deception, and operations security), which place the force in a defensive posture. Further exacerbating these gaps is the removal from or reduction in protection cells from echelons above brigade. Also, there is currently no unity of effort across protection-related activities.

b. Protection is not a program of record and it is not a list of tasks that a commander may perform. Army protection is an Army warfighting function employed by all Army branches, commanders, and staffs at every echelon from team to theater Army, and the homeland. Commanders must integrate it into every operations process and think of it in all domains, the EMS, and IE. Army protection is the enterprise of preserving CCAAs, denying threat and enemy freedom of action, and enabling access. Army protection enables the force to compete and win.

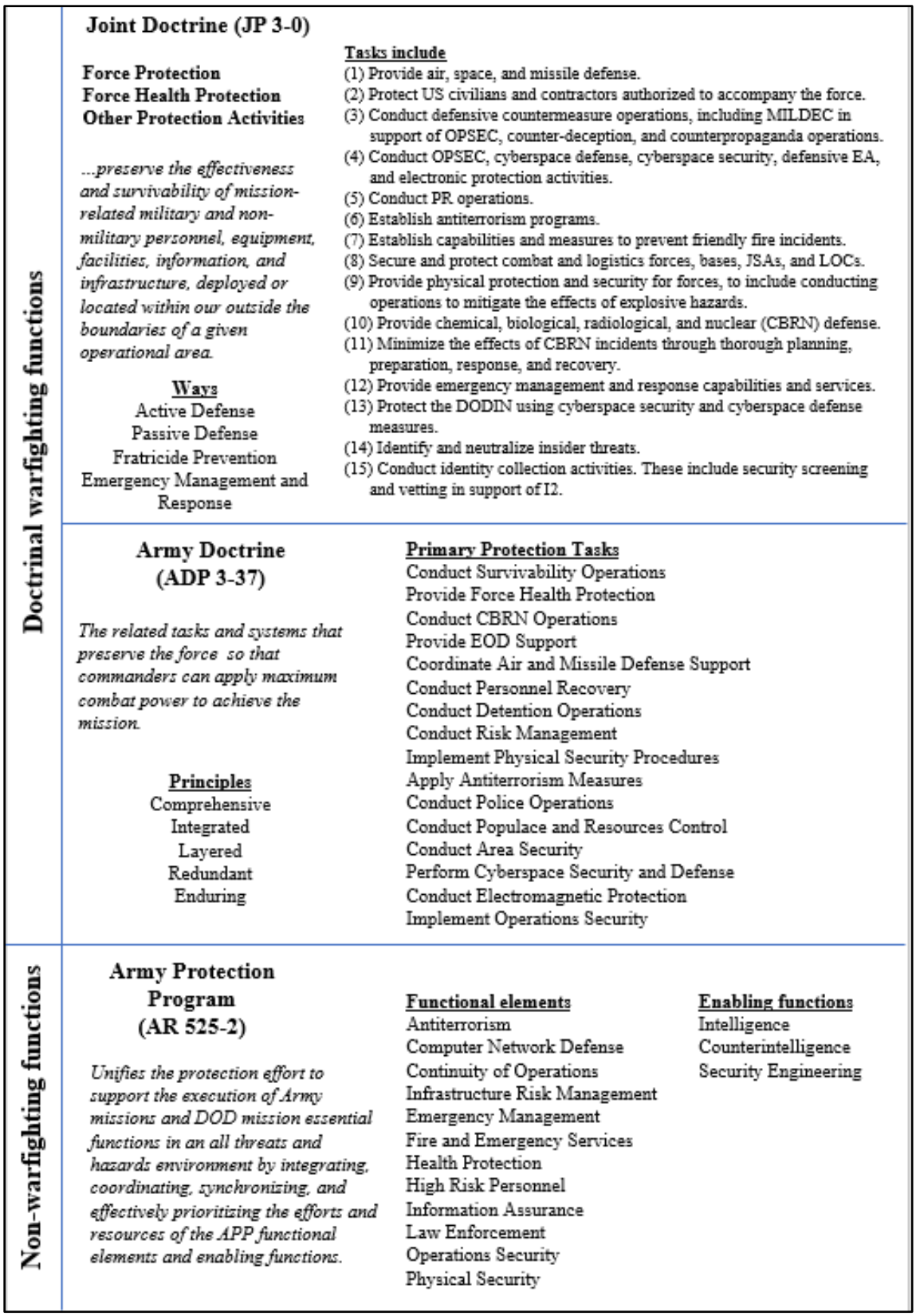


Figure 1-1. Army Protection Doctrine and Policy

Chapter 2
Operational Environment

2-1. The OE and protection

a. On the future battlefield the Army will face an enemy that contests international norms and seeks to achieve strategic objectives on its terms. The future OE presents unique and unprecedented challenges that the Army must be prepared to overcome during the continuum of competition, armed conflict, and the return to competition. Adversaries will create or leverage conditions intended to fracture partnerships, stress the will of friendly actors, and flip friendly force advantages in multiple areas to the side of the adversary. Peer and near-peer adversaries challenge future Army operations by using a combination of military and non-military capabilities in all domains, requiring a new protection construct and an expansion of protection capabilities to counter them effectively. How future Army forces protect against these challenges will determine if they survive and accomplish their missions.

(1) The future OE is extremely complex, on an expanded battlefield, with characteristics typified by dense urban terrain (DUT), growing and dynamic populations, traditional and newly critical information infrastructure, a changing climate, and with adversary propaganda, information operations, and military operations designed to achieve their objectives short of armed conflict.

(2) On the battlefield of the future, new enemy capabilities expand the decisive spaces beyond the traditional close combat area. Enemy capabilities have and will evolve to enable them to conduct operations within the homeland, against power projection capabilities, in the support areas and into the deep maneuver and fires areas of the battlefield.

(3) Technological advancements and improved capabilities in firepower, communications, and coordination of joint effects enable similarly sized formations to operate in vastly larger operating spaces.

(4) The future force will face peer and near-peer adversaries that are technologically advanced and capable of contesting in all domains, the EMS, and the IE. The future battlefield will be increasingly hyperactive and lethal, and it will be difficult to enter decisive spaces and to sustain operations due to formidable antiaccess/area denial (A2/AD) systems.

b. Future adversaries will leverage components of space, cyberspace, electromagnetic warfare and information to challenge friendly freedom of action. They will rely on an increasing number of “non-traditional” actors, including proxies and surrogates, who operate in the battlefield with anonymity to pursue their objectives. In this regard, collaboration between Army conventional forces and Army special operations forces will be critical to addressing problems posed by "non-traditional" actors.

(1) Many actors will have access to advanced technologies to contest and hold at risk U.S. forces in all domains, the EMS and the IE.

(2) Future adversaries invest in artificial intelligence (AI), quantum computing data processing, space systems, and robotic and autonomous systems (RAS) to compete with and eventually dominate U.S. capability.

(3) Future adversaries rely on all domain intelligence, surveillance, reconnaissance (ISR) from national and district levels to collect targeting information on headquarters, communications, critical infrastructure, and power projection facilities in the homeland.

(4) Adversaries incorporate advanced lethal kinetic, hypersonic, and directed energy weapons systems with greater range, velocity, and capacity.

(5) Adversaries plan to employ all domain nonlethal capabilities to reduce friendly force tempo, deny essential services, and understand and influence populations and officials, altering friendly decision making.

(6) Adversaries may employ or threaten the employment of advanced weapons of mass destruction (WMD) or weapons of mass effect (WME) to inflict grave infrastructural, psychological, and economic damage or death at any point along the competition continuum and across the battlefield to achieve physical, cognitive, virtual, or temporal objectives consistent with their strategic ends.

(7) Future threats, obstacles, and hazards increase the difficulty of friendly forces to survive and move across the battlefield. Enemies exploit commercial technologies such as additive manufacturing, biometrically enabled surveillance, identity intelligence, AI-enhanced autonomous control systems, satellite communications, computer processors, and sensors to create tailored weapons and advanced improvised explosive devices (IED), complicating the development of countermeasures.

c. The expansion of the future battlefield (domain, time-space, and geography) greatly increases and complicates the OE and protection WfF. Adversary activities during competition, particularly space and high-altitude operations, cyberspace and information activities, directly contribute to stand-off, challenging the ability of Army forces to immediately access all domains from strategic and operational distances. Much of this activity projects into the operational and strategic support areas, including the homeland, and future forces must effectively deny it to ensure the friendly freedom of action required for effective deterrence.

d. Adversaries will target mobilization, force generation, deployment, and sustainment capabilities, including public and private sector enablers as well as other domain capabilities (space and cyberspace). Adversaries will launch cyberattacks against critical infrastructure and information networks to destroy or degrade command and control (C2). The efforts of Army forces to provide necessary protection effects are increasingly complex due to changing political, cultural, and technological factors, and increasing private sector partners. The expansion and complication of the operational space has increased protection requirements with the escalation from competition to armed conflict as information, missile, and other attacks on the support areas, including the homeland, complement increasingly harmful virtual and cognitive attacks.

e. Other challenges driving MDO.

(1) Future adversaries create stand-off by expanding the battlefield in time, across all domains, and from the theater into the homeland during competition and armed conflict. Long-range lethal and nonlethal capabilities allow the enemy to control escalation on their terms during competition and to set the conditions for transition to armed conflict. The enemy will seek to overwhelm and destroy soft and unsuspecting targets, activities, and single points of operational failure. States characterized as weak and/or near failing are principal marks for the adversary to conduct offensive operations short of armed conflict.

(2) The future force will compete in all domains, the EMS, and the IE. The future Army will operate on a larger battlefield and rely on host nations, partners, and government agencies to achieve objectives. Near-peer states compete below armed conflict as a regular tactic to achieve objectives. Traditional nation-states will have difficulty imposing their will within a politically, culturally, technologically, and strategically complex environment. This environment limits friendly freedom of action, but also conceivably creates opportunities as enemy forces labor under the same constraints.

(3) The future force and partners will not be able to rely on secure areas for sanctuary to build readiness, combat power, sustain operations and rest, recover, or reconstitute. Bases, installations, camps, sustainment areas, assembly areas, lines of communications (LOC), and both movement and mobility corridors will be actively contested across the entire battlefield, and freedom of action will be disrupted.

(4) As adversaries seek to achieve their strategic objectives below the threshold of armed conflict, the U.S., through its strategic objectives, aims to expand the competitive space to allow policymakers to resolve differences, build capabilities and capacity in case of transition to armed conflict, and secure the environment. If the U.S. fails to meet its objectives to win without fighting, the cost to fully reverse an attempted *fait accompli* action will be immense. The objectives of MDO are to provide the ability to prevent a *fait accompli* action while avoiding full mobilization and a drawn-out war. Therefore, forces must be postured for success in competition. True winners and losers may not be obvious in limited armed conflict. All actors will strive to consolidate gains and produce sustainable outcomes for long-term deterrence and politically acceptable outcomes.

(5) The ability of Army units to deploy by air and sea from the strategic support area to the joint operating area (JOA) is critical to the prosecution of operations in theater. Protection of sea and air LOCs will take on greater emphasis due to the adversary's increased capabilities to attack them. The requirement for shortened deployment timelines drives the need for Army capabilities to be lighter and more deployable.

(6) Dense urban terrain (DUT) will create challenging conditions for all actors in future conflict. DUT presents distinct physical, cognitive, and operational characteristics and compounds the friction of war by increasing the number of tasks required within a given physical and temporal space. Any bypassed DUT can create continuous security issues for follow-on forces. The future adversary will use DUT to mitigate joint force strengths and create positions of advantage.

Adversaries will often seek to enhance their effectiveness and survivability by operating in these environments.

2-2. The adversary challenge to protection

Russia is the pacing threat presenting the most significant challenge to the U.S. Army through 2028. China, through aggressive investment and proliferation of technology, will overmatch friendly forces in many areas and will be the greatest threat to the U.S. Army (and other parts of the Joint Force) in 2035 and beyond. Russia and China may employ similar approaches, including using different techniques and capabilities, to challenge U.S. forces and partners in competition and in armed conflict. Although the focus of this concept and the U.S. Army operating concept is on Russia and China, other global threats seek to create political and military stand-off to destabilize regional security. Those threats will employ the same techniques and proliferate the same advanced technology at a reduced scale. This concept addresses those additional challenges.

a. Adversary stand-off to win in competition without fighting. Russia, China, and other actors are currently in continuous competition with the U.S. and its partners around the world. Russia and China strive to meet their strategic objectives by fracturing and separating U.S. alliances and partnerships, and achieving resolutions below armed conflict through diplomatic and economic actions, irregular warfare (IW), information warfare, cyberspace warfare, exploitation of social, ethnic, or nationalistic tensions and the threat of conventional forces. By employing stand-off and separation techniques, adversaries can reduce the friendly force's ability to identify hostile intent, make decisions, and react.

(1) Russia and China employ national and district level ISR during competition to understand friendly force posture and likely actions. As they prepare the OE and set conditions for achieving objectives short of armed conflict or in conflict, they conduct surveillance of adjoining states, allies, and the U.S. homeland. They conduct ISR through space-based and special purpose forces (SPF) capabilities, sympathizers, open-source collection, ground-based intercepts, and sensors. ISR enables enemy long-range strikes, future conventional force operations to include *fait accompli*, and confirmation they have achieved objectives to continue or terminate operations.

(2) Russia and China destabilize governments in their region through unconventional and whole-of-government means. They attempt to coerce friendly and neutral actors to shift their allegiances, further fracturing cohesion. Russia and China empower and encourage proxies, surrogates, and activists to conduct terrorism, subversion, non-attributable attacks from the physical and cognitive sanctuary, criminal and unconventional activity, kidnapping, and direct action strikes on their behalf. They conduct information warfare, interfere with social media, inject false narratives, and conduct offensive cyberspace and electromagnetic warfare (EW) to create ambiguity in understanding, political recognition, decision, and reaction. They employ offensive cyberspace, EW, and counter-space capabilities to degrade and deny friendly communications, positioning, navigation, and timing (PNT) and ISR. Russia and China continue to pursue kinetic and non-kinetic weapons systems capable of denying, degrading, disrupting, and destroying satellites in orbit, placing U.S. and allied nation satellites at greater risk.

(3) The conventional threat through long-range fires, counter-space, and combined arms ground forces, in conjunction with ISR, irregular, unconventional, and information warfare,

enables Russia and China to strike with very little warning. The adversary's ability to combine all domain effects and overwhelm an opponent is the most challenging hurdle facing friendly forces. Russia and China may escalate conventional action and stand down at the last minute to stimulate friendly force reaction.

b. Russia and China seek to achieve physical stand-off by employing layers of A2/AD systems designed to rapidly inflict unacceptable losses and delay on U.S., allied, and partner military forces, giving the enemy the opportunity to achieve campaign objectives before any formidable response.

(1) Enemy understanding in depth and reinforcing stand-off in conflict. Russia and China employ advanced all domain capabilities to clearly understand the OE, friendly force intentions, and the current situation in the support areas to their deep fires area. They rely on national and district level ISR to collect targeting information on fixed sites (headquarters, communications, critical infrastructure, and power projection facilities); detect predictable patterns of operations; and monitor changes to friendly force posture. The enemy targets CCAAs that friendly forces intend to converge at some point in the operation. The adversary denies friendly forces key terrain. Russia and China understand that the bulk of forces, equipment, and combat power travels from U.S. installations, through intermediate bases and ports of debarkation (air/sea), then travels along maneuver corridors to positions of advantage and decisive spaces. They aggressively disrupt friendly force projection during armed conflict.

(2) Coordinated long-range fires, air and missile defenses, and reconnaissance capabilities are the center of gravity for conventional capabilities to execute stand-off operations in conflict. Long-range fires include land, sea, and air-launched ballistic missiles; land and sea-based long-range surface-to-air missiles; and long-range multiple rocket launchers. Russia and China are able to contest critical C2 and sustainment assets in the support areas. The enemy uses long-range strike capabilities against civilian infrastructure and resources that support military operations, such as transportation networks, energy generation and distribution systems, and the defense industrial base. The enemy employs various types and quantities of obstacles in ground and sea movement corridors to challenge friendly force freedom of movement and reduce tempo of operations.

(3) Nation-states and/or non-state actors may conduct IW as an element of competition between adversaries, as a component of international armed conflict, as an application of contingency response, or as a distinct armed conflict. Weaker adversaries may utilize IW approaches to disrupt or neutralize the security provided by the military and other security forces of an established political authority. Stronger adversaries may utilize IW approaches indirectly through proxies to achieve their strategic objectives while avoiding escalation to direct conflict.

(4) Russia and China employ advanced technologies, procedures, and techniques to achieve strategic objectives quickly and decisively. They employ electromagnetic warfare, counter-space, and offensive cyberspace operations to jam, spoof, exploit, or destroy friendly space-based ISR, communications platforms, C2 networks, and PNT capabilities. The enemy uses information warfare to target friendly leaders, populations, and forces to influence outcomes. Both Russia and China have invested heavily in robotics, autonomy, artificial intelligence, and UAS swarming and

teaming techniques in order to increase capability and expand capacity to gain a significant competitive advantage over friendly forces. They also employ advanced energy and hypersonic weapon systems that are smaller, faster, and cheaper with expanded range, able to shoot multiple shots and are highly mobile. Nuclear, cyber, and other WME threaten the U.S. homeland, allies, partners, and friendly military forces. The adversary employs WMD or WME to accomplish strategic objectives or reverse friendly force consolidated gains.

2-3. Protection challenges in MDO

a. Defeating stand-off will be a significant problem for friendly forces. The adversary will attempt to separate joint forces and achieve strategic and operational objectives in multiple ways, including conventional and advanced A2/AD systems, irregular and information warfare, and actions in competition short of armed conflict using various actors.

b. Securing and protecting bases and infrastructure will be essential to the future force's ability to compete and win. The use of bases for intermediate staging, sustainment, and related activities will be required to conduct large-scale combat operations (LSCO). The future force must be able to establish bases and enable access for onward movement and sustainment of forces. Bases, due to their size and immobility, will be difficult to conceal and will be generally considered high value targets for enemy attacks due to the concentration of friendly forces and materiel. Bases will be highly contested and difficult to sustain forward on the battlefield.

c. All activities forward on the battlefield, including LOCs, critical infrastructure, and temporary holding areas, must be resilient and mobile. Forces operating in these areas must be able to conduct counterintelligence activities and develop strategic resiliency, able to reconstitute, rebuild, and able to project friendly power more effectively than the adversary can destroy it.

d. U.S. forces will expand the competitive space below the threshold of armed conflict in order to deter the adversary and prevent escalation while continuously preparing to transition.[2] If conditions deteriorate, forces can transition rapidly to armed conflict to quickly achieve objectives. The joint force must present a compelling deterrence force to remain in competition with the adversary, and if conflict is inevitable, the future force can expand competition in its favor to control threat aggression. The ability to protect our forces contributes to the credibility of our deterrence.

e. U.S. forces rely on projecting power from the homeland to expand the competitive space and quickly transition to set conditions for a favorable outcome. The future force projects power to build combat capability and sustains operations to meet strategic objectives. Protecting power projection capabilities will be a challenge, and without this capability, the force will struggle to

[2] The idea of expanding the competitive space is advocated in the 2018 National Defense Strategy and the MDO concept. Multi-domain operations require strategic and operational commands to effectively expand the competitive space through daily support to U.S. interagency partners, as well as allied and partner governments. Expanding the competitive space consists of applying Army capabilities or posturing forces in coordination with these partners in such a way as to achieve effects that maintain or obtain U.S. policy objectives while deterring escalation to armed conflict. These actions can encompass all elements of decisive action and include all elements of combat power. For example, actions might include active cyberspace and information operations to counter adversary information warfare, an exercise with a multinational partner to show U.S. commitment, or even posturing forces in strategic positions of advantage that are capable of defeating enemy forces in a quick, decisive fashion to force a return to competition on favorable terms. The primary goal of U.S. policy and MDO is to "win" in competition while avoiding armed conflict.

deter an enemy *fait accompli* action or present a formidable deterrent to the adversary. The adversary compounds this with unprecedented ability to see and act deep into the strategic support area, degrading and denying friendly force projection. Near-peer adversaries may achieve this by recruiting and employing foreign and domestic extremists who employ terrorist tactics in attempts to strike the homeland. Proliferation of WMD and related technologies will continue. Russia and China already possess WMD, while other actors are trying to obtain them. Efforts to develop or acquire WMD, their delivery systems or their underlying technologies, particularly by rogue states or non-nation state actors, constitute a major threat to homeland security.

f. Future Army forces rely on the support areas to converge multi-domain capabilities and shape the conditions for decisive operations. The joint force secures the area and reinforces support by converging capabilities across all joint, interagency, intergovernmental, and multinational (JIIM) partners. Support areas are the enemy's deep fight.

g. Protective measures must be able to detect and thwart new enemy capabilities and protect against enemy first strike capabilities. America has experienced devastating surprise attacks in modern times. The attack on Pearl Harbor by Imperial Japanese forces in 1941 and the 11 September 2001 terror attacks illustrate how enemies utilize surprise to gain immediate tactical, operational, strategic, and informational advantages. Future enemies are likely to utilize surprise attacks in the initial days of conflict to gain immediate advantages. Enemy SPF are likely to target CCAAs in the strategic support areas. SPF may immediately precede kinetic attacks with massive denial of service attacks on military and civilian communications through jamming, blocking, or spoofing communications using satellite or undersea cable systems. CCAAs require improved survivability, recoverability, and redundancy so forces can maintain functionality and preserve combat power after a surprise attack.

h. Future Army forces must have protection against chemical, biological, radiological, and nuclear (CBRN) threats. CBRN weapons will be available to threat forces in regions where U.S. forces may deploy. The adversary may accomplish delivery of CBRN weapons by several means globally and across the expanded battlefield, causing extensive injury and contamination. The consequences of these emerging threats by dangerous actors are significant, given WMD proliferation around the globe. Adversaries could use harmful chemicals such as chemical weapons, toxic industrial and commercial chemicals, and chemical toxins of biological origin such as ricin. Nuclear and biological weapons pose the most strategically significant risk due to their devastating effects. Nuclear and radiological threat weapons vary in size, composition, lethality, and range. Army forces must also protect against infectious disease outbreaks regardless of source, and against bioweapons and bioterrorism threats; typically monitored and managed by employment of the military health protection condition (HPCON) system.

i. Biological threats are infectious diseases that have the potential to spread and cause an outbreak or pandemic. Key elements to defeating CBRN threats are preparedness, detection, protection, and mitigation. Negating the effects of CBRN hazards will be critical to mitigating their degradation of combat power. This includes encapsulating, removing, or neutralizing residual contamination from personnel and equipment to prevent further exposure, along with administering emergency medications and treatments and decontamination of facilities, buildings, and infrastructure.

Chapter 3
Military Problem and Components of the Solution for Protection

3-1. Military problem
How do Army forces, as elements of the joint force, achieve all domain protection on the expanded battlefield to preserve combat power, power projection, freedom of action in depth, and access to decisive spaces to create protected windows of superiority while achieving U.S. strategic objectives and deterring adversaries in competition, or when necessary, enabling the rapid transition and ability to prevail in armed conflict, and a return to competition on favorable terms?

3-2. Central idea
Army forces, as part of JIIM teams, conduct protection activities in all domains, the EMS and IE, to preserve commanders' CCAAs, deny threat and enemy freedom of action, and enable access to achieve protected windows of superiority.

3-3. Solution synopsis

a. The character of future threats, the OE and protection challenges, along with how commanders conduct MDO to win, has challenged concept developers to explore a broader menu of activities to achieve MDO objectives. Learning derived from MDO experimentation indicates that preserving CCAAs and countering threats are absolutely required to enable access to positions of advantage and decisive space across the expanded battlefield and competition continuum, to exploit conditions and win.

b. Critical to solving the major challenges described in the previous chapter is avoiding a *fait accompli* whereby the enemy is able to disrupt U.S. and partner forces' activities to a level that prevents the coalition force's ability to project decisive power at the right time and place to achieve a position of advantage. Friendly forces accomplish this by deploying and employing a strategically credible and ready force, with sufficient capabilities and rapidly enough, to impact the enemy's decision cycle or counter his actions once begun. This response requires achieving protected windows of superiority to execute the necessary deployment activities.

c. The protection warfighting function manifests itself differently at echelon, in depth through competition, armed conflict, and the return to competition. The future force must be able to overcome the enemy's ability to overwhelm with combined all domain effects through protection outcomes, denying activities, and enabling access. The main ideas within the protection function relate to proactively employing more active defense measures across these solutions. MDO challenges require the future force to proactively deny and defend against enemy action leading to the three components of the solution: *preserve CCAAs, deny threat and enemy freedom of action, and enable access*.

d. The Army teams with the joint force, government agencies, and the private sector to develop, protect, operate, exercise, and restore resilient homeland capabilities for the projection of military

effects from, into, and across all domains at strategic distances despite adversary multi-domain A2/AD capabilities.

e. Army forces conduct defense support of civil authorities (DSCA) tasks in support of homeland operations when the size and scope of events exceed the capabilities or capacities of domestic civilian agencies.

3-4. Components of the solution

a. Preserve CCAAs. Preserving CCAAs is the foundation for resilient and survivable individuals, formations, and operations across the battlefield and the competition continuum. Preserving CCAAs is necessary for the future force to survive and win in large-scale combat in MDO. CCAAs may be the individual Soldier, mission and objective related readiness, force projection, combat power and formations, access to decisive spaces, decisive points, connections, sustainment assets, facilities, LOCs, main supply routes, information, understanding, and infrastructure (not all inclusive).

(1) Planning and prioritizing protection.

(a) Understanding CCAAs. Commanders at all echelons must understand which CCAAs are most essential to the success of their mission such that if degraded, destroyed, neutralized, or disrupted by enemy effects in all domains, the EMS, and the IE, this would cause mission failure or unacceptable risk. Intelligence estimates are crucial to understanding how threats in all domains could affect CCAAs. When commanders or staffs deem deliberate employment of protection capabilities in all domains, the EMS and IE insufficient, a collection, sensor or indicator and warning plan must be established and further converged with forces, functions or autonomous systems charged to preserve the CCAAs. Staffs can use a protection prioritization list across all echelons to identify and track CCAAs they must preserve.

(b) Informed risk. A commander choosing to employ protection capabilities must identify and accept informed risk decisions. For instance, the MDTF has a particular location of forces, systems, patterns, and linkages to the joint force to achieve convergence. However, the MDTF may not have sufficient mobility, survivability, or protection in all domains during the course of a campaign. These shortfalls become dependencies upon the higher and adjacent organizations that commanders and staffs must dynamically understand, integrate, and synchronize to assure the preservation of MDTF mission effectiveness. One method any formation could use is the creation of a protection prioritization list. While the creation of the protection prioritization list is in current protection doctrine, commanders and staffs must examine the available people, processes, and systems to enable the protection WfF through the lens of "what must be protected," from what, how to see them, warn, preserve from, deny, and measure the effects for dynamic assessment.

(c) Process to determine protection priorities. Commanders and their staffs must deliberately assess what CCAAs must be protected, and from what threats, obstacles, or hazards in MDO during both competition and armed conflict, depending on the commander's objectives. For maximal efficiency and effectiveness, future Army forces utilizing the C2 Joint Operating Ecosystem (JOES) and working with the future tiered decision-making model must develop protection

decision support tools (such as, AI-enabled) to assist with determining protection prioritization, when, where, and from what threat. A multi-domain common operational picture (MDCOP) will help commanders and staffs achieve the desired understanding. The commander or staffs must also sense or collect against the threat, obstacle, or hazard; select single or combined protection capabilities to neutralize or mitigate the threat, obstacle, or hazard; along with additional recommendations for denial activities and protective countermeasures, or to preclude the threat.

(d) Commanders develop understanding of CCAA protection through detailed analysis of threat capabilities and friendly force vulnerabilities. Commanders rely on the ability of the force to stimulate, detect, see, and understand threats, obstacles, and hazards across the battlefield. The realization of this process is the integration, synchronization, and implementation of layered, all domain protection and defenses that enhance a commander's ability to apply maximum combat power to accomplish assigned missions while making appropriate risk decisions.

(e) The Army conducts counterintelligence to preserve CCAAs and reduce the threat's ability to recognize friendly disposition and intentions. Counterintelligence teams detect, identify, and characterize the adversary, resident populations, and institutions to better understand the threat. Counterintelligence teams, with cyberspace, electromagnetic warfare, special operations forces, MP, security forces, CA, security force assistance, and host nation support, develop situational understanding of the operating environment. Counterintelligence assets are instrumental in protecting bases, sustainment nodes, and operating areas from infiltration, collection, and targeting by foreign intelligence, security services, criminals, surrogates, insurgents, and international terrorist organizations throughout the competition continuum. The counterintelligence capability is critical to future operations; commanders and staffs take employment considerations balancing risk of losing assets against the reward of the intelligence gained.

(f) Inherent in the concept of preserving CCAAs is the determination of what constitutes essential versus non-essential forces. The Army may desire to remove non-essential elements of the future force beyond the range of threat fires capability. The future Army must modernize non-essential friendly capabilities to enable them to perform their missions remotely, either through tele-operation or other automated or semi-automated means. Removing non-essential forces beyond long-range precision fires attack ranges would greatly reduce the risk to those units while reducing or eliminating the protection prioritization dilemmas commanders would otherwise face. Commanders must take into account the second and third order impacts of separating non-essential forces.

(2) Operations in the homeland. Homeland operations are Army operations in support of homeland defense, DSCA, homeland security, and enabling power projection. Army forces, in conjunction with the joint force and interagency partners, deter and defeat attacks against the U.S. homeland, mitigate the consequences of attacks or disasters and enable Army effect projection from the homeland across all domains throughout the competition continuum. Homeland operations incorporate all planning and execution designed to detect, deter, preempt, respond to, mitigate, and recover from the full spectrum of incidents and threats to the homeland, whether man-made or natural. It includes an understanding of authorities, policies, and informational impacts, as well as political and cultural influences that contribute to the complex OE in the homeland.

(a) The mission to deter and defeat attacks relies on the concept of an active layered defense in the forward regions, the approaches, and the homeland. This includes identifying and providing for the mutual effects of homeland events and expeditionary operations, consideration of cyberspace operations, space operations, and Army participation in JIIM efforts that protect our nation from attack. It is a concerted whole of government approach to identify threats and hazards, mitigate vulnerabilities, and understand risk. The Army works with local, state, and federal governments (to include Federal Bureau of Investigation and U.S. Department of Homeland Security) and private sector partners to develop, protect, operate, exercise, and restore resilient homeland capabilities for the projection of military effects from, into, and across all domains despite enemy multi-domain stand-off measures.

(b) Resilient and capable installations are essential to maintaining the ability to project power and require an agile adaptive C2 system to plan, prepare, execute, monitor, and assess successful fort-to-port operations. It is imperative that the Army remain aware of DSCA operation requirements that may have an impact on resource and force allocation and mission assurance. Potential ongoing DSCA operations consist of domestic disaster relief, pandemic response, counter-WMD (CWMD) and CBRN response, defense support to civilian law enforcement agencies (e.g., border security) and terrorist protection and response.

(c) Homeland defense. Army forces, in conjunction with the joint force and interagency partners, protect the U.S. homeland, territories and sovereignty against internal and external adversaries, aggression, and other hostile actions. The future force conducts homeland defense operations across all domains, the EMS and the IE to deter and defeat attacks. This in-depth defense strategy allows the DOD to engage enemies as far from U.S. shores as possible, while defeating attacks as they approach the homeland. Force posture, readiness, force protection, and antiterrorism activities are defensive signs and measures to reduce vulnerability from attacks. Force protection and antiterrorism integrate into all Army operations, and awareness pervades every mission. Army forces provide technical information, police operations, survivability, mobility, and CWMD information to protect and defend camps, posts, stations, and the homeland. Installations in the U.S. homeland and around the world must be resilient against disruption and attack, with robust capabilities to prevent, protect, respond, mitigate, and recover from all threats and hazards affecting mission readiness, sustainment, and force projection.

(d) DSCA. Army forces, as part of the joint force, help mitigate attacks and disasters within the homeland through DSCA operations. Operations include CBRN consequence management, rescue engineering, crisis response, domestic disaster relief, defense support of civilian law enforcement agencies, and other designated support. Consequence management includes the plans, policies, procedures, training, and equipment needed to mitigate loss of life and property and to assist with response and short-term recovery after a CBRN event. Rescue engineering capability provides technical support and advice to task force leaders and commanders to assess damage, mitigate physical and health hazards, enable safe entry, and ensure movement through a disaster site to assist rescue and lifesaving operations. The U.S. Army deploys specially trained and equipped structural engineers and teams to augment federal urban search and rescue forces, incident support teams, military technical rescue organizations, and general-purpose troops during urban operations, structural collapse incidents, and other disasters. The forces required vary

depending on the type of DSCA response, and a large DSCA event or multiple events can consume time and equipment and potentially limit additional military force response.

(e) Protect power projection. Essential to assuring Army forces can respond with strategically significant credibility beyond prepositioned formations and capabilities is the survivability of CCAAs that enable rapid joint power projection. Enemies will likely attempt to disrupt U.S. joint power projection to be successful. The enemy will attack the strategic support area to disrupt and degrade deployments and reinforcements attempting to gain access to the operational support area using strategic lethal and nonlethal weapons, as well as special operations reconnaissance and strikes. This disruption spans from the U.S. homeland across strategic, operational, and tactical support areas to contested spaces. Identifying critical power projection systems, nodes, and modes, including mission essential functions and their vulnerabilities, is paramount.

- U.S. forces must know how enemies identify and degrade power projection capabilities through all domains, and then execute layered and redundant preservation measures, including dynamic aggregation and disaggregation, coupled with active defensive and denial measures. Commanders enhance these defensive measures by conditions-based authorities fused with JIIM capabilities to retain freedom of action that assures relevant and credible maneuver across strategic and operational distances.

- To achieve this, Army forces, including power projection activities, must be able to understand all domain threats and avoid, disarm, render safe, or survive and recover quickly from threat effects. Forces must ultimately influence protective counteractions to expand preservation of projection effectiveness to defeat enemy stand-off and enable the friendly ability to penetrate. Army forces must have the ability to process and manage large amounts of sustainment and movement data integrated with information and battle management systems to anticipate requirements, aid decision making, and maintain situational awareness of power projection operations.

(f) AMD. Army AMD units provide deterrence and preserve CCAAs in the strategic support area to enable freedom of action in the U.S. homeland and rapid power projection to globally penetrate enemy A2/AD. The U.S. homeland, aspects of the strategic support area, and other support areas must be able to survive against a determined enemy seeking to disrupt or destroy the future force's ability to project power rapidly to penetrate A2/AD. Future Army forces must provide defensive fires to defend the strategic support area, strategic lines of communications and other support areas against all aerial attacks through future capabilities that can detect, track, and warn those affected of an imminent attack; engage and destroy incoming targets, protect from impact and blast; and mitigate any hazards that may occur. Future forces must leverage JIIM capabilities when possible to increase capacity to actively and passively defend facilities, air and seaports, Army pre-positioned stock (APS), and critical infrastructure. Any future capability must be able to engage in competition, deter the enemy by preventing vulnerabilities in friendly targets of opportunity, or achieve quick strategic wins short of full-scale armed conflict following an attack on the homeland.

(3) Assuring convergence capabilities. Convergence enables the future Army to compete against near-peer threats by combining capabilities to create overmatch or gain an advantage.

Convergence allows the force to break enemy formations physically, virtually, and cognitively. Therefore, converging multi-domain capabilities will be necessary for MDO. As part of joint teaming, the Army will field systems-of-systems capabilities operated by new or enhanced organizations. This new technology will become a high value target to the enemy and will be vulnerable to detection, degradation, and destruction. Converging capabilities require mobility, survivability, and all domain protection to assure operational application and availability at the point of need.

(4) All domain control measures. The future force must establish all domain control measures to reduce unnecessary overlaps; assure authorities and custody of effects; and prevent friendly disruption, fires, or degradation in unity of effort. Control measures can be conditions-based to prevent limitations and restrictions to employing advanced all domain capabilities as tensions escalate. All domain control measures include authorities, permissions, and restrictions to defend the network in cyberspace; sharing common understanding to support tactical and operational maneuver; converging all domain capabilities to preserve CCAAs; and coordinating between echelons to enable a layered defense across the area of operations. These should also be viewable in the MDCOP.

(5) Balance dispersion and unpredictability. The increased range in combination with the enemy's ability to synchronize ISR with lethal and nonlethal effects requires that U.S. forces integrate and synchronize mobility, all domain protection, operational security (OPSEC), survivability, and terrain management. There are times when massing forces achieves desired protection at points of force aggregation; at other times, disaggregating forces combined with movement control in temporary windows of superiority provides protective value through dispersion. Through deception, the future Army creates unpredictability, expanding the competitive space for policymakers. Army forces must know when they are vulnerable and understand when they have the advantage.

(6) Security operations. Security operations mitigate enemy penetration and exploitation of seams and gaps within friendly forces. A huge challenge with MDO is securing and preserving CCAAs in the support area to enable decisive action in decisive spaces. Many organizations are capable of performing security operations, such as MP, special operations, and maneuver forces, and their actions can be coordinated with joint and host nation partners. Security operations include screen, guard, cover, area security, and local security. In MDO, security spans into all domains, the EMS, and IE and incorporates the virtual and cognitive dimensions. The future Army performs security operations that provide early and accurate warning of enemy actions, preserve CCAAs with time and maneuver space within which to react to the enemy, and allow commanders to effectively develop the situation and apply the right measures to defeat hostile actions.

(7) Inherent protection. Future Army forces at all echelons employ organic capabilities and effects to protect Soldiers and equipment from enemy threats. These capabilities include camouflaging individuals and equipment to prevent detection; the wearing of body armor, personal protective equipment (PPE), and mission oriented protective posture gear; and the utilization of design-built and add-on vehicle armor. In addition to passive armor and protective equipment, future Army forces will increasingly deploy advanced devices and systems to provide active protection against enemy air and missile capabilities. These systems include active protection

systems against anti-tank missiles, short-range rockets, mortars, and air threats such as UAS and manned aircraft. To maximize effectiveness, friendly forces integrate active protection systems with threat sensing capability. Other inherent protection capabilities will include advanced technology to detect all domain threats, provide 360-degree hemispheric protection, communicate over the JOES meshed C2 network, provide visual and auditory warning, train and equip formations to defeat basic level threats, and deter against intermediate level threats and provide health monitoring. Commanders must weigh the organic capabilities of units and formations when deciding when and how to assign higher echelon protection capabilities.

(8) The Army protection program (APP). The APP complements and reinforces the protection warfighting function during competition as it becomes more likely that enemies will affect future operations in the strategic support area under MDO. As the Army manages risks in day-to-day operations, it will overcome adversary challenges and shape operations for the warfighter. The nexus of both the warfighting function and APP will drive complementary and reinforcing activities to preserve CCAAs across force generation and projection platforms, the battlefield, and during competition and armed conflict.

b. Deny threat and enemy freedom of action. Passive measures are insufficient to preserve CCAAs and prevent threats in all domains, the EMS and the IE, including obstacles and hazards, from degrading mission accomplishment. This will result in larger applications of combat power at sub-optimal times and places. The protection WfF serves a role in targeting, all domain C2, and the operations process. Active protection processes should characterize the threat and nominate protective denial or defensive measures to expand the preservation of CCAAs throughout all domains, the EMS and the IE. Denying enemy freedom of action is the active approach to denying the enemy's ability to see, understand, and strike friendly force CCAAs. Coordinating all domain defense with fires, maneuver, and C2 creates the opportunity to deny enemy A2/AD and preserve CCAAs. Actively denying enemy freedom of action consists of a menu of protective measures that limit enemy access to positions of advantage.

(1) Deny WMD and WME.

(a) Future enemies may employ or threaten the employment of weapons that inflict grave destruction and psychological and economic damage upon the military, governments, populations, economies, and national infrastructure of sufficient magnitude to alter the balance of competition or armed conflict. WMD include CBRN weapons. WME encompasses WMD and other non- or less-destructive means capable of inflicting grave large-scale effects such as cyberspace-delivered viruses, malware, zero-day exploits, or other cyberspace effects; electromagnetic pulses (EMPs); jamming; or other capabilities that compromise communications utilizing the EMS. It also includes improvised destruction of infrastructure or facilities that can cause large-scale secondary hazards (WME sites).

(b) Future forces must have the capability to deny the full range of WMD threats at echelon across the competition continuum in MDO and must understand the nature of these weapons including origins, delivery means, and their effects, and be capable of preventing, mitigating, and recovering from their use. An enemy's deliberate damage or destruction of WMD/WME sites or even threatening to do so may require friendly forces to alter routes or take mitigation measures.

Additionally, risks from friendly operations may compel future Army forces to establish a no-fire area to avoid friendly-fire damage or destruction of WMD and WME sites. Army protection capabilities supporting countermobility operations may include coordination for early insertion of SOF, augmented with explosive ordnance disposal (EOD) and specially trained CBRN subject matter experts, to gain control and prevent enemy sabotage of WMD and WME sites.

(2) Deny irregular warfare. The threat employs and integrates irregular warfare and conventional capabilities that present unique challenges to friendly forces, work to fracture alliances, and reduce effectiveness. The adversary conducts irregular warfare in their deep area striving to disrupt activities in the friendly force support area. Army forces identify and deny threat irregular warfare through security cooperation that influences and improves relationships with local communities and builds partner capabilities and capacities. Friendly forces conduct irregular warfare with JIIM partners to deny the threat and preserve supporting operations across the entire MDO framework. U.S. forces work with and through neutral and friendly actors to enable the force to set conditions for indirect interaction with threat irregular activities. Denying enemy irregular warfare conducted in friendly support areas requires coordination with special operations forces, and direct engagement to preserve CCAAs using MP, maneuver, and other security elements including those of JIIM partners.

(3) Countermobility operations. Enemies will seek to create advantageous conditions by conducting operations in complex terrain and other populated areas to diminish the potential employment of friendly countermobility capabilities as a way of offsetting friendly advantages. To counter, Army forces must use the effects of natural and manmade obstacles in the land domain to deny enemy forces freedom of movement and maneuver. Future countermobility systems will employ a scalable range of effects allowing combined arms forces to shape where and when enemy movement and maneuver occur, and prevent the enemy from gaining a position of advantage. Engineer forces employ obstacles to achieve the desired effect in support of maneuver forces by providing countermobility capabilities to shape the terrain to slow or divert the enemy, to increase time for target acquisition, and to increase weapon effectiveness. In competition, forces use barriers, obstacles, and minefields as flexible deterrent options without posing an offensive threat, while defensive employment along a hostile land border can demonstrate friendly resolve. Defensive barrier, obstacle, and minefield employment can help protect friendly ports, LOCs, and key facilities, and free combat forces for other operations.

(4) Deny land, sea, and air based fires.

(a) Denying air and missile threats is primarily achieved through AMD, which is direct (active and passive) defensive action taken to destroy, nullify, or reduce the effectiveness of hostile aerodynamic, cruise and ballistic missile threats against friendly forces and assets. Enemy air and missile threats continue to grow in quantity and capability. Air threats denied by AMD systems include aircraft (manned, and all classes of UAS), aerodynamic and hypersonic missiles. Manned aircraft include bombers, fighters, ISR, EW, transport, helicopters, commercial aircraft, and refuelers. Small and non-transmitting UASs present a unique challenge to AMD, as they are difficult to detect. Aerodynamic missiles include air-breathing missiles like cruise missiles, air-to-surface missiles, air-to-air missiles, and surface-to-air missiles. A ballistic missile is any missile

that does not rely upon aerodynamic surfaces to produce lift and follows a ballistic trajectory when terminating thrust.

(b) U.S. enemies have frequently and successfully deployed rockets, artillery, and mortars against air bases, forward operating locations, forward operating bases, and critical infrastructure. Enemy future fires effects are likely to incorporate multi-echelon and multi-domain capabilities to target friendly forces in the close, operational, and strategic support areas. Army direct and indirect fires protection capabilities must support lower echelons of employment in order to deny the growing quantity of air, missile, and fires threats on the future battlefield. Future Army forces require unique counter-fire capabilities to operate in distinct terrains to deal with the special battlefield geometry these environments present.

(c) Future Army forces require the capability to preserve CCAAs against directed energy weapons (DEW) to include laser, microwave, sound, and particle beam lethal and nonlethal threat systems across the battlefield and competition continuum. The enemy and/or adversary may use DEW discreetly; radiation above and below the visible spectrum is invisible to the naked eye and does not generate audible sound. Because lasers can maintain energy for great distances, they are suitable for use in space warfare. Large high-power DEWs may offer enemies unique targeting opportunities to neutralize friendly systems. Potential effects of nonlethal DEW threat systems on personnel include difficulty breathing, disorientation, nausea, pain, and vertigo. Adversaries may employ these nonlethal threat systems clandestinely against high-value targets, critical personnel, and even civilian elements in competition to disrupt friendly operations, influence populations, and shape the battlefield prior to armed conflict. Future Army forces require the ability to understand when adversaries are attacking with DEW, and be able to mitigate the effects on friendly personnel and equipment.

(5) Deny RAS, UAS, and swarms. Enemies employ small UAS (classes I, II, and III) that challenge current U.S. air defense capabilities to identify, track, and destroy them due to their size and signature. Ground RAS also present challenges to friendly forces, providing the enemy with potentially overmatching capability and improved capacity. Swarming autonomous capability presents overwhelming challenges to future force systems in terms of detection, monitoring, and destruction of equipment and infrastructure. Future Army forces must deploy organic systems at all echelons to detect and deny RAS, UAS, and drone swarm threats.

(6) Deny ISR activities.

(a) Enemy forces conduct intelligence preparation of the battlefield (IPB) to analyze and produce information that directly supports their C2 planning and direction processes. The enemy employs ISR capabilities to produce intelligence estimates, determine potential friendly courses of action, identify named areas of interest, determine high-value targets, and plan and conduct the targeting of friendly forces. Army forces, with JIIM partners, must deny enemy IPB in order to enable protection of CCAAs and to preserve combat power. The ability to disrupt, control, and manipulate enemy ISR and IPB is key to achieving operational and tactical surprise. Protecting access to relevant cultural, social, religious, economic, and government information can hinder enemy analysis and prevent its understanding of the possible effects of friendly courses of action

on them. It can also prevent their leaders from determining where and when to focus attention to influence events early, ready forces, and set conditions for future operations.

(b) The enemy employs a layered approach of observation, ISR and sensing to see and understand friendly operations in the U.S. homeland, across the strategic and operational support areas, and down to the lowest tactical level. The enemy wants to posture itself to gain advantage, anticipate escalation to armed conflict, and seek vulnerable targets of opportunity that they can quickly and decisively attack. The adversary observes and senses by employing national-level ISR of fixed sites, government and commercial space-based ISR, reconnaissance, special purpose forces, sympathizers, proxies, sensors, ground observation teams, UAS, radars, and signal intercepts. Friendly forces want to deny or degrade the adversary's ability to sense and observe to reduce risk to the force, create windows of superiority, and preserve CCAAs. The future force will employ cross-domain, full-spectrum, and EMS obscuration capabilities to deny enemy freedom of action, deny and degrade the adversary's ability to see and understand, observe, and sense to reduce threat overmatch.

(c) The Army's counterintelligence objective is to neutralize foreign intelligence entities through multi-domain vulnerability assessments, investigations, collection, technical services, support to research, development, acquisition, and other operations. Counterintelligence converged with signals, electromagnetic warfare, cyberspace, CA, special operations forces, and space capabilities enhances the force's ability to collect, identify, and characterize enemy intelligence activities for the purpose of preserving friendly CCAAs across the entire MDO framework and throughout the competition continuum. The counterintelligence activity assists in preserving CCAAs and actively denies enemy freedom of action in the enemy's deep area by reducing their understanding of friendly force actions.

(7) Deny coercion activities. The enemy will attempt to separate the U.S. from partners and allies, deny U.S. objectives, and destabilize areas in order to expand competition space on favorable terms to achieve their strategic objectives through coercion and without fighting. Army forces must quickly identify when, where, and through what means this coercion occurs. This may require a whole of government approach to deny coercion, relying on JIIM capabilities. Army forces must be part of the assessment and recommendations for coercion denial actions to succeed in competition short of armed conflict that denies enemy objectives. Army forces must deny this coercion to assure and reinforce partners and allies through cooperation and competition in pursuit of mutual goals. The force will interdict coercion through bolstering protection activities through mutually supporting goals of readiness, relationships, and interoperability that offer alternatives to partners and allies rather than capitulating to coercion activities and objectives. Army forces must be able to identify CCAAs to be preserved that establish or enhance alliances and partnerships while denying the enemy the ability to employ coercive means that weaken them. Assessments of coercive means and intent against partnerships and vulnerabilities can lead to partner discussions and agreements on long-term protection objectives that preserve from, deter, and deny enemy activities attempting to fracture partnerships and alliances.

(8) Rapidly adapt protection against emerging enemy tactics, techniques, and procedures (TTP). New enemy and adversary tactics, techniques, and procedures will naturally occur as the environment changes or enemies and adversaries adapt. Continuous assessment allows

commanders and staffs to evaluate the progress of achieving desired effects and to adapt protection measures as necessary. When existing protection measures are insufficient, commanders can use existing protection forces, activities, and measures in new ways or combinations to try to address these emerging challenges.

(9) Deny deception. Future Army forces require the capability to detect and deny enemy deception across all domains to preserve CCAAs across the battlefield. Enemy forces employ a combination of physical, virtual, and electromagnetic decoys to operationalize their comprehensive deception plans. Army forces must expect the enemy to execute operations to deceive friendly ISR collection and IPB analysis to gain tactical, operational, and strategic surprise; confuse friendly commanders as to enemy intentions; and to trick friendly forces to waste resources and effects on operationally insignificant missions. Commanders must be able to quickly identify when the enemy is using deception and to understand its implications to the force and operations. The future force must have the ability to identify and unmask the deception, employ forces to use the deception in our favor, or continue to operate while avoiding the deception and presenting to the adversary that their attempts are successful. Commanders require decision aids that can take intelligence from multiple sensors or sources and determine recommended responses.

(10) Deny space, cyberspace, and electromagnetic warfare. The enemy has expanded the battlefield through space, cyberspace, and electromagnetic warfare. The enemy employs offensive cyberspace and electromagnetic warfare to create stand-off in competition and armed conflict. Cyberspace effects combined with conventional and unconventional capabilities create enemy overmatch that threatens the U.S. homeland, allies, partners, and friendly military forces. Through cyberspace and the EMS, the enemy can jam, spoof, exploit, disable, and destroy friendly space, cyberspace, and EMS communications, computing, ISR and PNT. The communications network and the EMS are critical enablers the future force must have to operate in MDO. Cyberspace and the EMS will be a priority for the future force to preserve, counter, and deny enemy freedom of action in this domain. Friendly forces must be able to deny space, cyberspace, and electromagnetic warfare by reducing or denying the enemy's ability to use these services and capabilities against the force. Denying activities restrict enemy observation, tracking, and targeting of friendly forces; deny the enemy use of space, cyberspace, and EMS services and capabilities; and focus competition in the physical dimension, lessening hyperactivity.

(11) Deny information warfare.

(a) The adversary is likely to employ information warfare during everyday activities at home station, abroad, and at the forward tactical edge, targeting friendly leaders, populations, and forces. Information warfare impacts operations in competition and in armed conflict, and will likely keep friendly forces in contact with adversaries for some time to come. Enemy information warfare combines with national-level unconventional and conventional capabilities to create an overwhelming influence on domestic and foreign audiences. Information warfare can be destructive, crippling command nodes and civilian networks and degrading and denying U.S. access to the IE. Friendly forces must identify the adversary's attempt to conduct information warfare and deny it through effective mitigating strategies. With the nature of the IE being global,

the span of information warfare is enormous, and it will require a whole of government approach, along with synchronized actions amongst JIIM partners.

(b) Denying information warfare starts by defending the network, securing command nodes and other infrastructure, and assuring access to services and capabilities. The force must take aggressive actions to deny false narratives, influence actors with a unifying message to survive and win, and reduce vulnerabilities in command nodes and civilian networks. Friendly forces must comply with their role in the IE, be resilient, and understand the impact their actions have at all times. The Army relies on information, intelligence, cyberspace, and irregular warfare capabilities to conduct counter information warfare operations.

c. Enable access. The future force enables access to denied spaces through projecting power from the strategic support area, penetrating, dis-integrating, and exploiting enemy A2/AD, and expanding into the enemy's area of stand-off. As friendly forces push forward, security and protection will hold the gained area while creating and exploiting windows of superiority to further pressure enemy defenses. To enable access, future Army forces require access to space, the EMS, and the IE through distributed and resilient networks to provide all domain-sensing capabilities to continuously detect and monitor enemy activity across the battlefield and competition continuum. These systems, combined with fires and quick reaction forces, enable friendly forces to control terrain, thus preventing, disrupting, deterring, and defeating enemy operations anywhere on the battlefield. Ultimately, the objective is to maintain momentum, consolidate gains, and make temporary control of terrain permanent.

(1) Penetrating and dis-integrating enemy A2/AD systems. Friendly forces penetrate and dis-integrate enemy A2/AD systems to create exploitable conditions and freedom of action by two means. The first is physically attacking those systems with lethal or nonlethal fires capabilities. The second is creating the conditions based on friendly force CCAAs such as usable terrain, infrastructure, and protection conditions in shaping and sustaining operations across the expanded battlefield from the homeland in the strategic support area through the deep maneuver areas. Critical to MDO is the ability to maneuver across strategic and operational distances in time to stop or quickly reverse an enemy's attempted *fait accompli* objectives and while avoiding the premature application of combat power. Protection-enabling capabilities from higher echelons can be attached or augmented through support relationships (direct support, reinforcing, general support reinforcing, or general support) to shape, establish, and retain support areas and operational maneuver corridors.

(2) Counter obstacles and hazards. Army forces will encounter obstacles and hazards across the operational environment. These will include mines, IEDs, unexploded ordnance, non-combatants, restricted terrain, interference in the EMS, and disinformation. When coupled with a dense urban environment, this creates an extremely challenging situation for friendly forces. To overcome these challenges require a combined arms approach converging multiple capabilities to detect and counter obstacles and hazards thus enabling freedom of maneuver and action. To enable access and set the conditions for successful operations, EAB forces shape the terrain ahead of time by identifying obstacles and hazards and developing a mitigating strategy that ensures forces counter impediments to maintain tempo of operations across the OE. If required, forces conduct post-hazard analysis to understand the enemy better.

(3) The protected maneuver corridor. The future force must be able to move and maneuver across the battlefield in all domains to overcome A2/AD, hold areas, consolidate gains, and establish access to achieve mission objectives. Collectively this is a combined arms effort converging Army and JIIM capabilities in all domains, the EMS and the IE to gain access, expand, secure, and preserve movement across strategic, operational, and tactical support areas. The future force establishes the protected movement corridor in the strategic and operational support areas to build combat power, penetrate, and overcome enemy defenses. It expands into the close area, achieving positions of advantage, maintaining tempo, and preserving mobility. The enabling force shapes the deep maneuver area ahead of the tactical combat force in decisive space to ensure access and exploit windows of superiority. This critical operation expands across multiple echelons and requires all elements of combat power. Cross-domain convergence of capabilities maintains and synchronizes effort to enable the force to maneuver and overcome complex A2/AD.

(4) Protective lethal and nonlethal fires. Fires deliver lethal and nonlethal effects across the battlefield to support preserving CCAAs. Protection cells work closely with the fires cell to ensure coverage of high priority CCAAs against enemy threats. Networked protection sensors distributed across the battlefield will have access to fires information systems to cue effects and support as needed. Nonlethal effects may be employed or leveraged from offensive cyberspace, electromagnetic warfare, information operations, and space.

(5) Army deception operations for protection. Future Army forces employ full-spectrum deception capabilities to deny enemy intelligence preparation of the battlefield and information collection, which enables the protection of CCAAs and the preservation of combat power. Future deception capabilities, including EMS jammers and mimicry devices, confuse and complicate enemy targeting to influence the enemy to expend munitions on false targets. Future Army units and Soldiers employ organic deception capabilities to preserve combat power. Forces conduct integrated, all domain deception operations to achieve tactical, operational, and strategic surprise at a larger scale across the battlefield, to include the EMS and IE, and competition continuum.

(6) Mitigate damage to critical infrastructure. Enemy forces may damage or destroy critical infrastructure in their homeland or in countries surrounding them to deny or disrupt friendly force actions across the battlefield. The enemy can do this in competition and in conflict to influence audiences as part of an information warfare campaign across the region. Critical infrastructure may include oil fields, dams, nuclear facilities, ammunition depots, historic sites, and hospitals. During the transition to armed conflict and beyond, friendly forces penetrate and dis-integrate enemy forces and may also destroy infrastructure to achieve a military effect. Future forces must identify critical infrastructure, preserve it, and deny the enemy access to it. Future forces must also develop plans to mitigate the possible destruction of critical infrastructure by the enemy when its use is critical to friendly force operations.

(7) Establish and protect basing. The future force establishes bases in the support area to secure and preserve CCAAs and enable operations. Future Army forces must secure personnel and equipment in the operational support area to prevent theft, sabotage, and destruction. Unlike recent conflicts, bases will be smaller and more austere. For reasons of safety, security, and resiliency, personnel operating in the support areas will be separate from the local population and

threat actors. Forces will likely pool in holding areas that are temporary and static in the tactical support area and close area. Friendly forces must protect critical activities like aviation operations and field hospitals. Future Army forces must secure fixed and temporary bases and holding areas to protect against all types of hazards to preserve operating capabilities.

(8) Condition-based authorities. Future Army forces act in competition and transition to armed conflict against enemies in all domains, with maximum situational awareness of threats in all domains established by sensors and a shared MDCOP. With emerging enemies operating in all domains, response time is critical. Forces cannot rely upon a deliberate process for approval for actions; they must rely upon disciplined initiative. Delegating authorities to appropriate lower-level commanders will help reduce delays in implementing protection actions. Specific examples of authorities that might require conditions-based delegation are changes in the rules of engagement, cyberspace authorities, or access to restricted terrain. These authorities enable commanders to act in all domains, with both lethal and nonlethal means, in a timely manner, preventing a *fait accompli*, while protecting CCAAs.

(9) Timely mobilization and deployment operations. Future Army forces require the capability to quickly mobilize and deploy from strategic support areas to the JOA to deter escalation and defend against enemy offensive operations across the battlefield and competition continuum. Mobilization and deployment are critical to deterring the enemy during the competition period and winning in armed conflict. The enemy will contest all deployments, challenging tempo of movement and restricting the build-up of combat power. Mobilization and deployment are especially challenging for protection-enabling formations, where the bulk of capabilities and capacity is in the reserve components. Many different approaches are possible to improving mobilization and deployment timelines:

(a) Future forces reduce the weight and form factors of equipment, vehicles, and supplies to lessen deployment transportation air and sea requirements.

(b) Placing lighter forces that are more easily transported in the strategic support areas while calibrating heavier forces forward reduces sea and airlift deployment operational requirements.

(c) Future forces preposition equipment forward to enable rapid capability increase, thus improving deterrence in specific regions.

(d) Predictive maintenance to reduce required on-hand balances of class IX supply based on condition monitoring and persistent platform feedback.

(e) Automating and utilizing AI to improve medical readiness to reduce/eliminate mobilization medical requirements.

(f) Fielding advanced manufacturing capabilities to units to print repair parts on demand to improve equipment readiness at the point of need.

(g) Utilizing virtual simulators to improve Soldier and unit training readiness and reduce mobilization-training requirements.

3-5. All domain protection at echelon

a. A description of the warfighting function at echelon is important to revitalize the protection WfF as a core competency for the Army in MDO. Protection must become dynamic, anticipatory, and proactive. The Army must protect CCAAs across echelon to survive and win in future operations. Protection starts with the individual Soldier, who must understand the threat at all times and be aware of how the enemy will likely engage him or her on the future battlefield. At the unit level, the Army must be able to preserve itself, be resilient, and withstand enemy attack. When units are unable to protect themselves, commanders will coordinate with protection chiefs for support. Commanders at each echelon prioritize protection by coordinating support for and applying resources to the most critical needs to preserve the identified CCAAs.

b. Strategic support area (SSA).

(1) The SSA forms the foundation for MDO campaigning, includes the homeland, and supports cross combatant command coordination. The U.S. Army and DOD conduct critical installation and infrastructure security and protection. Headquarters, Department of the Army establishes policies and fields equipment to preserve installations. Installation commanders control access to and preserve their facilities through physical security. U.S. Northern Command and U.S. Army North, as well as other combatant commands and supporting Army Service component commands where the SSA may extend, also coordinate protection for their areas of responsibility.

(2) The SSA includes national level nuclear, space, cyberspace, and information capabilities. The force must have assured access and freedom of action across all domains. The Army will build and project combat power from the homeland and other locations to the operational support area. Commanders will coordinate the security and protection of strategic movement from the home installation to the joint operational area.

(3) The enemy can reach through to the SSA and create stand-off to disrupt friendly power projection. Future forces will deny irregular and information warfare to preserve CCAAs and enable freedom of action. The force coordinates with SOF and JIIM partners to disrupt irregular warfare, and operates in the IE to control the narrative and ensure messaging is accurate and meets mission objectives that preserves operations.

c. Theater.

(1) Theater protection capabilities focus on enabling the operational support area. The theater secures ports, LOCs, facilities, ground-based elements of space-based systems, the flow of forces and materials, and coordinates support with national technical means (space, cyberspace, EMS). The theater facilitates the linkage to interagency and host nation support to cover down on critical capabilities and capacities to expedite operations. Force presence in competition deters the enemy and preserves C2, sustainment, and force generation. The theater coordinates with national level assets assuring access to critical all domain technical capabilities for convergence at the point of need.

(2) The protection staff visualizes vulnerabilities for commanders, staffs, and leaders, and articulates strategies to overcome and preserve CCAAs. The staff must have a focus on predictive and proactive measures that deny the threat from achieving their objectives. The staff recommends measures to deny enemy stand-off, reducing the degradation, disruption, and denial of friendly force operations. Protection staffs advise commanders on the transition criteria required for advancing operations based on when the force is postured to best protect itself.

(3) The theater Army requires a multi-functional capability to provide operational and campaign quality planning, synchronization, integration and C2 of protection capabilities in support of Joint Forces Land Component Command requirements in both competition and conflict. This capability will support the commander preparing the environment and enabling protected maneuver at operational distances and the independent maneuver of theater forces.

(4) During competition, and as the force sets the theater, theater assets prepare the operating environment by understanding critical aspects that will affect future operations. The staff must understand threat CBRN, health, criminal, and irregular actors, terrorist organizations, obstacles, and friendly and neutral forces. The staff examines the area's suitability to conduct future operations by identifying LOCs, critical infrastructure, potential protected positions, and areas to support basing. The theater Army continues to coordinate and deny irregular and information warfare, preserving and defending access to all domain capabilities. Persistent presence builds resilience in the theater security area, enabling force deployments to quickly overcome A2/AD and penetrate, dis-integrate, and exploit the enemy.

(5) As tensions grow and the transition from competition to armed conflict continues, the theater force secures friendly LOCs, facilitates movement of equipment, and integrates with JIIM partners to increase security and protection capacities, thus freeing up the force to move to protected positions. The protection staff identifies enemy systems that present the greatest protection challenge to the force through all domain sensors, counterintelligence, and SOF, and coordinates counteractivities to deny enemy freedom of action in friendly support areas. Theater defenses have access to and operate in the cyberspace and space domains, the EMS, and IE.

(6) Once operations transition back to competition through the consolidation of gains, the theater takes responsibility of the area. The theater will track and remove enemy remnants left over and bypassed that present risk to the force. Once the theater Army meets conditions, it transitions control of the area to the host nation or a military authority. The theater Army will continue to support operations through security and preservation of LOCs, ports, and holding areas as U.S. forces exit the area.

d. Corps.

(1) The corps maneuvers into the operational area to gain a position of advantage, shape security, and enable the transition to armed conflict or LSCO as tensions continue to escalate. The corps sets conditions for the divisions, assigned brigade combat teams (BCTs), and enabling supporting units to gain access and defeat enemy A2/AD. The protection cell at corps integrates with intelligence to see and understand the environment, coordinate counterintelligence to clearly

recognize threat actors, and identify key enemy systems that present the greatest risk to friendly forces. The staff must have a focus on predictive and proactive measures that deny the threat from achieving their objectives. Protection prioritizes requirements, coordinates and synchronizes support, and preserves CCAAs across the area. The force secures areas, units, supplies, and activities through security operations, survivability, and deception. The force gains access to the space and cyberspace domains and the EMS and IE for friendly force use, to control the information narrative, assure communications, and conduct denial activities.

(2) The corps protection cell coordinates with the other staff sections to synchronize and converge multi-domain capabilities that deny the enemy freedom of action in the friendly support areas (enemy deep areas). The staff coordinates space, cyberspace, EMS, and IE effects down to the corps area of operations. The protection staff coordinates lethal and nonlethal targeting with the fires cell, identifying and denying enemy systems that present a protection challenge to the force.

(3) The corps continuously shapes for the division by engaging and clearing threats that present close range challenges to the BCTs. The corps pushes protection and security capabilities to the division to support operations. They ensure the division has engineer, military police (MP), medical, AMD, CBRN, cyberspace, EMS protection, and EOD capabilities as needed. The corps integrates with SOF to deny irregular warfare conducted in the support areas and to identify and locate enemy systems that will affect friendly operations from the deep areas.

(4) During LSCO, the corps sets conditions for the division to transition, gain access to denied areas, consolidate, and facilitate continuous onward movement thus reducing risk to the force. The corps shapes the area for the division and BCTs; maintains, protects, and secures LOCs with dedicated assets; and employs obscuration and deception to improve survivability of friendly forces operating in and around the enemy.

(5) The corps requires a multi-functional capability to provide operational planning, synchronization, integration, and C2 of protection capabilities in support of theater Army requirements in both competition and conflict in order to integrate and synchronize protection in the corps area. The protection element secures key terrain, nodes, and activities in the area, and protects movement through the corps support area. The protection element integrates other protection activities at corps to enable the division and subordinate BCTs.

(6) The protection chief at the corps must describe, visualize, and articulate to the commander, staffs, and leaders on conditions and situations prior to transitioning, expanding operations, and moving forces when there is a protection risk to the force. This chief must think and act in a manner that is proactive and predictive of the threat, with the tools available to deny the threat prior to the threat acting. The protection cell establishes measures that best describe when conditions are right for transitioning.

e. Division.

(1) The division provides additional capabilities to help protect assigned BCTs in its close immediate area. The protection staff assesses vulnerabilities, determines risks, coordinates, and

synchronizes support to enable cross-domain maneuver. The staff must have a focus on predictive and proactive measures that deny the threat from achieving their objectives. The protection cell works with and through the other warfighting functions and supporting staff cells to identify the threat and determine what CCAAs must be protected, identify what is critical, and coordinate resources required to preserve essential CCAAs either organically or by coordinating outside of the division for support.

(2) The presence of divisions in the joint security area creates deterrence and shows the resolve of U.S. forces in competition. Constant integration and convergence of cross-domain capabilities generates and preserves combat power to support operations. In the transition to conflict, the division coordinates with theater AMD to ensure coverage of CCAAs. The division staff also coordinates activities to preserve combat power and deny enemy freedom of action through denying enemy air, UAS, fires, ISR, and other conventional force activities. Friendly forces protect and preserve information and access to effects and capabilities in the space and cyberspace domains, the EMS, and IE to enhance division operations. Friendly forces employ OPSEC and deception to mask friendly force movement and action, and the protection cell participates in the targeting process by identifying and targeting key enemy systems in all domains that present a challenge to friendly operations.

(3) Divisions and assigned units operate while highly dispersed, only aggregating capabilities on a target to overwhelm the enemy quickly, then rapidly disaggregating and moving to the next objective. The division creates conditions through all domain capabilities that enable BCTs to penetrate deeper into enemy A2/AD, maintain separation, reduce risk, consolidate short gains, and continuously expand, maintain momentum and control the tempo of the operations. Throughout LSCO, the force employs deception techniques to preserve assets and create confusion with the enemy. When absolutely necessary, the division and BCTs conduct deliberate all domain defense to survive and withstand adversary actions.

(4) The division requires a multi-functional capability to provide tactical planning, synchronization, integration, and C2 of protection capabilities in support of corps requirements in both competition and conflict. The division protection element secures and protects LOCs and the support area, and coordinates the application of protection across the division area of operations. This cell must think and act in a manner that is proactive and predictive of the threat, with the tools available to deny the threat prior to the threat acting.

f. Brigade combat team.

(1) The BCT is inherently responsible for protecting itself and has the organic assets to achieve all domain protection. Divisions allocate BCTs with additional required resources needed for the duration of the mission based upon weighting of the main effort and supporting efforts. The division will shape close, and the corps will shape deep, to enable BCT maneuver while preserving their freedom of action. Critical in protecting the force is detecting threats, obstacles, and hazards that can halt movement, slow momentum, and stop the force in its tracks thus exposing it to enemy direct engagement.

(2) The BCT operates dispersed, moving, and converging multi-domain capabilities in a manner that takes advantage of enemy vulnerabilities to apply maximum force to the absolute point of need and overwhelmingly achieve its objectives. In LSCO, the BCT conducts cross-domain maneuver, integrating fires, aviation, and effects from space, cyberspace, and the EMS and IE, making it a valuable resource to conduct and augment protection operations as an enabler when not engaged in decisive operations. The presence of the BCTs during competition and in the transition to armed conflict provides value at preserving CCAAs at the division level and below against all domain threats.

(3) A brigade protection chief is critical in advising the commander and staff on vulnerabilities and risk, and recommends measures that overcome enemy activity and preserve CCAAs. This chief must think and act in a manner that is proactive and predictive of the threat, with the tools available to deny the threat prior to the threat acting. The protection cell communicates requirements to the division for coordination and allocation of resources as well as ensuring subordinate units are capable of protecting themselves. The protection chief informs the commander when conditions are not favorable for transitions. The BCT will operate in and through the space, air, and cyberspace domains, the EMS, and IE to conduct their missions, and must have assured access and the ability to overcome degradation and denial of effects in those areas.

(4) Protection in today's BCT is ad hoc. Further analysis is required to determine the validity of a brigade protection chief and cell, and the appropriate resourcing at echelon. The future Army must ensure the protection chief has the right expertise to implement all-domain protection at the BCT echelon, if the Army validates the requirement.

3-6. Army protection in MDO

a. The activities and functions described in this section have a specified contribution to the protection WfF across the battlefield and competition continuum. These units and capabilities bring a significant contribution to preserving the force, and collectively their sum is greater than their singular application.

b. Protection cells at EAB headquarters. The EAB headquarters at the division, corps, and theater Army require a WfF staff to visualize and outline protection requirements to the commander, prioritize and synchronize mitigating strategies, and coordinate protection. A protection cell is the preferred solution, with the required staff assigned to provide expertise. The protection cell conducts working groups with representatives from the other staff sections to round out the synchronization of the WfF. Members of the cell participate in other working groups as required. The future Army must train and prepare leaders on the skills necessary to analyze all domain threats, protection planning, protection assessment, threat mitigation, and convergence of capabilities to create options for the commander.

c. Military police. Future MP forces train, equip, and organize to detect, deter and defeat all levels of threats and to preserve CCAAs across the expanded battlefield. MPs protect the force with their strengths and unique capabilities, demonstrated through their common behaviors and attributes developed from four core competencies of Soldiering, policing, investigations, and

corrections. MPs provide a full range of capabilities across their three disciplines of police operations, detention operations, and security and mobility support. MPs preserve, secure, engage, and destroy the enemy across the support and close areas, enabling commanders to apply maximum combat power to decisive spaces during LSCO. MPs, through advanced platforms, enable increased mobility, survivability, and lethality. MPs include military and civilian personnel (employed by the DOD or JIIM partner) performing these functions across the MDO framework.

(1) Area security. The future force conducts area security to preserve CCAAs against enemy attack, sabotage, and criminal activity across the battlefield. MPs support area security operations in the support areas so commanders can apply maximum combat power to decisive spaces. Area security focuses on preserving bases, tactical assembly areas, movement corridors, lines of communications, ports, and prepositioned stocks. The future force will rely on joint and multinational partners to contribute to area security in the support areas. MP forces conducting area security require the lethality, survivability, and mobility to engage enemy forces and to be interoperable with JIIM partners.

(2) Security and mobility. MPs conduct security and mobility operations to preserve and secure CCAAs against enemy attack along routes and in and around areas, specific sites, infrastructure, and activities. MPs conduct reconnaissance and surveillance; identify threats, obstacles, and hazards; patrol routes and movement corridors; control populations; and engage with the enemy with direct contact. Future MP teams require increased lethality, survivability and mobility to engage enemy targets in the support areas in LSCO during armed conflict, and must be a formidable deterrent in competition. Future MP forces require advanced technology to increase security and mobility capability and expanded capacity to meet the demand of the future battlefield.

(3) Antiterrorism. MPs employ defensive measures to preserve CCAAs against terrorists, criminals, and irregular threats across the entire battlefield and in both competition and armed conflict. In MDO, the enemy, criminals, terrorists, and surrogates will seek to destroy and disrupt vulnerable CCAAs in armed conflict, and will act in competition with actions short of armed conflict that enables them to accomplish strategic goals without escalation. The future force must understand the threat, identify vulnerabilities, and deny enemy action to preserve CCAAs.

(4) Physical security. The future force employs physical security measures in-depth across the MDO framework to preserve CCAAs. As the force establishes a presence in competition, MPs must secure critical facilities, holding areas, sustainment nodes, key infrastructure, and C2 nodes. The enemy seeks to directly and indirectly degrade or destroy vulnerable CCAAs through criminals, irregular threats, and surrogates across the battlefield. MPs can advise on proper physical security measures and augment security of the most critical CCAAs. Current and emerging physical security technology and techniques employed at bases, installations, and critical facilities around the world should be considered for use in tactical combat operations.

(5) Detention operations. MPs conduct detention operations to control populations that pose a threat to friendly military operations across the battlefield. Detention operations include controlling detainees, enemy prisoners of war, civilian internees, and corrections functions for the control and evacuation of U.S. military prisoners. Detention operations are essential to LSCO in

MDO to preserve friendly force freedom of action across the expanded battlefield. MPs secure, move, and process detainees and prisoners and secure areas to reduce impact to friendly operations.

(6) Police operations. MPs conduct police operations to preserve CCAAs and to facilitate a lawful and orderly environment. MPs maintain order and discipline in the ranks for commanders and uphold governance and the rule of law during competition. The enemy infringes on stability through criminals, irregular activity, and surrogates to achieve small-scale quick wins that fracture alliances between U.S. forces and multinational partners. Police operations are critical during consolidation of gains and return to competition as operations transition from armed conflict back to competition.

(a) Police intelligence operations (PIO) underpin police operations by enhancing situational understanding, civil control, and law enforcement activities and enabling the preservation of CCAAs. The future force requires a clear understanding of terrorists, criminals, irregular activities, and other threat actors who seek to disrupt friendly actions across the expanded battlefield in both competition and armed conflict.

(b) PIO enhances situational understanding and informs decision making. It enables MPs and supported commanders by improving situational awareness, contributing to understanding the OE and providing police intelligence. PIO provides timely, relevant, and accurate criminal intelligence and crime analysis products that identify crime patterns, trends, hotspots, environmental conditions, and problems that threaten the accomplishment of the commander's desired end state. PIO enables the force to act against threat actors, prevent adverse actions, preserve multinational partnership, and ensure freedom of action.

(7) Biometric and expeditionary forensic capabilities enable identity intelligence. This capability will prove instrumental in Army forces' ability to effectively deny and defeat near-peer competitors during MDO across the competition continuum. Forensic and biometric identification enable MPs to locate and identify actors across the expanded battlefield. Threat actors will strive to blend into the population, fight and manipulate among the people, and create blurred dilemmas for commanders. Biometrics identifies threat actors and expeditionary forensics preserves CCAAs, supports targeting, and enables prosecution of threat and criminal actors. Future Army forces require advanced forensic and biometric capabilities to enhance identification of threat actors and provide support to policing and protection of the force.

d. Intelligence. Intelligence capabilities contribute to protection by collecting and sharing information about the OE. Intelligence capabilities contribute to protection by collecting, storing, analyzing, and disseminating detailed, timely, relevant information about the threat and the OE. To accomplish this, intelligence leads the staff in conducting IPB of all domains, the EMS and IE, and portrays the enemy's course of action during wargaming to include conventional and asymmetric all-domain capabilities and strengths and vulnerabilities.

(1) Collection and analysis. Intelligence collects using traditional all-source intelligence platforms, including signals intelligence, geospatial intelligence, human intelligence, CI, technical intelligence, measurement and signature intelligence, and open-source intelligence. Intelligence Soldiers collect, exploit, and disseminate information from other sources such as biometrics,

forensics, document exploitation, cyberspace, and operational reporting. The goal is to visualize the enemy as a complex system of inter-related capabilities and provide the commander with sufficient situational awareness to enable his understanding and decision-making process to include protecting the force.

(2) Some protection efforts that provide information rely on intelligence analysis and production to realize their value. For example, biometrics/expeditionary forensics rely upon identity intelligence to produce the biometrics enabled watch list. Other times, there is a symbiotic relationship between protection and intelligence, such as when detention operations and interrogations derive value from each other.

(3) Intelligence provides valuable links between non-DOD intelligence community entities, including Department of State, Department of Energy, and Department of Justice that are especially valuable in protection efforts during competition. This includes facilitating terrorist prosecutions and security of the defense industrial base. Additionally, it can provide the ability to leverage the deep bench of experts in fields where the Army does not have much experience, including facility-related control systems.

(4) Counterintelligence (CI). U.S. Army CI is the Army component of U.S. Military Department Counterintelligence Organizations (MDCO) that conducts counterintelligence activities to detect, identify, assess, counter, exploit, and neutralize adversarial, foreign intelligence service, international terrorist organization, and insider threats to the Army and DOD.

(5) Security programs. Army protection and intelligence execute supporting functions for the Army commander for information security, personnel security, industrial security, and physical security to include sensitive communications, facilities, and special access programs.

e. Civil affairs (CA). CA organizations bring a critical capability to protection when operations require interaction with the local populations and multinational partners. CA forces set conditions by, with, and through local civilians and JIIM partners to leverage capabilities and cooperation to enable operations. CA conducts civil reconnaissance by mapping civilian networks assisting in detecting obstacles, threats, and hazards. CA capabilities support protection in identifying enemy conventional and irregular warfare opportunities, assisting in unifying friendly efforts and consolidating friendly gains.

f. CBRN. CBRN units provide support to protection through the core CBRN functions of assess, protect, and mitigate. CBRN forces accomplish the assess function through the integrating function of CBRN hazard awareness and understanding (HAU) and employment of robust reconnaissance and surveillance (CBRN R&S) to provide the commander with real time understanding of enemy CBRN threats or hazards in the OE. The CBRN protect function provides an integrated, layered, systematic capability that ensures personnel, systems, and critical functions/actions are maintained at tempo, negating desired enemy effects. Innovative contamination mitigation provides tactical and operational forces the ability to minimize force attrition due to the effects of CBRN hazards in OE while rapidly reconstituting combat power.

(1) Assess. Enhance CBRN protection through a functionally integrated communications network that increasingly nests R&S capabilities with C2 nodes, enabling commanders to understand the threat and make informed, risk-based decisions to protect the force and retain freedom of action ahead of the enemy decision cycle to use CBRN.

(2) Protect. Provide the force with tailorable PPE and collective protection solutions that minimize risk to forces and allow maneuver units to exploit the CBRN environment to gain or maintain positions of relative advantage in LSCO.

(3) Mitigate hazard effects. Provide maneuver units with immediate organic decontamination solutions that reduce risk to forces and allow commanders to retain flexibility without reduction in combat power or sacrificing positional advantage.

g. Medical. Medical units support protection through FHP that promotes, improves, or conserves the behavioral and physical well-being of Soldiers. FHP is comprised of preventive and treatment aspects of medical functions that include combat and operational stress control (COSC), dental services, veterinary services, operational public health, and laboratory services. These measures enable a healthy and fit force, prevent injury and illness, and protect the force from health hazards during MDO. Soldiers face health challenges caused by environmental, industrial, occupational health, and direct combat exposure. The future Army force must understand the environment, identify health threats, and disseminate information to the force. FHP is critical to preserve CCAAs in MDO.

(1) The Army health system (AHS) at echelon requires the capability of protection of patient movement item nodes, ground and air evacuation routes/flight paths, ambulance exchange points, medical logistics sites, medical facility (temporary and permanent) locations and sites associated with medical host nation support support. They provide medical treatment and evacuation to clear the battlefield and maximize return to duty and to enable corps, division, and BCT freedom of action and maneuver.

(2) The Army has dependencies on public and private strategic capabilities (e.g., MEDCOM, Public Health Command, Armed Forces Health Surveillance Network, National Disaster Management System, CONUS/Veteran's Administration/host nation facilities). These dependencies enable a network of critical skill providers, joint integration, availability of expanded capabilities/capacities, and strategic force health protection capabilities. The potential divestiture of strategic medical capabilities and the ability to integrate and synchronize the delivery of U.S. medical strategic capabilities/enablers will affect the theater Army and corps during LSCO.

(3) Future Army forces require the capability to conduct occupational and environmental health site assessments using autonomous and semi-autonomous data collection methods in both competition and in armed conflict. These assessments will help prevent illness and injury to the Joint Forces while conducting MDO in a JOA and to enable theater army, corps and division freedom of action and maneuver.

h. Engineer. Engineer capability at all echelons across the continuum of MDO enables the protection WfF to preserve personnel and physical assets. Engineer units enhance protection

primarily through the employment of survivability and terrain shaping capabilities, and enable access by assuring mobility and trafficability within protected maneuver corridors.

(1) Survivability operations are the activities that alter the physical environment to preserve CCAAs while enhancing the quality or capability to withstand hostile actions and enables friendly forces to fulfill its primary mission. MDO requires Army forces at echelon to possess the capabilities to conduct continuous survivability operations and activities within the land domain. The future force will require technologically advanced survivability capabilities to enable continuous survivability in all domains. Specific engineer activities enabling survivability include the construction of cover, fighting, and protective positions the hardening of facilities; and the employment of camouflage and concealment to disguise the appearance of friendly military targets. Engineer tasks that support survivability operations occur primarily at the operational and tactical levels of war.

(2) . Army forces conduct countermobility operations by using the effects of natural and manmade obstacles in the land domain to deny enemy forces freedom of movement and maneuver. Countermobility tasks enable combined arms forces to shape where and when enemy movement and maneuver occur, and prevent the enemy from gaining a position of advantage. Future countermobility systems will employ a scalable range of effects. Enemies will seek to create advantageous conditions by conducting operations in complex terrain and other populated areas to diminish the potential employment of friendly countermobility capabilities as a way of offsetting friendly force advantages. Engineer forces employ obstacles to achieve the desired effect in support of maneuver forces. Army forces provide capabilities to shape the terrain to slow or divert the enemy, to increase time for target acquisition, and to increase weapon effectiveness in support of the combined arms team.

(3) Engineer forces deny the utility of explosive hazards by detecting explosives and explosive components, mitigating explosive hazard effects, and preventing or neutralizing explosive hazards to protect personnel, equipment, facilities, and maintain mobility. To deny explosive hazards, forces identify and provide early warnings of suspected explosive devices to be used against personnel, vehicles, command nodes, and aircraft in near real time. Engineer, CBRN, and MP forces assist in the intelligence process by performing post-blast analysis, fragmentation analysis, and site exploitation, as well as tracking explosive hazards to enable situational awareness and predictive analysis. Future forces require advanced capabilities to safely detect, mitigate, and neutralize explosive hazards.

(4) Tactical level engineers build, repair, and maintain fighting and protective positions to enable the protection WfF. Engineers clear and maintain routes to preserve mobility and enable access.

(5) Operational level engineers harden facilities and emplace protective obstacles to enable the protection WfF. Engineers maintain and improve critical sustainment and power projection nodes to better enable access. Engineer divers and firefighting teams provide specialized enhanced protection capability to preserve personnel and assets.

i. Fires.

(1) AMD. AMD organizations provide deterrence and preserve CCAAs across the battlefield in competition and armed conflict enabling freedom of action and rapid power projection to penetrate enemy A2/AD. Capabilities include detection, tracking, discrimination, early warning, and destruction of enemy ballistic, cruise, hypersonic and other air targets in support of geographic combatant commanders. The Army accomplishes AMD by theater level multi-component brigade-size organizations operating at echelon above corps supporting the warfighting combatant commander. The Army Air and Missile Defense Command staff supports the joint or combined forces air component command by planning, coordinating, and integrating theater-level air and missile defense operations.

(2) Ground-based midcourse defense (GMD). GMD is the U.S. anti-ballistic missile system for intercepting incoming warheads in space, during the midcourse phase of ballistic trajectory flight. It is a major component of the U.S. missile defense strategy to deny intercontinental ballistic missiles. U.S. Missile Defense Agency developed and sustained GMD with operational control by U.S. NORTHCOM and execution by U.S. Army Space and Missile Defense Command.

j. Cyberspace and electromagnetic warfare. Cyberspace and electromagnetic warfare organizations provide cybersecurity activities, defensive cyberspace operations, electromagnetic protection, and defensive electromagnetic attack to preserve CCAAs.

k. EOD. EOD units enable the protection WfF to preserve personnel and physical assets through the employment of EOD capabilities and tasks across the battlefield in competition and in armed conflict.

(1) Technical intelligence. EOD units contribute to force protection intelligence, targeting, and denying enemy deception and deniability through exploitation and analysis of captured enemy ordnance.

(2) Enhancing survivability. EOD units enhance survivability operations through their unique ability to nondestructively render safe and remove explosive hazards from CCAAs.

(3) Protecting the homeland and SSA. EOD units protect the homeland and the SSA through persistent DSCA operations, immediate response authority, and close working relationships with civil authorities and JIIM partners.

(4) Mitigate explosive hazard effects. EOD units provide commanders with technical intelligence and threat assessments, giving them the ability to make risk-based decisions on protective posture and tactics, techniques, and procedures in a given area to mitigate the risk of explosive hazards.

l. Space and high-altitude. Space and high-altitude capabilities provide the tools enabling protection operations at each echelon to extend the power of joint space capabilities via the tactical space layer. The space domain will be comprised of a multitude of small satellites and other platforms linked together by a mesh network focused on providing beyond line-of-sight communications, PNT augmentation, navigation warfare (NAVWAR), missile warning, deep

sensing ISR, and deny space activities. In the future MDO environment, the enemy will cut into friendly decision timelines, reducing the force's ability to plan and execute operations. To succeed against a near-peer competitor requires on demand, resilient communications on a theater scale, which is tactically responsive to the warfighter during competition and armed conflict. Army space forces deny adversary space-based ISR and support forward commanders through tasking of assigned space ISR assets.

(1) Satellite communications. Satellite communications provide the necessary connectivity for worldwide communications for mobile forces operating over large, dispersed areas. It provides the Army critical connectivity for tactical maneuver forces and Soldiers whose rapid movement and geographically dispersed deployments move them away from direct access to land lines and line-of-sight communication. Satellite communications enable protection through sensing, communications, long-range targeting, and friendly force tracking.

(2) Missile warning. Missile warning systems detect the movement of ballistic missiles and high-energy infrared events such as the hot exhaust of an intercontinental ballistic missile. Joint tactical ground stations provide warning of missile launches. These stations receive downlink data directly from space-based infrared sensors on missile launches. Forward deployed and strategically located, joint tactical ground stations provide warning and threat characterization supporting U.S. homeland defense and theater ballistic missile defense.

(3) Environmental monitoring. Space forces provide data on meteorological, oceanographic, and space environmental factors affecting military operations. Space capabilities provide data for forecasts, alerts, and warnings of the space environment, which may negatively influence space assets, space operations, and terrestrial users. Imagery capabilities can provide joint force planners with current information on subsurface, surface, and air conditions, such as trafficability and land use, beach conditions, vegetation, cloud cover, and moonlight percentage.

(4) NAVWAR operations. NAVWAR is the deliberate defensive and offensive action to assure and prevent PNT information through coordinated employment of space, cyberspace, and electromagnetic warfare operations. The effects of a NAVWAR environment on systems are complex and range from limited in scope and area to enveloping an entire OE. NAVWAR effects include varying conditions from mildly degraded to totally disrupted global navigation satellite system signals, and may include spoofing, which is an emulated signal with false and misleading information. Space operations focus on space-based PNT signals, situational understanding, and space control operations. Cyberspace operations protect friendly networks that leverage global navigation satellite system, while targeting similar adversary capabilities. Electromagnetic warfare operations in support of NAVWAR include electromagnetic support, electromagnetic attack, and electromagnetic protection; deny adversary access to global navigation satellite system information; and protect friendly capabilities within the EMS.

(5) Space activities integrate with intelligence, information warfare, cyberspace operations, electromagnetic warfare operations, and signal assets to support force protection, target development, and information operations as required. Space operations enhance many areas across the Army to include situational understanding, fires, movement, cyberspace electromagnetic activities, electronic warfare, information operations, protection, and many others.

Space adds high-tempo, noncontiguous, dispersed, and decentralized attributes to the future force conducting operations across the battlefield and competition continuum.

3-7. Protection across the competition continuum

a. The U.S. Army in MDO must deter and defeat the threat in competition and in conflict. The Army Operating Concept describes five problems aligned to the three parts of the competition continuum that the force must accomplish to achieve the strategic objectives: competition, conflict (penetrate, dis-integrate, and exploit), and return to competition on more favorable terms. Protection enables MDO across the competition continuum by preserving CCAAs, denying enemy and threat freedom of action, and enabling access. The following sections describe how protection enables MDO across the competition continuum. Additional contributions may be identified through focused MDO learning and experimentation. Appendix D includes more information about the competition continuum.

b. Contributions to competition. Army forces, as part of JIIM, compete with a near-peer adversary by defeating their operations below the threshold of armed conflict, expanding the competitive space, and deterring an escalation of violence. Protection in competition achieves four critical objectives: deter conflict, deny expansion of competitive space below armed conflict, enable rapid transition to armed conflict, and protect the force (preserve – deny – enable). Protection operations and activities in competition include:

(1) Train Soldiers, commanders, staffs, and JIIM partners on protection procedures.

(2) Train units on employing integrated protection effects.

(3) See and understand the operating environment.

(4) Prepare, integrate, and synchronize for operations.

(5) Preserve CCAAs.

(6) Build partner capacity.

(7) Calibrate force posture required to deter and defeat.

(8) Deny enemy information/unconventional warfare.

(9) Conduct survivability of C2 and logistic nodes.

(10) Plan and execute protective deception operations, to include supporting OPSEC.

(11) Coordinate protection authorities.

(12) Synchronize and plan protection requirements with forward deployed Army Special Operations Forces in support of Theater Special Operations Command (TSOC) and Special Operations Joint Task Force (SOJTF) objectives.

(13) Enable the rapid transition to armed conflict.

(14) Monitor the environment for threat actors.

c. Contributions to armed conflict. When competition fails and operations transition to armed conflict, the Army seeks to rapidly defeat aggression through calibrated force posture, multi-domain formations, and converging capabilities. In armed conflict, friendly forces penetrate threat stand-off, dis-integrate A2/AD, and exploit freedom of maneuver to quickly and decisively win. Protection enables the force in armed conflict to preserve, deny A2/AD, and enable access. Protection activities in armed conflict include:

(1) Enable the force to penetrate, dis-integrate, and exploit.

(2) Conduct continuous protection assessment.

(3) See, understand, and characterize the threat and risk to the force.

(3) Enable strategic and operational maneuver.

(4) Coordinate for AMD support.

(5) Support consolidation of gains in decisive spaces.

(6) Defend cyberspace and protect the EMS and IE.

(7) Conduct activities to deny enemy A2/AD.

(8) Conduct mobility support, countermobility and survivability.

(9) Conduct recovery of isolated personnel and forces.

(10) Mitigate threat effects in the support areas.

(11) Cover, conceal, camouflage, and deceive the adversary.

(12) Coordinate aerial surveillance and converge capabilities to preserve the force.

(13) Support see-deceive-maneuver.

d. Contribution to a return to competition on more favorable terms. Friendly forces consolidate strategic gains and return to competition under more favorable military and political conditions. This includes deterring the threat's return to armed conflict and assisting partner forces to restore

order. Protection enables transition back to competition by securing the initiative and maintaining operational contact in all domains, the EMS and the IE. Protection activities in a return to competition:

(1) Secure key terrain in all domains.

(2) Secure friendly populations and resources.

(3) Regenerate partner and Army capacity.

(4) Recalibrate the protection force posture.

(5) Expand influence in all domains.

(6) Re-establish essential services and governance.

(7) Re-establish deterrence.

(8) Conduct denial activities to preserve the force.

3-8. Supporting ideas

a. The following supporting ideas enhance the protection WfF to preserve CCAAs.

b. AI, data science, cognitive engineering, decision support tools, and enabling C2. AI will reduce the cognitive demands on staffs and commanders created by the speed, complexity, and scale of the future MDO environment. These tools enable the conduct of protection planning and execution. Army forces must seek to disrupt enemy targeting by enabling commanders to see themselves from the enemy's perspective by continuously sensing, identifying, and analyzing data automatically identifying courses of action so that commanders can synchronize and prioritize protection requirements and outcomes. AI-enabled systems enhance understating and support commanders in making critical operational decisions to preserve CCAAs, deny enemy freedom of action, and enable access across the battlefield and competition continuum. This includes assessing threats, obstacles, hazards, the EMS, and CBRN data, and rapidly providing commanders with large amounts of data for risk-based decision making.

c. RAS. RAS enhance protection outcomes by increasing situational awareness, lightening Soldier physical and cognitive workload, facilitating movement, securing and preserving CCAAs, and sustaining the force. Future forces require RAS to remove Soldiers from hazardous conditions like chemically contaminated areas and complex obstacle breaches, improve overall capability, and increase capacity.

d. Active and passive defense. Army formations use both active and passive measures to protect key elements of combat power, particularly from air and missile attack. From distributed positions along temporary protected corridors or distributed areas of operations, Army forces strike critical nodes reducing the enemy's ability to respond and limit friendly maneuver options. To

create temporarily protected positions of advantage, forces can use both physical and non-physical means in combination to shield key interests.

(1) Active defense is the approach to actively attack or counterattack through limited offensive action to deny or restrict freedom of action to the enemy. The solution "deny enemy freedom of action" is the primary way protection forces actively defend in MDO. This concept is driving an assertive effort to shift toward an active approach to protection. Active protection measures include using deception, electromagnetic warfare jamming, information warfare, security patrols, lethal and nonlethal effects, and denial activities.

(2) Passive defense minimizes the effects caused by hostile action without taking offensive action. Measures include camouflage, concealment, employing sensors, hardening facilities, encryption, fortification, and dispersion.

e. Counter-targeting. Operations, targeting and other processes must sufficiently embrace protection requirements and capabilities. Protection activities must take a more active role in counter-targeting by employing active and passive defense measures to disrupt the threat's targeting cycle. Army forces must integrate an inverse, reverse, or counter-targeting process to identify and mitigate operational vulnerabilities faster than threats can identify or target them during MDO. Risk management, protection assessment, and targeting enable the future force to target and deny enemy freedom of action in their deep areas, enabling friendly force access to the support areas and close area. This process enhances the future Army forces' approach to data and information flow leading to better application of C2 across multiple domains.

f. Deny enemy coordinated campaign. The enemy executes a coordinated campaign combining multiple capabilities to overmatch friendly forces. The future force will converge multi-domain capabilities and apply them to decisive spaces to overcome enemy advantages. This inverse action preserving CCAAs enables the force to penetrate, dis-integrate, and exploit. As a preemptive measure in MDO, and through the protection WfF, the future force will counter the enemy's ability to apply combined all domain stand-off capability against friendly forces to deny enemy freedom of action. From a commander's perspective (BCT, sustainment brigade, division, or corps), countering the enemy's coordinated campaign includes understanding vulnerabilities, what the intended enemy action against friendly forces is, and identifying mitigating strategies.

g. Deep sensing. To preserve the force, the future Army must be able to understand threats with a maximum amount of warning time and determine what denying action will work best, and if a denying activity is successful. Future forces will rely heavily on information from sensors operating across multiple domains and across all areas in the MDO framework, including the deep fires area, to stimulate, detect, see, and understand the enemy across the complex OE. Multi-domain sensors are capable of simultaneously sensing in more than one domain. Providing persistent, reinforcing, and complementary multi-domain sensors that are active, passive, manned, unmanned, and remotely operated can offset capacity issues within the force. Organic sensors in conjunction with cyberspace, space, air defense, field artillery, intelligence, joint, multinational, and commercially available sensors provide expanded situational awareness performing better protection missions in MDO.

h. Multi-domain obscuration. Army forces must possess the capabilities and capacity required to protect the force from targeting and attack in all domains and across the EMS and IE, to preserve operational security and to retain freedom of maneuver at the tactical and operational levels. Obscuration solutions must not be hazardous to personnel, equipment, or the environment to avoid limitations on employment for training or operations.

Chapter 4
Conclusion

The AC-P describes how the Army preserves the force from threats in all domains, generating stand-off which enables commanders to apply maximum combat power to accomplish the mission. It describes protection outcomes and requirements integrated across multiple proponents on an expanded battlefield and across the competition continuum as part of MDO. This concept contributes to experiments, studies, analyses, and continued development of the Army operating concept and the Army concept framework. The central idea of the AC-P is that Army forces, as part of JIIM teams, conduct protection activities in all domains, the EMS and IE, to preserve commanders' CCAAs, deny threat and enemy freedom of action, and enable access to achieve protected windows of superiority. The required capabilities to achieve this central idea enable modernization across DOTMLPF-P.

Appendix A
References

Army regulations, DA pamphlets, FMs, Army doctrine publications (ADP), and DA forms are available at https://armypubs.army.mil/. TRADOC publications and forms are available at http://www.tradoc.army.mil/publications.htm. Joint publications are available at http://www.dtic.mil

Section I
Required References

ADP 3-37
Protection, 31 JUL 19

TP 525-3-1
The U.S. Army in Multi-Domain Operations 2028, 6 DEC 18

TP 525-3-8
The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045, 21 DEC 18

Section II
Related References

ADP 3-0
Operations, 31 JUL 19

Army Expeditionary Forensics in 2028-2040 White Paper, 9 APR 19 (Available from Army Futures and Concepts Center by request)

AR 525-2
The Army Protection Program, 8 DEC 14

ATP 4-02.8
Force Health Protection, 9 MAR 16

DODD 3020.40
Mission Assurance, 20 NOV 16 (Change 1 Effective 11 SEP 18)

FM 3-0
Operations, 6 DEC 17

FM 3-11
Chemical, Biological, Radiological, and Nuclear Operations, 23 MAY 19

FM 3-13.4
Army Support to Military Deception, 26 FEB 19

FM 3-34
Engineer Operations, 2 APR 14

FM 3-39
Military Police Operations, 9 APR 19

FM 3-50
Army Personnel Recovery, 2 SEP 14

FM 3-63
Detainee Operations, 2 JAN 20

FM 4-02
Army Health System, 26 AUG 13

Joint Concept for Human Aspects of Military Operations, 19 OCT 16

Joint Concept for Integrated Campaigning, 16 MAR 18

Joint Concept for Robotic and Autonomous Systems, 19 OCT 16

Joint Operating Environment (JOE) 2035
The Joint Force in a Contested and Disordered World, 14 JUL 16

JP 3-0
Joint Operations, 17 JAN 17, Incorporating Change 1, 22 OCT 18

JP 3-10
Joint Security Operations in Theater, 25 JUL 19

JP 3-11
Operations in Chemical, Biological, Radiological, and Nuclear Environments, 29 OCT 18

JP 3-27
Homeland Defense, 10 APR 18

JP 3-31
Joint Land Operations, 3 OCT 19

JP 3-33
Joint Task Force Headquarters, 31 JAN 18

JP 3-34
Joint Engineer Operations, 6 JAN 16

JP 3-41
Chemical, Biological, Radiological, and Nuclear Response, 9 SEP 16

JP 3-42
Joint Explosive Ordnance Disposal, 9 SEP 16

JP 3-63
Detainee Operations, 13 NOV 14

Operationalizing Robotic and Autonomous Systems in Support of Multi-Domain Operations White Paper, 30 NOV 18 (retrieved from: http://arcic-sem.azurewebsites.us/App_Documents/UQ/RAS-In-Support-of-Multi-Domain-Operations-White-Paper_Signed_131500Dec18....pdf)

TP 525-92
The Operational Environment and the Changing Character of Warfare, 7 OCT 19

Appendix B
Required Capabilities

B-1. Introduction
The Army Concept for Protection required capabilities (RCs) are based on the broad ideas and required capabilities from the MDO and EAB concepts, proponent feedback and input, findings from related experimentation and supporting ideas found in chapter 3 of this pamphlet. Section B-3 lists protection dependencies on other functions and activities.

B-2. Protection warfighting function required capabilities

a. Preserve CCAAs.

(1) RC 1. Future Army forces require the capability to assess friendly vulnerabilities, determine protection requirements, prioritize CCAAs, and employ coordinating measures to preserve forces across the battlefield and competition continuum. (AC-P 3-4 a; AOC B-2 d; EABC B-2 b)

(2) RC 2. Future Army forces require the capability to train and prepare leaders on conducting the protection staff function to preserve the force and apply maximum combat power across the battlefield and competition continuum. (AC-P 3-4 a; AOC B-2 i; EABC 3-4)

(3) RC 3. Future Army forces require the capability to augment Soldier performance and capacity to increase situational awareness, lighten Soldier physical and cognitive workloads, facilitate movement, secure and protect CCAAs, and sustain the force with improved distribution across the battlefield and competition continuum. (AC-P 3-9; EABC 3-4 f (3))

(4) RC 4. Future Army forces require the capability to store and process large amounts of data from multiple sources, analyze, aid in decision making, reduce cognitive load of commanders and leaders, determine threat intent, develop friendly courses of action to preserve CCAAs, and maintain enhanced situational understanding across the battlefield and competition continuum. (AC-P 3-9; AOC 3-3; EABC B-2 h)

(5) RC 5. Future Army forces require the capability to conduct, synchronize, and analyze ISR activities to identify, characterize, and deny all domain threats, obstacles, and hazards across the battlefield and competition continuum. (AC-P 3-4 a (1); AOC B-2 d; EABC B-2b)

(6) RC 6. Future Army forces require the capability to C2 protection capabilities and plan, coordinate, integrate, synchronize, and converge protection effects in and across all domains, the EMS and the IE and throughout the competition continuum. (AC-P 3-4 a (1); AOC B-2 i; EABC 3-5e)

(7) RC 7. Future Army forces require the capability to protect the OE by building partner capacity and interoperability and by setting the theater through such activities as establishing basing and access rights, conducting preparatory intelligence activities, and mapping the EMS and computer networks in the operational support area in competition. (AC-P 3-4 a (1); AOC B-2 b; EABC 4-3 c., 4-4 a, 4-4 b)

(8) RC 8. Future Army forces require the capability to provide protection of installations, LOCs, the organic industrial base, depots, arsenals, munitions factories, and stockpiles through a synchronized Army and other government agencies whole of government approach to support readiness to deter, react, and project forces in response to pacing threat aggression. (AC-P 3-4 a (2); AOC B-2 e; EABC 3-4)

(9) RC 9. Future Army forces require the capability for a deployable and integrated air and missile defense to deny regional and trans-regional missile threats to preserve CCAAs across the MDO framework, including installations and key infrastructure within the strategic support area, in competition and armed conflict. (AC-P 3-4 a (2); AOC B-2 k; EABC 3-4)

(10) RC 10. The future Army requires installations to be resilient against disruption and attack with robust capabilities to prevent, protect, mitigate, respond to, and recover from all threats and hazards affecting mission readiness, sustainment, and force projection across the battlefield and throughout the competition continuum. (AC-P 3-4 a (2); AOC 4; EABC 3-4)

(11) RC 11. Future Army forces require the capability to process and disseminate large amounts of sustainment and movement data; be predictive; inform decision making; integrate with other Army information, information management, and battle management systems; and be protected and resilient; to enable power projection and distribution across the MDO framework. (AC-P 3-4 a (2); AOC 4; EABC 3-4)

(12) RC 12. Future Army forces require the capability to protect individual Soldiers, platforms, and equipment from enemy attack and against environmental hazards to preserve life,

enable freedom of action, and ensure resiliency in the force in MDO across the competition continuum. (AC-P 3-4 a (7); AOC 3-3 c; EABC 3-4)

(13) RC 13. Future Army forces require the capability to conduct FHP operations to preserve the force from health threats associated with MDO operations. (AC-P 3-5 f; AOC B-2 k; EABC 3-4)

(14) RC 14. Future Army forces require the capability to mitigate CBRN contamination using multiple, scalable means that reduce the hazard; reduce manpower, time and resources; and increase commanders' flexibility to support MDO. (AC-P 3-5 e; AOC B-2 k; EABC 3-4)

(15) RC 15. Future Army forces require the capability to conduct police operations to protect CCAAs, facilitate and preserve the rule of law, and deny irregular threats across the battlefield and competition continuum. (AC-P 3-5 b; AOC B-2 k; EABC 3-4)

(16) RC 16. Future Army forces require the capability to conduct detention operations to shelter, sustain, guard, protect, and document detainees while simultaneously supporting host nation and partner enemy prisoner of war operations across the battlefield and competition continuum. (AC-P 3-5 b; AOC B-2 k; EABC 3-4)

(17) RC17. Future Army forces require the capability to conduct police intelligence operations to synchronize information from multiple sources and to analyze and disseminate a clear understanding of criminal and security threats to commanders across the battlefield and competition continuum. (AC-P 3-5 b; AOC B-2 k; EABC 3-4)

(18) RC 18. Future Army forces require the capability to conduct battlefield forensics and biometrics activities to authenticate friendly forces and identify intelligence to target threat actors, explosives, CBRN hazards, and cyberspace-crimes across the battlefield and competition continuum. (AC-P 3-5 b; AOC B-2 k; EABC 3-4)

(19) RC 19. Future Army forces require the capability to conduct continuous survivability operations to preserve combat power in decisive spaces and to protect CCAAs across the battlefield and the competition continuum. (AC-P 3-5 g; AOC B-2 k; EABC 3-4)

(20) RC 20. Future Army forces require the capability to converge land, air, and maritime capabilities with operations in space, cyberspace, and the EMS to support the opening of and exploitation of windows of superiority; thereby protecting the ability to conduct friendly operations in degraded, disrupted, or denied operational environments across the battlefield and competition continuum. (AC-P 3-4 a (3); AOC B-2 j; EABC B-2 f)

b. Deny enemy freedom of action.

(1) RC 21. Future Army forces require the capability to characterize threats then plan and coordinate the denying activity with the appropriate element to preserve CCAAs and deny enemy freedom of action across the battlefield. (AC-P 3-4 b; AOC B-2 i; EABC 3-5 e)

(2) RC 22. Future Army forces require the capability to detect, identify, and characterize WMD and WME; prevent their employment; mitigate their consequences; and prevent catastrophic death and destruction across the battlefield and the competition continuum. (AC-P 3-4 b (1); EABC 2-2 b)

(3) RC 23. Future Army forces require the capability to detect, characterize, and deny irregular warfare to preserve CCAAs across the battlefield and competition continuum. (AC-P 3-4 b (2); EABC 4-3 h (1) (a))

(4) RC 24. Future Army forces require the capability to conduct countermobility, deny enemy freedom of action and restrict freedom of movement, and to enable friendly force freedom of maneuver across the battlefield to achieve a decisive tactical advantage. (AC-P 3-4 b (3); AOC 3-6 d (3); EABC 4-4 e (2))

(5) RC 25. Future Army forces require the capability to sense, target, and neutralize or destroy enemy aircraft, drones, missiles, rockets, artillery, and mortars both before and after launch; and to integrate with JIIM partner deny air and missile capabilities across the battlefield and competition continuum. (AC-P 3-4 b (4); AOC B-2 h; EABC 4-3 e (2))

(6) RC 26. Future Army forces require the capability to protect CCAAs against directed energy weapons (DEW) to include laser, microwave, sound, and particle beam lethal and nonlethal force threat systems across the battlefield and competition continuum. (AC-P 3-4 b (4); EABC 4-3 e (2))

(7) RC 27. Future Army forces require the capability to deny RAS, UAS, and drone swarms to reduce adversary speed, stand-off, communication, and decision making across the battlefield and competition continuum. (AC-P 3-4 b (5); AOC 2-3; EABC 2-1 a)

(8) RC 28. Future Army forces require the capability to deny or degrade adversary ISR capabilities in all domains to detect and understand friendly intent and actions to preserve CCAAs and enable freedom of action across the battlefield and throughout the competition continuum. (AC-P 3-4 b (6); AOC 3-5 d, B-2 h; EABC 4-3 c (2) (a))

(9) RC 29. Future Army forces require the capability to counter observation and sensing to preserve CCAAs across the battlefield and competition continuum. (AC-P 3-4 b (6); AOC 2-3 c (1); EABC 2-1 b)

(10) RC 30. Future Army forces require the capability to understand in depth the environment, enemy actions, and suspected actors through counterintelligence activities to preserve CCAAs, deny enemy actions, and enable freedom of action throughout the battlefield and competition continuum. (AC-P 3-4 b (6); AOC 3-5 d, B-2 h; EABC 4-3 c (2) (a))

(11) RC 31. Future Army forces require the capability to detect, characterize, and deny enemy coercion activities to preserve CCAAs across the battlefield and competition continuum. (AC-P 3-4 b (7); EABC 4-3 h (1) (a))

(12) RC 32. Future Army forces require the capability to detect and deny adversary all domain deception to preserve CCAAs across the battlefield and competition continuum. (AC-P 3-4 b (9); EABC 2-2 a (2))

(13) RC 33. Future Army forces require the capability to detect, characterize, mitigate effects, and deny enemy use of space, cyberspace, and the EMS that degrades and denies friendly operations across the battlefield and competition continuum. (AC-P 3-4 b (10); AOC 3-6 e; EABC 4-3 e)

(14) RC 34. Future Army forces require the capability to deny enemy information warfare to preserve friendly force access to the IE, control the threat narrative, influence domestic and foreign audiences and reduce impact on command nodes and the network across the battlefield and throughout the competition continuum. (AC-P 3-4 b (11); AOC B-2 h; EABC 4-3)

c. Enable access.

(1) RC 35. Future Army forces require the capability to detect and counter obstacles and hazards, enable freedom of movement, and preserve CCAAs across the battlefield resulting in a secure environment. (AC-P 3-4 c (2); AOC 3-6 d (3); EABC 3-4)

(2) RC 36. Future Army forces require the capability to establish and maintain protected movement (strategic, operational, and tactical), mobility (close and tactical support), and maneuver (deep maneuver and close) corridors in all domains to ensure persistent freedom of action across the battlefield and the competition continuum. (AC-P 3-4 c (3); AOC 3-7; EABC B-2 j)

(3) RC 37. Future Army forces require the capability to increase the accuracy, speed, and synchronization of protective lethal and nonlethal force effects across all domains to preserve CCAAs across the battlefield and competition continuum. (AC-P 3-4 c (4); AOC B-2 g; EABC 4-3 e (1))

(4) RC 38. Future Army forces require the capability to deny explosive hazards to enable sustainment, protect CCAAs, and maintain freedom of action across the battlefield and competition continuum. (AC-P 3-5 j; AOC B-2 k; EABC 3-4)

(5) RC 39. Future Army forces require the capability to establish and retain bases and support areas with integrated protection to preserve CCAAs across the battlefield and competition continuum. (AC-P 3-4 c (7); AOC B-2 b; EABC 3-4)

(6) RC 40. Future Army forces require the capability to employ CBRN R&S that informs commanders at all echelons via integrated early warning which provides real time understanding of CBRN threats and hazards by means of deployable platforms and novel sensors dispersed throughout the battlefield, creating predictability and enabling forces to respond in timely manner to reduce the impact of adversary attack. (AC-P 3-5 e; AOC B-2 k; EABC B-2 h, 3-4)

(7) RC 41. Future Army forces require the capability to conduct security and mobility support that protects and secures LOCs and movement corridors to enable operational and tactical

maneuver across the battlefield and competition continuum. (AC-P 3-5 b; AOC B-2 k; EABC 3-4)

(8) RC 42. Future Army forces require 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 is exploitable by the adversary and reduces freedom of action across the battlefield. (AC-P 3-4 c (6); AOC B-2 k; EABC 3-4)

(9) RC 43. Future Army forces require the capability to conduct civil reconnaissance of the operational environment to provide situational understanding to assist in decision making, set the conditions to interact with the local civilian population, identify critical threats, and leverage multinational capabilities to enhance operations that enable the future force to preserve CCAAs across the battlefield and competition continuum. (AC-P 3-5 d; AOC 3-3 b (1), 3-9 c; EABC 3-4)

(10) RC 44. Future Army forces require the capability to protect timely mobilization and deployment from strategic support areas to the JOA to deter escalation and defend against threat offensive operations across the battlefield and competition continuum. (AC-P 3-4 c (9); AOC 3-3 b; EABC B-2 g.)

Appendix C
Science and Technology

C-1. Introduction

a. This appendix recommends key science and technology capabilities that support the central idea and the three components of the solution enabling Army forces to conduct cross-domain protection activities in all domains, the EMS and IE, and to fulfill their roles in 2028 and beyond. Keys to successful all domain protection include extensive improvement in modeling adversary capabilities and strategies; cyber, information, communications network and physical security; assured PNT; cognitive hardening; detection and mitigation of explosive and CBRN hazards; sensors and sensor systems; RAS; survivability; signature management; and sustainability. Improvements in AI and ML will enhance the improvement of these capabilities.

b. Acquiring these capabilities requires targeted investment, extensive experimentation and constant reassessment within all the scientific fields that will contribute to the development of the needed technologies. With these capabilities, Army forces can conduct all domain protection throughout the battlefield, through activities across multiple domains, the EMS and the IE to create synergistic effects in the physical, temporal, virtual, and cognitive realms that preserve CCAAs, deny enemy freedom of action and enable access. To achieve this, the Army must work with the Army Modernization Enterprise (AME), academic experts, joint partners, industry leaders, and key stakeholders to develop the requisite capabilities.

c. This appendix cannot encompass all research within the AME. It will serve as a running estimate of relevant and disruptive scientific discoveries and emerging technologies the Army can

leverage to realize the required capabilities described in this concept. Science and technology stakeholders will review this appendix at least annually to account for evolving protection requirements, breakthrough technological innovations and breakthrough scientific discoveries.

C-2. Preserve CCAAs

a. New or improved materiel systems must enable leaders to better and more quickly visualize, understand and describe current and future actions; anticipate effects and functions across domains; act and react; and synchronize and execute ISR and C2 faster than adversaries.

(1) A robust MDCOP must incorporate sensors and their inputs from across the spectrum (CBRN, explosive hazard, ground, biometrics, electro-optical / infrared (EO/IR), synthetic aperture radar (SAR), radio detection and ranging (RADAR), light detection and ranging (LIDAR), hyperspectral imaging (HSI), multispectral imaging (MSI), other advanced sensors). It must also ingest inputs from DOD and National systems and vital data from the political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) operational variables; the areas, structures, capabilities, organization, people, events (ASCOPE) civil considerations and the diplomatic, informational, military, economic, financial, intelligence, and legal (DIMEFIL) instruments of national power.

(2) The MDCOP must also be able to incorporate inputs from appropriate civilian U.S. entities and be tailorable and as near real time as possible. Human and AI analyses should be continuous and complementary, use the latest input feeds, continuously incorporate advancements in cognitive engineering, and be reflected in the COP as appropriate. Analyses should include objective display of data, predictive analyses to project future states such as friendly and adversary strengths, dispositions, known and likely adversary actions in each domain, and recommendations for friendly action in each domain. Future leader development will include training in highly complex, multivariate and fast-moving scenarios utilizing chemical, biological and/or mechanical enhancements, and potentially new human-machine communications methods, to inform and improve decision making, cognitive speed and accuracy. The proliferation of sensors and increased data volume will require robust AI and ML technologies capable of rapidly processing data in or near real time, and potentially able to seamlessly self-optimize and self-reprogram to maximize analytical validity speed. Optimizing the human-machine interface and interaction will be vital in future operations.

b. The force will require technologies to increase the speed, precision, accuracy, resolution, and efficiency of ground, sea, low-altitude, high-altitude, and space-based sensors and their ability to peer through naturally-occurring and manmade impediments to sensing, to include through solid objects, and at reduced size, weight, and power (SWaP) than today's technologies. Technologies must be plug-and-play, nonproprietary, engineered for common connections, power supplies, software, communications network protocols, fast repair and other factors to minimize the integration and other burdens inherent in acquisition, operation, and sustainment. Sensors must be able to detect the full range of adversary equipment, actions, and effects, from DEW/EW to hypersonic kinetic to cyber to informational/cognitive, and from extended ranges. Whenever possible, sensors should be software-addressable, capable of being tailored to the output desired, and sensor packages should be capable of sensing different types of targets. Whenever possible,

sensors, particularly EO/IR sensors, should be paired with onboard lethal and nonlethal capabilities to provide timely surveillance and detection and to maximize engagement opportunities. Sensors must be capable of operating underground, in DUT, degraded visual environments, and all other conditions. Technologies should attempt to provide passive, wide-area, non-line-of-sight solutions that are augmented with appropriate AI/ML to reduce human-in-the-loop signature characterization. As discussed above, technologies should immediately feed a continuously analytic MDCOP while increasing capabilities in police and police intelligence, detention, forensics/biometrics, population and resource control, health protection, threat mitigation, and survivability operations.

c. Army forces will leverage optimized situational understanding (SA) and a continually-updated and integrated intelligent MDCOP to execute actions to preserve and protect troops, MDO formations and critical Homeland and deployed MDO capabilities and infrastructure. Army forces will utilize advanced technologies to protect troops and platforms, protect LOCs, industrial bases, depots, and other critical infrastructure across MDO, from the SSA / homeland through the deep maneuver area. Systems should tailor output to the user's ability to consume the information. When a human subject matter expert is not available, a technically and operationally applicable solution should be offered. Query responses should inform as to why the recommendation was made. Queries will be added to a query archive.

d. Army forces will converge the capabilities and technologies described above to perform all domain protection operations, simultaneously applying land, air, and sea capabilities from surface to space and in cyberspace, the IE, and the EMS, to decisively apply effects in the appropriate domains to achieve overmatch and defeat adversary activities. Tactical and National inputs and capabilities will be leveraged as appropriate to this end. Convergence will require a redundant, secure, resilient, and self-healing communications network connectivity capability, and will be significantly enhanced by robust edge computing and AI capability at the platform or unit level.

e. Adversary advances in science and technology and innovative methods of blocking, interfering with, spoofing, or hijacking our communications networks and sensors require friendly forces to be able to function in conditions in which sensors and communications networks are degraded or denied. Warfighters down to the individual platform and Soldier level must be able to move, shoot, communicate, and function at a high level without access to the communications network, without access to a shared COP or even access to data from sensors not carried on the Soldier or platform. Soldiers should be able to consume and process partial, limited, or restricted information as available. This will require doctrine and training to include these conditions, as well as materiel solutions which can function in isolation.

C-3. Deny threat and enemy freedom of action

a. Army forces in competition and conflict require the capability to decisively deny adversaries the freedom to act and maneuver in any domain and also require the capability to detect, deny, degrade, disrupt, deceive, counter and even control adversary ISR in all domains. These capabilities require a wide suite of capabilities which must work independently and in concert with each other. Army forces must have automatic and human-in-the-loop proactive and reactive capabilities, able to passively or actively detect adversary ISR and any activity in the physical,

virtual, and cognitive domains, then react quickly and comprehensively, using the appropriate suite of tools and along the appropriate PMESII-PT, ASCOPE, and DIMEFIL lines. Denial of enemy action will include protection from actions directed toward American civilians and assets in the homeland as well as toward the deployed force, as a "whole of government" effort. Denying adversary capability in the IE will require a training program which could also be used by civilians, and also technologies to screen out, block, or warn about false information promulgated by adversaries.

b. Denying adversary activity will require physical, virtual, and cognitive capabilities to leverage friendly sensor inputs and analyses of adversary plans and actions, then execute appropriate responses. Forces will deny, degrade, and block enemy activity in the fastest and most appropriate means, then if necessary take action to destroy enemy capabilities and deter future action, such as electronically blocking a cyberspace attack then using physical action to destroy the source, then broadcasting news of the attack to military and civilian populations in the cognitive space. Being able to discriminate friendly, adversary, and neutral air, ground, subsurface, and virtual/cyber assets and activities, then potentially autonomously targeting and neutralizing only adversary assets and capabilities, will be a critical requirement. Capabilities must be able to engage and apply effects at tactically and operationally required speeds and distances.

c. The force will require technologies and tactics to detect, deny, and counter the enemy ability to apply IW and UW in the cognitive domain, and to conduct IW and UW on its own, potentially using energetic or biochemical solutions to directly affect or slow cognition to achieve tactical to strategic effects. This is closely linked to the need to be able to detect and deny enemy deception while implementing our own deception. This may be achieved through physical, chemical, biological, cognitive, cyber, or other means.

d. The automated and electronic battlefield of the future means Army forces must control the space and cyber domains and the electromagnetic spectrum while denying them to the enemy. The proliferation of automated and controlled RAS, informed or controlled by AIs, will increase the speed of adversary ISR, combat, and other systems and will require a more proactive approach, including tactical denying of and protection from these systems and also from DEW, WME, and WMD. Systems may need to function on a continuous basis to "shield" from or inhibit adversary capabilities, or may need to remain passive and in a "ready" status until activated, then act in milliseconds. Friendly RAS, from very small to very large size platforms and acting independently or in groups or swarms, will deny adversary RAS at higher speeds and volumes than humans can achieve. Technologies must be plug-and-play, nonproprietary, engineered for common connections, power supplies, software, communications network protocols, and other factors to minimize integration and the burdens inherent in operation and sustainment. A hybrid approach to RAS engagements will include cheap and disposable RAS in volume combined with non-disposable and also intelligent RAS, applied for different tactical to strategic effects.

e. To achieve higher levels of convergence in the hyper-automated, hyper-electronic OE, forces will require a redundant, secure, resilient, and self-healing communications network connectivity capability, and will be significantly enhanced by robust edge computing and AI capability at the platform or unit level. Forces must be prepared to operate and achieve convergence in highly to fully-denied communications conditions, in which RAS and other assets must act without network

connectivity. Therefore RAS and other assets should be able to switch from a "communications network-reliant" mode to an "independent" mode, able to be quickly programmed for missions based on verbal commands, preprogrammed instructions, or command packages.

C-4. Enable access

a. Army forces in competition and conflict require the capability to quickly build partner capability, set the theater, enable force projection, leverage military and civilian resources to mobilize and deploy from the SSA to the JOA, and set the theater. Having integrated protection, future Army forces will establish and retain bases within support areas as well as secure movement and maneuver corridors. Future Army forces will also preserve CCAAs and LOCs by reducing, neutralizing, bypassing, or destroying adversary obstacles and hazards through security and mobility support operations.

b. The force will require the capability to leverage a homeland-to-theater MDCOP and apply resources to enable access to resources and assets during movement and after arrival in theater. The MDCOP must be able to ingest large amounts of data from military and civilian sources throughout this process, requiring sensors and nonmilitary data sources to provide a continuous flow of data. Forward-deployed RAS operating autonomously, under remote human control or onsite under human or AI control, will perform difficult and dangerous tasks, such as preparing aerial ports of debarkation and sea ports of debarkation, LOC, conducting small and large-scale obstacle breaching and gap crossing operations, construction of forward arming and refueling points, ammunition supply points, intermediate staging bases, and other key infrastructure and resources.

c. The MDCOP will also begin producing fuels, lubricants, and power using locally sourced materials and advanced solar, small scale nuclear, and biological technology. They will emplace offensive and defensive capabilities and begin conducting initial protection activities and setting initial protection conditions before manned formations arrive. Advanced air and ground RAS will scout the theater for explosive, CBRN, and other hazards and inform the MDCOP, which will present continually updated status and recommendations to human decision makers. Where appropriate, RAS will neutralize hazards and either secure the area or begin the exploitation process, identifying safe and unsafe areas.

d. Once manned forces arrive, combinations of manned and unmanned assets will continue to expand the footprint, providing cross-domain protection wherever manned formations operate.

C-5. Desired technical and scientific advancements to support required capabilities

a. Breakthrough technological innovations.

(1) Enhanced sensing, SA, human-machine interface, AI, and RAS.

(a) Development of a rapid "big-data" collection and processing capability, in the form of an MDCOP with a highly enhanced capability to simultaneously ingest, process, and display thousands or more separate inputs and analytics across PMESII-PT, ASCOPE, and DIMEFIL. A

highly robust MDCOP will leverage AI, ML, and human commands to increase SA, reduce decision-making times, enable better tactical and operational decision making, and increase mission success, while reducing casualties. (RCs 1, 3, 4, 5, 7, 15, 17, 30)

(b) Development of self-optimizing and self-programming AI, capable of enhanced ML and data mining. Rapid ingestion and analysis of rapidly changing data through continually updated algorithms will enable continual updates to SA and the MDCOP, enabling informed decision making and adaptation to adversary actions and other conditions. (RCs 1, 3, 4)

(c) Development of systems for context-aware information filtering integrated with advanced visualization technology, where high-performance computing infrastructure is leveraged to analyze data streams at multiple levels of context, prioritize, and visualize the analyzed data in a variety of mediums, and will enable rapid decisions through the production of actionable information. This advancement will enable the integration and consumption of large quantities of data, spanning multiple data types, and enable graphic display, while reducing cognitive overload. (RCs 1, 3, 4, 5, 26, 27, 29, 31, 32, 33, 37, 38, 40, 41).

(d) Development of models or processes and AI/ML that automate terrain reasoning and evaluation. Capability will increase SA, increase decision-making speed and accuracy, and contribute to persistent access across all environments. (RCs 20, 24, 35, 36)

(e) Development of broadly multifunctional sensors, capable of operating underground, in DUT and all other conditions, with little to no degradation in performance, and without significant human manipulation or control. Sensors leveraging EO/IR, sonic, seismic, electromagnetic, and other detection options will increase the fidelity of the MDCOP and further increase Soldier and platform SA and protection of personnel, facilities, and materiel. (RCs 1, 3, 4, 11, 17, 18, 25, 26, 27, 35, 41)

(f) Development of enhanced signature recognition of multiple hazards at distance and through enemy cover, concealment, and deception. The ability to recognize the signatures of hypersonic objects, DEW sources, buried and other hazards, through natural and artificial obscurants and through solid objects, will enable faster and more robust SA and decision making and increased protection of personnel, structures, and materiel. (RCs 1, 3, 4, 11, 17, 19, 22, 23, 24, 26, 27, 28, 29, 31, 38, 39, 41, 42, 43, 44).

(g) Development of technologies for detection of adversary ISR activity in all domains and environments, including location and type of enemy system. Rapid location and identification of enemy systems, potentially using disposable systems, will enable rapid and robust protection of friendly systems and engagement of enemy systems with appropriate deception, interdiction, or attack effects. (RCs 1, 3, 4, 5, 17, 19, 23, 26, 27, 28, 29, 31, 39, 40, 41, 44)

(h) Development of rapid cross-domain effect recognition, enabling detection and identification of adversary equipment actions and effects, from physical object to cyber to informational / cognitive. Detection of effects, even if the action of platforms or munitions is undetected, will enable friendly forces to protect from or interdict the effect and attack its source. (RCs 1, 3, 4, 5, 17, 19, 23, 26, 27, 28, 29, 31, 38, 40, 41, 42, 43, 44)

(i) Development of technologies for rapid, precise, and dependable remote sensing of chemical, biological and nuclear contamination, using active, passive, and hybrid technological approaches. Rapid detection of these hazards will enable increased Soldier protection and survivability through faster physical and medical responses, population of tactical or medical COP(s) and AI(s) for response and analysis, and enable increased Soldier protection and survivability. (RCs 1, 3, 4, 8, 12, 15, 16, 17, 35, 36, 40, 41)

(j) Development of a distributed sensing system, including sensors and models for cooperative active and passive sensing. Distributed and networked sensors will provide for enhanced SA, a highly informed MDCOP, reduce decision-making times, enable better tactical and operational decision making, and increase mission success while reducing casualties. (RCs 1, 3, 4, 11, 17, 22, 32, 32, 33, 35, 41)

(k) Development of improved technologies for enemy directed energy source position determination, including location and type of enemy systems. Rapid location and identification of enemy systems will enable rapid and robust protection of friendly systems and engagement of enemy systems with appropriate deception, interdiction, or attack effects. (RCs 1, 3, 4, 26)

(l) Development of technologies to leverage sensitive radio frequencies (RF) for detection of adversary receivers, particularly passive RF detection systems. Rapid location and identification of enemy systems, potentially using disposable systems, will enable rapid and robust protection of friendly systems and engagement of enemy systems with appropriate deception, interdiction, or attack effects. (RCs 1, 3, 4)

(m) Development of expert propagation model system with access to tactical high-resolution geospatial data and forecasted weather to assess and visualize predicted command post, platform, or personal device signatures for EO (line of sight), RF, acoustic, seismic, infrasound, IR, and LIDAR systems. System monitors self-signature and maintains SA of self-emissions continually updated with weather and local terrain including urban terrain. Continuous signature planning and management will enable increased protection through decreased enemy ability to engage friendly resources and assets. (RCs 1, 3, 4, 6)

(n) Development of paired sensor-shooter/effect tandems. Sensors paired with onboard lethal/nonlethal capabilities will minimize or eliminate the kill chain when executing an effects mission, thus increasing the accuracy and precision of detection and engagement. (RCs 1, 4)

(o) Development of synthetic biologicals for use in forensics, biometrics and police/police intelligence operations including the detection of species, individuals, novel tagging, and manufacture signatures. The ability to engineer customized taggants and other technologies will increase the flexibility, accuracy, and precision of these operations, enabling increased protection of friendly forces. (RCs 15, 16, 22)

(p) Development of enhanced human identification capabilities to enable recognition at greater stand-off distances, including facial detection and recognition in low light settings, through vehicle windows and at various pose angles, gait/anthropometrics and voice. Recognition of

friends/foes at increased distances increases protection of friendly forces through reduction of fratricide and increase in the volume and speed of detection of enemy forces. (RCs 15, 16, 19, 21)

(q) Development of enhanced inorganic and synthetic biologicals for improved and less costly sensors to detect chemical and biological hazards and changes in human performance and condition. Rapid detection of these hazards and changes will enable increased Soldier protection and survivability through faster physical and medical responses and provide a means to record individual exposures to manage individual cumulative risk. (RCs 1, 3, 4, 13, 15, 17, 22, 41)

(r) Development of invasive and noninvasive sensors to detect biomarkers predictive and indicative of exposure to hazardous chemicals, biological and radiological hazards and pharmaceutical based agents, excessive heat or other stress, immune response, and other critical factors. The capability to rapidly detect these changes will feed tactical or medical COP(s) and AI(s) for response and analysis, enable the projection of the point of medical surveillance forward to a field location by sequencing sampled fluids and or residue without the need for a field laboratory, and enable increased Soldier protection and survivability through faster physical and medical responses. (RCs 3, 8, 12, 13, 15, 17, 28)

(s) Development of multiple mode settings and improved human-machine interfaces for RAS. Includes development of an alternative geospatial navigation solution based on 3D visual terrain referencing and navigation and frequency-modulated LIDAR or other technologies to derive solutions as input to global positioning system (GPS)-denied ground RAS systems, providing accurate estimates for local navigation. RAS which can operate in "intelligent" and/or communications network-linked mode or in network-denied mode using preprogrammed specific or intent guidance and onboard navigation will enable missions to continue without continuous human control. (RCs 1, 2, 3, 6, 18, 23, 24, 31, 33, 36, 38, 41, 42, 43)

(t) Development of a multi-scale, multi-temporal, multi-terrain geospatial data collection, processing and dissemination capability to build a 2D and 3D standard and sharable geospatial foundation encyclopedia. A flexible system designed to ingest raw 2D imagery as well as aerial / terrestrial 3D point clouds producing spatial-temporal analysis of recent archived data to support commander's critical information requirements (CCIR), predictive friendly force and threat force courses of action development, and advanced IPB. Capability will increase SA, increase decision-making speed and accuracy, and contribute to persistent access across all environments. (RCs 1, 3, 4, 5, 7, 13, 26, 35, 41)

(u) Development of large area, long stand-off airborne collection of quick turnaround 3D terrain and urban infrastructure providing high-resolution foundation data supporting analysis and visualization of threat courses of action, obstacles and environmental hazards, and enabling prediction of threat actions and vulnerabilities, critical to protection planning and prioritization. Capability will increase SA, increase decision-making speed and accuracy, and contribute to persistent access across all environments. (RCs 1, 3, 4, 11, 17, 26, 35, 41)

(v) Development of photonic integrated chip components with advanced capability for waveguide-enhanced Raman spectroscopy, while leveraging recent advancements in compact Raman spectrometer design, will enable the detection of chemical and biological threats in the

vapor phase. This advancement will lead to the realization of a fast, high-fidelity, sensitive and low-SWAP chemical detector that will enable real-time understanding of CBRN threats and hazards enabling forces to effectively respond and minimize the effects of an incident. (RCs 5, 8, 10, 17, 22)

(w) Development of technologies to identify, enhance, and reduce the psychological effectiveness of language, tone, images, sounds, and chemicals. The capability to identify likely adversary deception/IW/UW activities and optimal methods to deny them will enable increased protection of U.S. military and Homeland civilian populations and vulnerable non-U.S. populations. (RCs 1, 2, 3, 4, 27, 29, 31, 36, 37)

(x) Development of smart military and civilian communications networks, facilities, and infrastructure able to detect and block adversary activity, warn friendly forces of intrusion and attack, and also attack intruders, in the cyber and physical domains. This technology, leveraged through a common user interface, will enable improved SA and increase the protection of personnel, materiel, structures, and both physical and cyber infrastructure. (RCs 1, 4, 6, 7, 8, 9, 10, 13, 14, 23, 27, 29, 31, 33, 36, 39, 41)

(y) Development of an adaptive tasking capability that coordinates efforts across autonomous and manned platforms, utilizing converged sensor data to provide tasking or targeting information to each platform or operator enabling efficient and effective use of resources to complete required tasks. Capabilities will enable rapid and efficient employment of sensors and platforms and increase mission speed. (RCs 1, 4, 6, 27, 31, 41, 42, 43)

(z) Development of a semi-autonomous or fully autonomous capability to construct basic structures and obstacles. Capabilities will enable faster mission accomplishment and enable personnel to perform other vital tasks, potentially out of the range of enemy weapons systems, increasing Soldier protection and survivability. (RCs 35, 41, 42, 43)

(aa) Development of a semi-autonomous or fully autonomous capability to clear obstacles and obstructions from avenues of approach. Capabilities will enable faster mission accomplishment and enable personnel to perform other vital tasks, potentially out of the range of enemy weapons systems, increasing Soldier protection and survivability. (RCs 23, 27, 30, 35, 36, 41, 42, 43, 44)

(ab) Development of remote and independent RAS to perform dangerous tasks under dangerous conditions in potentially contaminated areas. Automating these tasks will increase the speed of operations and protect personnel, structures, and materiel. (RCs 18, 22, 23, 24, 33, 35, 41, 42, 43)

(ac) Development of sensors and equipment on manned and RAS platforms to rapidly, accurately, and precisely detect and neutralize CBRN, explosive and nonexplosive hazards and/or obstacles remotely and ahead of forces. Automating these tasks will increase the speed and tempo of operations and protect personnel, structures, and materiel. (RCs 18, 22, 23, 24, 25, 27, 28, 30, 35, 41, 42, 43)

(2) Obscuration, camouflage, cover, concealment, and deception.

(a) Development of synthetic biologicals for obscurative coatings and concealments, for broad or narrow-spectrum applications. Customized biologicals will enable tailorable and scalable applications, improving protection of troops and materiel. (RCs 19, 28, 29)

(b) Development of advanced multispectral camouflage, effective across the EMS. Advanced camouflage will enable tailorable and scalable applications, potentially tunable as well, which will improve protection of troops and materiel. (RCs 19, 28, 29)

(c) Development of multispectral and tailored obscurants, effective in the visible and other EMS domains. Advanced obscurants will enable tailorable and scalable applications, potentially tunable as well, which will improve protection of troops and materiel. (RCs 19, 28, 29)

(d) Development of bispectral obscuration for artillery and mortar delivery, nominally in the form of microparticles and nanoparticles. Advanced and tailored obscuration engineered for projection and remote delivery will enable tailorable and scalable applications, potentially tunable as well, which will improve protection of troops and materiel. (RCs 19, 28, 29)

(e) Development of highly conductive, anisotropic new materials within the microparticle and nanoparticle dimensions which are packable and dispersible, for highly effective obscurants from the ultraviolet through microwave portions of the EMS. Multispectral and bispectral obscurants will increase protection across a larger portion of the EMS for high-value assets against advancing threat sensor technology, and enable concealment during breaching operations. (RCs 19, 28, 29)

(f) Development of new obscurant materials that are survivable in very high G forces, while still able to disseminate efficiently into individual particles will enable the development of a leading obscurant round that produces a cloud which conceals the flight of following lethal munitions from radar. Such tailored obscurant rounds will delay enemy forces' ability to react and deny their ability to target and intercept munitions in flight. (RCs 19, 28, 29)

(g) Development of cyberspace and electromagnetic activities for camouflage, including RF and cyber decoys. These capabilities will degrade enemy SA and lead to uniformed enemy decision making while enabling increased protection of friendly troops and materiel. (RCs 1, 5, 19, 28, 29)

(h) Development of radio frequency physical decoys (RF spectrum replication). These capabilities, tailorable and programmable according to the tactical situation, will degrade enemy SA and lead to uniformed enemy decision making while enabling increased protection of friendly troops and materiel. (RCs 1, 5, 23, 28, 29)

(i) Development of rapidly deployable multispectral physical decoys (EMS decoys). These capabilities, tailorable and programmable according to the tactical situation, will degrade enemy SA and lead to uniformed enemy decision making while enabling increased protection of friendly troops and materiel. (RCs 1, 5, 23, 28, 29)

(j) Development of technologies for techniques or materials to conceal EMS signatures. These capabilities, tailorable and programmable according to the tactical situation, will degrade enemy SA and lead to uniformed enemy decision making while enabling increased protection of friendly troops and materiel. (RCs 1, 5, 23, 28, 29)

(k) Development of reconfigurable wideband antennas, transceivers, digital signal processors, and intelligent algorithms applied to the electromagnetic environment and network/cyberspace domains, which autonomously create a complex and chaotic battlefield environment and allow commanders to manage the adversary's common operating picture. This advancement will enable commanders to seize, retain, and exploit the initiative by delaying the adversary's decision-making process and response time through increased chaos and uncertainty of friendly forces' position and activity on the battlefield. (RCs 1, 5, 23, 28, 29)

(3) Physical and communications network/cyber protection.

(a) Development of improved active protection systems for tactical vehicles, and the ability to install the capability into semi-permanent structures. Capabilities which span the spectrum from electronic to physical responses, including nonlethal and lethal, counter-UAS, protection swarms, DEW, and other methods which account for the full range of known enemy capabilities, will enable increased protection of friendly troops and materiel. (RCs 5, 8, 9, 10, 12, 14, 23, 41)

(b) Development of adaptive active armor technologies to expand the range of protection with active steering countermeasures for ground combat vehicles. These advancements will enable the interception of threats even in vulnerable locations such as in front of sensors, damaged areas, or otherwise lightly protected surfaces. (RCs 5, 12, 23, 35, 41)

(c) Development of wearable and/or portable passive and active protection systems to protect individuals and small teams even when dismounted and away from ground platforms. Capabilities which span the spectrum from electronic to physical responses, including nonlethal and lethal, counter-UAS, protection swarms, DEW, and other methods which account for the full range of known enemy capabilities, will enable increased protection of friendly troops and materiel. (RCs 5, 12, 23)

(d) Development of materials, mechanisms, and construction or emplacement methodology to provide lighter weight protection from evolving ballistic, blast, and directed energy threats. Development of advanced natural and engineered materials and energetics will reduce logistical requirements and enable increased protection of friendly troops, structures, and materiel. (RCs 5, 8, 9, 10, 12, 23)

(e) Development of optimized sensing of threat lasers and optics will enable the development of a low SWaP directed energy counter-measure which neutralizes missile guidance systems. This soft kill capability will disrupt missile trajectories at stand-off, enabling increased protection of friendly troops, material and structures. (RCs 5, 8, 10, 23, 41, 42, 43, 44)

(f) Development of algorithms for cooperative teaming, multi-agent assignment, and vision-based navigation and object pose estimation will enable the autonomous protection of ground combat vehicles using unmanned aerial systems. This advancement will enable sacrificial threat intercept by friendly unmanned vehicles, thus enabling increased protection of friendly troops, materiel and structures. (RCs 3, 5, 23, 26, 27, 41)

(g) Development of advanced screening, reflective, absorptive, transformative, or other materials to deny DEW. This technology will enable improved SA and increase the protection of personnel, materiel, structures, and both physical and cyber infrastructure. (RCs 1, 8, 10, 23, 26)

(h) Development of synthetic biologicals for rapid vaccine and medicine development. The capabilities for tailored production upon need and broad-spectrum immune response and other enhancers as both prophylactic and response measures will enable increased protection of friendly troops and potentially American civilians from intentionally or unintentionally released hazards. (RCs 12, 13)

(i) Development of technologies for application of AI for global surveillance of indicators of communicable disease outbreaks or adversary activities indicating potential intentional CBRN activities, fed by open-source reporting, materiel and technology acquisitions and information, along with government-collected intelligence information. This technology will enable early situation awareness of use or spread of these hazards, enable rapid prophylactic and response measures, and enable increased protection of friendly troops and potentially American civilians from intentionally or unintentionally released hazards. (RCs 1, 4, 5, 8)

(j) Development of technology to rapidly decontaminate CBRN-contaminated equipment in all climate and weather conditions with massively reduced or eliminated requirement for water. Development of increasingly frictionless or contaminant-resistant surfaces, tailored slurries, biologicals, or other capabilities, which reduce or eliminate the need for water in the decon process, will enable increased protection of friendly troops and materiel. (RCs 5, 7, 8, 10, 12, 14, 22)

(k) Development of wide-area and large-scale semiautonomous or autonomous decontamination technology to support terrain and wide-area / large-scale decontamination operations such as the equipment in a motor park and the motor park itself. This capability will enable friendly forces to rapidly continue operations following a contamination event. (RCs 5, 7, 8, 10, 12, 14, 22)

(l) Development of multifunctional materials that provide capabilities in the areas of physical protection, sensing, adsorption, and decontamination of chemical hazards. Provision of catalysts and membranes/textiles will significantly enhance protection of the wearer through decomposition of adsorbed chemical agents. (RCs 5, 8, 10, 12, 14, 22)

(m) Development of technology for the use and recycling of indigenous, used, or other available materials into source materials for power and construction of facilities and protective structures. The use of these rapid processing techniques for compaction, melting, combustion, 3D printing, and other applications will significantly reduce logistical burdens and increase the speed of construction. (RCs 8, 43)

(n) Development of hardware and protocols for alternative communication modalities for both low probability of detection and classification will allow for secure, and resilient communications at all echelons. This advancement enhances information protection by concealing the transmission of critical information across all echelons and domains thereby enabling friendly forces to achieve operational and strategic objectives. (RCs 1, 6, 7, 10)

(o) Development of AI-driven broad-spectrum screening of personnel to achieve faster and more accurate medical readiness assessments. Reduction in post-mobilization medical requirements will increase personnel and force readiness and availability and reduce cost. (RCs 8, 13)

(p) Development of synthetic biologicals for improved human performance. Improvements in cognition, endurance, strength, resistance to disease vectors, and other performance measures will increase personnel effectiveness and readiness. (RC 3)

(4) Cognitive protection.

(a) Development of technology for electronic detection of and response to adversary information warfare (IWar) activities in military and civilian communications and media such as "deep fakes" and other effects. The ability to detect and apply cyber and/or physical effects as a form of "reactive armor" will provide accurate SA, improve decision making and protect military and civilian populations from adversary activities. (RCs 2, 3, 5, 23, 31, 32, 34, 43)

(b) Development of training protocols for instilling critical thinking and resiliency in military forces, which could also be used by the general population, to enable cognitive protection against adversary IWar. Military individual, institutional, and unit training, and supporting civilian training, with both including training in identification of and response to likely mis and/or disinformation, will provide both with accurate SA, improve decision making, and protect military and civilian populations from adversary activities. (RCs 2, 3, 23, 31, 32, 34, 43)

(c) Development, in conjunction with and in support of the Whole Of Government, a national standard for assessing and displaying information validity, similar to what is currently done with nutrition labels on food and indicators of web site trustworthiness. This capability, as a continuous and ubiquitous national and informational security measure, will provide accurate SA, improve decision making, and protect military and civilian populations from adversary activities. (RCs 2, 23, 31, 34)

(5) Enhanced materiel, modularity, interoperability, and repurposing.

(a) Development of massively interchangeable and integrated hardware and software which has plug-and-play capability, is nonproprietary, and is engineered for common connections, power supplies, communications network protocols, and other factors. This will reduce the integration and other burdens inherent in operations and sustainment and will reduce the logistical burden. (RCs 3, 4, 44)

(b) Development of customizable shipping and packing containers and materials, designed for multiple uses and able to be shipped and carried on multiple platforms, enabling receiving or other unit to use, reuse, or recycle all components, including as construction material or bulk source material for local 3D printing of supplies and equipment. This will reduce the logistical burden, reduce waste, increase operational readiness rates and increase speed of construction. (RCs 3, 4, 44)

(c) Development of technologies for autonomous or automated construction methods that enable access and remove operators from the point of application. Capability will provide increased speed of construction and protection of personnel. (RCs 8, 12, 42, 44)

(d) Development of technologies for rapidly assessing damage with remote means, and repairing critical infrastructure (ports, airfields, supply depots, roads) that preserve access to strategic and operational CCAAs. Capability will provide increased speed of construction and protection of personnel. (RCs 11, 42, 43, 44)

(e) Development of technologies for rapidly repairing damage to vehicles and equipment, restoring structural integrity and functionality, such as the application of heat or light to epoxy welds or joins. Capability will provide increased functionality, mission effectiveness, and protection of personnel and critical systems. (RCs 8, 10, 44).

(f) Development of networked, smart munitions capable of sensing and sending data and information through and to the communications network and to other munitions, including lethal and nonlethal applications, for terrain shaping or other denial operations. Capability will increase SA on area denial operations and of enemy activity and increase accuracy, precision, lethality, and proportionality of engagements. (RCs 4, 5, 24)

(g) Development of advanced explosives for use in munitions and terrain shaping applications. Capability will increase lethality, impact enemy movement and maneuver, and reduce friendly logistical burden. (RCs 19, 24)

(h) Development of advanced non-explosive obstacles for use in terrain shaping applications. Capability will impact enemy movement and maneuver and reduce friendly logistical burden. (RCs 19, 24)

(i) Development of advanced materials, optimized packaging, and reduction in size and weight. Reducing the weight and optimizing the form factors of equipment, vehicles, and supplies will reduce the transportation and logistical burden, cost, and waste. (RCs 3, 44)

(j) Development of synthetic biologicals to be used in self-healing concrete. The use of tailored or engineered organisms in concrete mixes will increase the durability and life of emplaced concrete, reducing the cost and logistical burden and increasing the usable lifespan of constructed structures and facilities. (RCs 8, 10, 19, 42, 44)

(k) Development of automated remote 3D printer/manufacturing equipment for remote/onsite fabrication of repair parts, tools, and other materiel. This will reduce the transportation and logistical burden, reduce waste, and increase operational readiness rates. (RCs 3, 44)

(l) Development of sprayable synthetic biologicals for roads and runways. The use of novel materials for dust abatement and soil stabilization will increase the durability and life of constructed facilities; reduce wear in air and ground platform rotors, engines, and machinery; reduce health and safety risk from degraded visual environments; and reduce cost and logistical burden. (RCs 3, 42, 44)

(m) Development of sprayable synthetic biologicals for armor and building materials. The use of novel materials to harden structures and building materials will increase structure and material durability and life, reducing the cost and logistical burden and increasing the usable lifespan of constructed structures and facilities; increasing protection for personnel, material and facilities; and reducing the transportation and logistical burden and reducing cost. (RCs 3, 8, 10, 42, 44)

(n) Development of synthetic biologicals for improved waste stream management. The reduction in or repurposing of waste will reduce cost and the logistical burden. (RCs 3, 44)

(o) Development of synthetic biologicals for improved fuels and energetics. Scalable production of enhanced products without traditional chemistry and resource limitations will reduce cost and the logistical burden and enable missions of longer range and duration. (RCs 3, 42, 43, 44)

(p) Development of synthetic biologicals for small scale power. The use of low power but longer-lived power sources, potentially renewable through "recharging" with organic matter vs electric methods, will reduce cost and the logistical burden and enable missions of longer range and duration. (RCs 3, 42, 43, 44)

(q) Development of synthetic biologicals for continuous fuel production. The onsite or onboard production of fuel will reduce cost and the logistical burden and enable missions of longer range and duration. (RCs 3, 42, 43, 44)

(r) Development of technology for autonomous or automated construction methods that enable access and remove operators from the point of application. Capability will provide increased speed of construction and protection of personnel. (RCs 3, 12, 19, 42, 44)

(s) Development of technology for rapidly assessing damage with remote, autonomous or automated means, and repairing critical infrastructure (ports, airfields, supply depots, roads) that preserve access to strategic and operational CCAAs. Capability will provide increased speed of construction and protection of personnel. (RCs 41, 42, 43, 44)

b. Breakthrough scientific discoveries.

(1) Enhanced sensing, SA, human-machine interface, AI, and RAS.

(a) Research into enhanced “big-data” collection and processing capability, including improved data input and processing capacity, human-machine interface, algorithms, and AI ability to self-reprogram and self-optimize for continuous effectiveness and speed. Mutually supporting discoveries in these areas will enable significantly faster and more robust SA and human-AI-RAS interaction, fully autonomous RAS, and faster and more informed decision making. (RCs 1, 3, 4, 5, 7, 15, 17)

(b) Research into advanced EO/IR, SAR, RADAR, LIDAR, HSI, MSI, ground, seismic, sound, algorithmic/IW, and other sensors for detection of adversary ISR activity in all domains and environments. Capabilities will enable rapid and robust SA, decision making, and engagement of enemy systems with appropriate deception, interdiction, or attack effects. (RCs 3, 4, 5, 17, 21, 23, 31, 40, 43)

(c) Research into the use of entangled photons in quantum imaging/quantum illumination will improve resolution, provide the possibility of imaging through obscurants, enable "seeing" in a different frequency domain than probe lights, and enable stealth by using a different photon to image than is used to illuminate the source. This advancement will enable “seeing” more and "seeing" better in degraded visual environments, the ability to understand and act faster than adversaries, potentially without being seen in the process. (RCs 1, 3, 4, 21, 25, 27, 30, 32)

(d) Research into enhanced signature recognition of multiple hazards at distance and through enemy cover, concealment, and deception. The ability to recognize the signatures of hypersonic objects, DEW sources, buried and other hazards, through natural and artificial obscurants and through solid objects, will enable faster and more robust SA and decision making and increased protection of personnel, structures, and materiel. (RCs 1, 3, 4, 11, 17, 19, 22, 23, 24, 26, 27, 28, 29, 31, 38, 39, 41, 42, 43, 44)

(e) Research into enhanced cross-domain effect recognition via sensors able to detect adversary equipment actions and effects, from physical object to cyber to informational / cognitive. Capability will enable faster and improved SA and decision making, and increased protection of personnel, structures, and materiel. (RCs 1, 3, 4, 5, 17, 19, 23, 26, 27, 28, 29, 31, 38, 40, 41, 42, 43, 44)

(f) Research into enhanced inorganic and synthetic biologicals for improved and less costly sensors to detect chemical and biological hazards and changes in human performance / condition. Rapid detection of these hazards and changes will enable increased Soldier protection and survivability through faster physical and medical responses and provide a means to record individual exposures to manage individual cumulative risk. (RCs 1, 3, 4, 13, 15, 17, 22, 41)

(g) Research into enhanced invasive and noninvasive sensors to detect biomarkers predictive and indicative of exposure to hazardous chemicals, biological and radiological hazards, pharmaceutical-based agents, excessive heat or other stress, immune response, and other critical factors. The capability to rapidly detect these changes will feed tactical or medical COP(s) and AI(s) for response and analysis, enable the projection of the point of medical surveillance forward to a field location by sequencing sampled fluids and or residue without the need for a field

laboratory, and enable increased Soldier protection and survivability through faster physical and medical responses. (RCs 3, 8, 12, 13, 15, 17, 28)

(h) Research into novel methods for rapid, precise and dependable remote sensing of chemical, biological, and nuclear contamination, using active, passive, and hybrid technological approaches. Rapid detection of these hazards will enable increased Soldier protection and survivability through faster physical and medical responses, population of tactical or medical COP(s) and AI(s) for response and analysis, and enable increased Soldier protection and survivability. (RCs 1, 3, 4, 8, 12, 15, 16, 17, 35, 36, 40, 41)

(i) Research into paired sensor-shooter/effect tandems. Sensors paired with onboard lethal/nonlethal capabilities will minimize or eliminate the kill chain when executing an effects mission thus increasing the accuracy and precision of detection and engagement. (RCs 1, 4)

(j) Research into broadly multifunctional sensors, capable of operating underground, in DUT and all other conditions, with little to no degradation in performance, and without significant human manipulation or control. Sensors leveraging EO/IR, sonic, seismic, electromagnetic, and other detection options will increase the fidelity of the MDCOP and further increase Soldier and platform situational awareness, protection, and mission success. (RCs 1, 3, 4, 11, 17, 18, 25, 26, 27, 35, 41)

(k) Research into enhanced distributed sensing systems, including sensors and models for cooperative active and passive sensing. Distributed and networked sensors will provide for enhanced situational awareness, a highly informed MDCOP, reduce decision-making times, enable better tactical and operational decision making, and increase mission success while reducing casualties. (RCs 1, 3, 4, 11, 17, 22, 32, 32, 33, 35, 41)

(l) Research into enhanced technologies for enemy directed energy source position determination, including location and type of enemy systems. Rapid location and identification of enemy systems will enable rapid and robust protection of friendly systems and engagement of enemy systems with appropriate deception, interdiction, or attack effects. (RCs 1, 3, 4, 26)

(m) Research into enhanced detection of adversary ISR, including location and type of enemy systems. Rapid location and identification of enemy systems, potentially using disposable systems, will enable rapid and robust protection of friendly systems and engagement of enemy systems with appropriate deception, interdiction, or attack effects. (RCs 1, 3, 4, 5)

(n) Research into novel methods of leveraging sensitive RF for detection of adversary receivers, particularly passive RF detection systems. Rapid location and identification of enemy systems, potentially using disposable systems, will enable rapid and robust protection of friendly systems and engagement of enemy systems with appropriate deception, interdiction, or attack effects. (RCs 1, 3, 4)

(o) Research into novel methods of monitoring self-signature and maintaining SA of self-emissions/RF signature. Continuous signature management will enable increased protection through decreased enemy ability to engage friendly resources and assets. (RCs 1, 3, 4)

(p) Research into enhanced synthetic biologicals for use in forensics, biometrics, and police/police intelligence operations including the detection of species, individuals, novel tagging, and manufacture signatures. The ability to engineer customized taggants and other technologies will increase the flexibility, accuracy, and precision of these operations, enabling increased protection of friendly forces. (RCs 15, 16, 22)

(q) Research into enhanced human identification capabilities to enable recognition at greater stand-off distances, including facial detection and recognition in low light settings, through vehicle windows and at various pose angles, gait/anthropometrics, and voice. Recognition of friends/foes at increased distances increases protection of friendly forces through reduction of fratricide and increase in the volume and speed of detection of enemy forces. (RCs 15, 16, 19, 21)

(r) Research into enhanced multiple mode settings and improved human-machine interfaces for RAS. RAS which can operate in “intelligent” and/or communications network-linked mode or in network-denied mode using preprogrammed specific or intent guidance and onboard navigation will enable missions to continue without continuous human control. (RCs 1, 2, 3, 6, 18, 23, 24, 31, 33, 36, 38, 41, 42, 43)

(s) Research into enhanced self-optimizing and self-programming AI, capable of enhanced ML and data mining. Rapid ingestion and analysis of rapidly changing data through continually updated algorithms will enable continual updates to situational awareness and the MDCOP, enabling informed decision making and adaptation to adversary actions and other conditions. (RCs 1, 3, 4)

(t) Research into human-guided AI cycle-of-learning protocols, integrating different forms of human interactions with AI at different stages of product development to effectively adapt a single AI’s behavior and performance over time. This will increase friendly force ability to respond to adversarial actions, new technologies, environmental changes, and mission requirements; decrease training data requirements; and increase appropriate Soldier trust and use of technology. Human-guided AI across product development enables the rapid insertion of new AI technologies, enhancing all domain protection throughout the battlefield. (RCs 1, 2, 3, 4)

(u) Research into mutually adaptive human-AI systems and interactive ML will lead to the creation of mechanisms to maintain system stability in the face of scenario change and techniques to leverage both human and artificial intelligences to ensure within-domain and cross-domain team performance. This advancement will enable human-AI adaptive systems that mimic cognitive learning and problem-solving functions to rapidly adapt to changing conditions while conducting protection operations. (RCs 1, 2, 3, 4)

(v) Research into creation, maintenance, and distribution of entanglement will be the basis of future quantum networks, which will include sensor nodes that will enable distributed quantum sensing for more advanced signature detection and time distribution. This advancement will enable sensing for more advanced signatures, including gradients and higher derivatives, to provide a much more complete picture of the field patterns being "seen”, enabling enemy signatures to be detected and monitored with greater sensitivity; along with clock synchronization for situational

awareness, greater bandwidth communications and networking, and more robust EW capabilities. (RCs 1, 3, 4, 21, 25, 27, 30, 32)

(w) Research into atom interferometry, including creation of macroscopic quantum superposition states, ways to prolong coherence, spin squeezing, entanglement creation, and resilience of quantum states against noise and external perturbations, will lead to more sensitive and robust sensors for electric, magnetic, electromagnetic and gravitational fields and also enable inertial sensing required for position, navigation, and targeting in the absence of GPS. The sensor advancements will enable enhanced detection and monitoring of both friendly and enemy signatures in robust and deployable packages, enabling greatly improved situational awareness and navigation and operation in GPS-denied environments. (RCs 1, 3, 4, 21, 25, 27, 30, 32)

(x) Research into causal feature relationship identification, where causal inference is used to aid in determining components, objects, and signals from different modalities with complex relationships. Advancements will enable the determination of the optimal number and sub-set of sensors within a sensor network to monitor and process time-series data to generate sources of potential actionable information. This will enable the efficient use of sensors, where sensors within the network that may be redundant or irrelevant to the task could be reallocated to satisfy other information requirements. (RCs 1, 2, 3, 4, 5)

(y) Research on semantic world models and contextual abstractions, including the development of distributed inference and decision-making algorithms that adapt to available resources and learning algorithms that are modular, composable, and data-efficient that will support adaptive perception-action-communication decision and control loops for distributed and collaborative perception and intelligence for a heterogeneous mix of robotic and autonomous systems (air/ground manned-unmanned and Soldiers). These advancements will enable agents within a distributed heterogeneous team to collaborate and build a shared situational awareness while moving through a contested environment, which will increase situational awareness and enable collaborative learning to understand, model and predict actions to inform missions and planning. (RCs 1, 2, 3, 4, 5)

(z) Research into models or processes and AI/ML that automate terrain reasoning and evaluation. Capability will increase SA, increase decision-making speed and accuracy, and contribute to persistent access across all environments. (RCs 20, 24, 25, 35, 36)

(aa) Research to develop a framework describing the interplay of small-scale multiphase flows with brain metabolism and sleep neurophysiology to quantitatively characterize glymphatic waste clearance dynamics and regulation mechanisms will enable increased Soldier performance by removing the mental ‘fogginess’ of extended wakefulness. This advancement will enable the protection of Soldiers through accelerated recovery from periods of extended wakefulness or chronic sleep deprivation leading to optimized sleep quality and superior learning rates as well as resilience to post-traumatic stress and traumatic brain injury effects. (RC 3, 4)

(ab) Research to establish non-destructive, real-time methods to comprehensively detect and quantify chemical warfare agents, toxic industrial compounds and their degradation products at ultra-trace levels will enable future forces, to quickly and accurately assess CBRN threats and

hazards. Advancements towards the rapid, sensitive, and selective detection of chemicals and contaminants in the environment will lead to real-time understanding of the CBRN environment, enabling forces to respond in a timely manner. (RCs 5, 22, 40)

(ac) Research to identify and model the co-evolutionary dynamics of neural, cognitive, and social networks as people transition between illness and wellness while engaged in rapid integration modalities will enable the discovery of underlying cognitive mechanisms necessary to reduce the time to recovery from the negative consequences of traumatic events to preserve warfighting capability. This advancement will lead to pathways to significantly enhance cognitive resilience and protect military and civilian populations from reducing the recovery time of adverse mental states such as post-traumatic stress disorder (PTSD), depression, anxiety, substance abuse, suicidal ideation, and suicide without the need for pharmaceutical intervention. (RCs 2, 3)

(ad) Research to identify and model the cognitive processes associated with hypnotherapy and mindfulness as tools to develop cognitive resilience will enable the discovery of underlying cognitive mechanism necessary to prevent the onset of cognitive ailments resulting from the experience of traumatic events and, thereby, preserve warfighting capability. This advancement will lead to pathways to significantly enhance cognitive resilience, increase Soldier readiness, and protect military and civilian populations from trauma-induced PTSD, depression, anxiety, substance abuse, suicidal ideation, and suicide. (RCs 2, 3)

(ae) Research to investigate the ability of photonic integrated circuit technology to measure biomarkers in sweat, interstitial fluid, and blood will enable the development of a highly sensitive wearable biomarker monitor to assess Soldier health. Access to actionable information about Soldier's health will enable preservation of the force through force health protection leading to a more ready and fit future force. (RC 3)

(af) Research into enhanced methods to identify, enhance, and reduce the psychological effectiveness of language, tone, images, sounds, and chemicals. The capability to identify likely adversary deception/IW/UW activities and optimal methods to deny them will enable increased protection of U.S. military and Homeland civilian populations and vulnerable non-U.S. populations. (RCs 1, 2, 3, 4, 27, 29, 31, 36, 37)

(ag) Research to discover novel underlying motion primitives through analysis of animal morphology, motor control, and improved physics models will enable the identification of theoretical performance limits while facilitating the development of a corrective control methodology for robust and stable steady-state gaits. The resulting advancements in appendage, body, and gait design will enable unprecedented robust, efficient, rapid, and agile movement of RAS assets in complex and varying terrain, empowering an autonomous teammate capable of executing hazardous operations such as structure breaching and clearing. (RCs 19, 24, 36)

(ah) Research to improve real-time planning and enable dynamic gait switching among motion primitives including the realization of transitions from horizontal to vertical movement (e.g. running to jumping to climbing motions while considering environmental characteristics in planning) and stability of transient effects during dynamic gait switching (that is, smooth stable transient from one motion primitive to another) will facilitate efficient dynamic locomotor

transitions of legged robotic platforms across vastly different complex terrains (such as, resistive soft soil and tall grass to multifaceted boulders and unstable rubble). These advancements will increase the operational space and tempo achievable by robotic platforms, increasing their survivability and utility to achieve protection outcomes such as increasing situational awareness, performance of dangerous tasks, and securing/preserving CCAAs. (RCs 19, 24, 36)

(ai) Research in dynamic whole-body mobile manipulation through computational multi-body dynamics analysis and ML will promote efficient use of the system's entire set of actuators and complete dynamics to achieve more physical work with lighter and cheaper remote systems. This advancement will enable RAS to perform potentially dangerous tasks such as sensor relocation, placement or removal of obstructions, and preparation of the battlefield under hazardous conditions, enhancing overall protection capability while reducing risk of harm to the Soldier. (RCs 19, 24, 36)

(aj) Research into energy dissipation and transfer approaches, including the quantification of impact energy that would need to be mitigated to ensure survival of air deployed ground robots and the determination of how much of this energy can be mitigated through transfer to other forms of energy through behaviors such as rolling, will enable the realization of ground robotic platforms that are capable of surviving drops from extreme heights and speeds. This advancement will enable the delivery of RAS for protection operations without the added risk of having the delivery platform slow-down, descend, land, or hover in a contested and potentially unpredictable landing zone. (RCs 19, 24, 36)

(ak) Research to understand mission and context-aware dynamic tasking, planning, and control for heterogeneous, layered, and scalable teams of robotic and autonomous systems to achieve effective collaboration, coordination and human-agent teaming, including the development of an adaptive, computational framework for composing and recomposing teams of autonomous human and computational assets, will enable the operation and control of large-scale heterogeneous group behaviors and interactions between humans and autonomous agents at the speed of battle. Advancements in heterogeneous group control and behaviors will enable the realization of freedom of maneuver for heterogeneous teams for dynamic operations in contested environments and their ability to operate tactically and in teams to perform ISR, protection, sustainment, and to create local/global overmatch situations. (RCs 1, 3, 5, 20)

(al) Research to develop theory and methods for heterogeneous teams to carry out tasks under dynamic and varying conditions in the physical world including the development of learning algorithms that can identify unfamiliar and out-of-distribution events, react to these events intelligently, and adapt rapidly (in real time) to large changes in the expected physical environment, losses of physical robots, loss or degraded communication between robots, and dynamic adversarial behaviors, will enable robust distributed intelligent systems capable of quickly adapting to new and rapidly-changing operational context and missions. Advancements in adaptive and resilient behaviors will enable heterogeneous teams that are capable of operating and engaging in complex and time varying contested environments while maintaining mission success in face of loss or intermittent or denied access to infrastructure and in the face of large environmental disturbances or changes in understanding. (RCs 1, 3, 5, 20)

(am) Research into improved remote and independent RAS to perform dangerous tasks under dangerous conditions in potentially contaminated areas. Automating these tasks will increase the speed of operations and protect personnel, structures, and materiel. (RCs 18, 22, 23, 24, 33, 35, 38, 41, 42, 43)

(an) Research into enhanced sensors and equipment on manned and RAS platforms to rapidly, accurately, and precisely detect and neutralize CBRN, explosive and nonexplosive hazards and/or obstacles remotely and ahead of forces. Automating these tasks will increase the speed and tempo of operations and protect personnel, structures, and materiel. (RCs 18, 22, 23, 24, 25, 27, 28, 30, 35, 41, 42, 43)

(ao) Research to detect bot accounts on social media, their role in the spread of mis and/or dis-information, the strategies they use, and the role of emotion contagion dynamics in groups and on-line will enable comprehensive understanding of the effect of adversary-generated mis/dis-information. This advancement will enable the early detection of adversarial groups and provide insight into the social media content bots exploit and the complex risk that is associated with mis/dis- information. (RCs 1, 4, 5, 6, 31, 32, 34, 43)

(ap) Research to model the dynamic interdependencies between social institutions (such as, government, family, education, economy, and religion), state building and state fragility will lead to understanding how adversarial groups create and exploit institutional disruption to undermine societal stability. Investigations into the spatial and temporal evolution of social dynamics on non-kinetic conflict will enable the prediction of precursors to conflict and identification of vulnerable regions. (RCs 1, 4, 5, 6, 31, 32, 34, 43)

(aq) Research to advance understanding of deviant cyber flash mobs and subsequently their actions, the identification of hidden relationships within and among different deviant groups using social cyber forensics, and the development of predictive models of deviant cyber flash mob behaviors particular for the transition from coordination activities to disruptive actions, will enable the protection of the military and civilian population against such actions. The discovery of hostile sociotechnical methodologies to promote social disruption will enable the development of counter methodologies to promote cognitive resilience and reduce susceptibility of the military and civilian populations from succumbing to the deleterious effects of such malevolent and disruptive behaviors. (RCs 1, 4, 5, 6, 31, 32, 34, 43)

(ar) Research to model the dynamics of cognitive processes over information networks for efficient information diffusion, controlling its veracity, and forecasting potential cognitive outcomes of these dynamics, will increase understanding on the cognitive and decision-making process that motivate the spread of information. This advancement will enable understanding of information flow dynamics, the derivation of models to provide insight on how authentic and misinformation are propagated differently, how to recognize intrinsic properties of misinformation, and the development of methods to quantify and potentially control the spread of misinformation. (RCs 1, 4, 5, 6, 31, 32, 34, 43)

(2) Obscuration, camouflage, cover, concealment, and deception.

(a) Research into enhanced synthetic biologicals for obscurative coatings and concealments, for broad or narrow-spectrum applications. Customized biologicals will enable tailorable and scalable applications, improving protection of troops and materiel. (RCs 19, 28, 29)

(b) Research into advanced multispectral camouflage, effective across the EMS. Advanced camouflage will enable tailorable and scalable applications, potentially tunable as well, which will improve protection of troops and materiel. (RCs 19, 28, 29)

(c) Research into a cross-domain obscuration capability to manipulate wavelengths of military significance across the EMS. Tailorable, scalable, tactical-level capability will reduce the number of hazards friendly forces are exposed to at critical times, increasing protection of personnel, facilities, and materiel. (RC 19, 27, 28, 29)

(d) Research into bispectral obscuration for artillery and mortar delivery, nominally in the form of microparticles and nanoparticles. Advanced and tailored obscuration engineered for projection and remote delivery will enable tailorable and scalable applications, potentially tunable as well, which will increase protection of troops and materiel. (RCs 19, 28, 29)

(e) Research into improved multispectral and tailored obscurants, effective in the visible and other EMS domains. Advanced obscurants will enable tailorable and scalable applications, potentially tunable as well, which will improve protection of troops and materiel. (RCs 19, 28, 29)

(f) Research into quantum entanglement engineering may enable "teleporting" information between particles without any physical connection and could result in an aerosol that can be tuned remotely to change its electromagnetic response for increased adaptivity. A tunable aerosol obscurant can be prepositioned and tailored as conditions require to adaptively obscure signatures from friendly systems, improving protection of troops and materiel. (RC 5, 19, 27, 28, 29)

(g) Research into remote activation, such as quantum entanglement or nanoelectromechanical systems sensors in combination with materials that can change their physical state, may enable the realization of obscurants with scalable effects that can be controlled remotely and with escalating effect (i.e. obscuration, anti-personnel, lethal). This capability will allow commanders to quickly respond to constantly changing dynamics on the battlefield. ((RC 5, 19, 27, 28, 29)

(h) Research into enhanced cyberspace and electromagnetic activities for camouflage, including RF and cyber decoys. These capabilities will degrade enemy situational awareness and lead to impaired enemy decision making while enabling increased protection of friendly troops and materiel. (RCs 1, 5, 19, 28, 29)

(i) Research into improved radio frequency physical decoys (RF spectrum replication). These capabilities, tailorable and programmable according to the tactical situation, will degrade enemy situational awareness and lead to impaired enemy decision making while enabling increased protection of friendly troops and materiel. (RCs 1, 5, 23, 28, 29)

(j) Research into improved rapidly deployable multispectral physical decoys (EMS decoys). These capabilities, tailorable and programmable according to the tactical situation, will degrade enemy situational awareness and lead to impaired enemy decision making while enabling increased protection of friendly troops and materiel. (RCs 1, 5, 23, 28, 29)

(k) Research into enhanced techniques or materials to conceal EMS signatures. These capabilities, tailorable and programmable according to the tactical situation, will degrade enemy situational awareness and lead to impaired enemy decision making while enabling increased protection of friendly troops and materiel. (RCs 1, 5, 23, 28, 29)

(l) Research into reciprocal and deterministic RF hardware and low-latency techniques/algorithms for time and phase synchronization of distributed transceivers will enable complex communication and resilient electronic warfare application of ground and air platforms to degrade adversary sensors and communications, allowing for extended operations within A2/AD environments. This advancement will enable offensive EW options for commanders to shape the adversary's information environment, potentially leading to windows of opportunity. (RCs 1, 5, 33)

(m) Research into ghost imaging (both classical, using thermally correlated photon pairs, and quantum, exploiting entangled photon pairs) may enable imaging of targets at stand-off without the enemy being able to use illumination to detect the location of the imaging system. This advancement would enhance friendly capability to perform ISR and targeting, and impact the enemy's ability to sense and target friendly forces, and enable freedom of maneuver, force protection, and C2. (RCs 1, 3, 5, 25, 27, 35)

(n) Research into the design and use of metamaterials, and the design and use of nanoparticles of various sizes, shapes, and surface roughness, which enable selective obscuration at select frequencies / wavelengths, or for cloaking of objects. This innovation will enable the manipulation and obscuration of signatures and emissions of future formations to confuse and deceive threat C2 systems and enhance the protection of troops, vehicles, and structures. (RCs 19, 28, 29)

(o) Research into high-fidelity modeling, simulation, and emulation technologies to enable research and demonstration of real-time cognitive EW concepts and techniques in complex, highly-realistic electromagnetic environments. This advancement will reduce the time of EW research and development, leading to resilient, threat-agnostic EW capabilities. (RCs 1, 20, 21, 23, 28, 29, 33)

(3) Physical and communications network / cyber protection.

(a) Research into enhanced active protection systems for tactical vehicles and the ability to install the capability into semi-permanent structures. Capabilities which span the spectrum from electronic to physical responses, including nonlethal and lethal, counter-UAS, protection swarms, DEW, and other methods which account for the full range of known enemy capabilities, will enable increased protection of friendly troops and materiel. (RCs 5, 8, 9, 10, 12, 14, 23, 41)

(b) Research into improved wearable and/or portable passive and active protection systems to protect individuals and small teams even when dismounted and away from ground platforms. Capabilities which span the spectrum from electronic to physical responses, including nonlethal and lethal, counter-UAS, protection swarms, DEW, and other methods which account for the full range of known enemy capabilities, will enable increased protection of friendly troops and materiel. (RCs 5, 12, 23)

(c) Research into enhanced materials, mechanisms, and construction or emplacement methodology to provide lighter weight protection from evolving ballistic, blast, and directed energy threats. Development of advanced natural and engineered materials and energetics will reduce logistical requirements and enable increased protection of friendly troops, structures, and materiel. (RCs 5, 8, 9, 10, 12, 23)

(d) Research into advanced screening, reflective, absorptive, transformative, or other materials and methods to deny DEW. This technology will enable improved SA and increase the protection of personnel, materiel, structures, and both physical and cyber infrastructure. (RCs 1, 8, 10, 23, 26)

(e) Research into enhanced synthetic biologicals for rapid pharmaceutical generation. The capabilities for tailored production upon need and broad-spectrum immune response and other enhancers as both prophylactic and response measures will enable increased protection of friendly troops and potentially American civilians from intentionally or unintentionally released hazards. (RCs 12, 13)

(f) Research into applications of enhanced AI for global surveillance of indicators of communicable disease outbreaks or adversary activities indicating potential intentional CBRN activities, fed by open-source reporting, materiel, and technology acquisitions and information, along with government-collected intelligence information. This technology will enable early situation awareness of use or spread of these hazards, enable rapid prophylactic and response measures, enable increased protection of friendly troops, and potentially American civilians from intentionally or unintentionally released hazards. (RCs 1, 4, 5, 8, 12, 13)

(g) Research into enhanced rapid decontamination of CBRN-contaminated equipment in all climate and weather conditions with massively reduced or eliminated requirement for water. Development of increasingly frictionless or contaminant-resistant surfaces, tailored slurries, biologicals, or other capabilities, which reduce or eliminate the need for water in the decon process, will enable increased protection of friendly troops and materiel. (RCs 5, 7, 8, 10, 12, 14, 22)

(h) Research into enhanced rapid wide-area and large-scale semiautonomous or autonomous decontamination technology to support terrain and wide-area / large-scale decontamination operations such as the equipment in a motor park and the motor park itself. This capability will enable friendly forces to rapidly continue operations following a contamination event. (RCs 5, 7, 8, 10, 14, 22)

(i) Research into enhanced multifunctional materials that provide capabilities in the areas of physical protection, sensing, adsorption, and decontamination of chemical hazards. Provision of

catalysts and membranes/textiles will significantly enhance protection of the wearer through decomposition of adsorbed chemical agents. (RCs 5, 8, 10, 12, 14, 22)

(j) Research into methods for the enhanced use and recycling of indigenous, used, or other available materials into source materials for power and construction of facilities and protective structures. The use of these rapid processing techniques for compaction, melting, combustion, 3D printing, and other applications will significantly reduce logistical burdens and increase the speed of construction. (RCs 8, 10, 19, 42)

(k) Research into enhanced military and civilian communications networks, facilities, and infrastructure able to detect and block adversary activity, warn friendly forces of intrusion and attack, and also attack intruders, in the cyber and physical domains. This technology, leveraged through a common user interface, will enable improved situational awareness and increase the protection of personnel, materiel, structures, and both physical and cyber infrastructure. (RCs 1, 4, 6, 7, 8, 9, 10, 14, 17, 20, 22, 23, 32, 33, 34, 35, 38)

(l) Research into threat-agnostic electronic warfare support algorithms that identify transmitters and receivers based on intrinsic hardware characteristics and cognitive electronic attack algorithms and concepts of employment will enable threats to be addressed with no prior information or intelligence. This advancement will enable electronic attack systems that will learn through feedback from damage indicators and converge in real time to execute more effective attacks. (RCs 4, 5, 6, 31, 23, 31, 34)

(m) Research into extremely heterogeneous networking, which utilizes multiple diverse communication technologies and intelligent networking protocols, will increase the accessibility, availability, and resistance of the physical layer of the electromagnetic spectrum and cyberspace domain. This advancement will enable the establishment of a resilient and secure cyberspace infrastructure. (RCs 4, 5, 6, 20)

(n) Research into context-aware networking, which enhances network performance through exploitation and inference of multiple environmental contexts (network, mission, radio, threat) will support predictive, anticipatory adaptation of networked information, including intrusion alarms or anomalous behavior. This development will maximize the overall information capacity of networks that will adapt to changing mission requirements and limitations of the network environment, specifically enabling greater understanding of cyber threats in the network. (RCs 4, 5, 6, 20)

(o) Research into network agility systems for autonomous cyber-defense and resilience to direct proactive cyber maneuvers that consider various network characteristics, topologies, and platforms to support and improve machine-learning techniques that evaluate multiple cost (i.e. performance) and security tradeoffs within Army networks. Advancements will provide commanders more options, contribute to better autonomous planning and control of cyber maneuvers, and increase the capability to deceive adversaries and protect Army cyber assets. (RCs 4, 5, 6, 20)

(p) Research into advanced systems for detection of cyber threats, to enhance situational understanding of the network through decentralized, distributed monitoring and vulnerability / attack analysis, will support autonomous, adaptive protection of Army cyber networks. This development will improve the robustness and resilience of the network in the face of dynamic mission requirements and powerful adversaries. (RCs 4, 5, 6, 20, 23, 31, 32, 33, 34)

(q) Research into adversarial machine learning (AML) for the cybersecurity domain enhances cybersecurity and resilience through development of attacks and defenses against advanced ML employed in the cyber domain, such as intrusion detection, network traffic classification, and firewalls. This research will enable military operations to leverage AML/ML advances for the cyber domain to understand vulnerabilities of ML systems and harden hosts against emerging and evolving AML threats. (RCs 4, 5, 6, 20, 23, 31, 32, 33, 34)

(r) Research into dynamic honeynet capabilities to improve robustness of cybersecurity through development of strategic approaches and technical capabilities to generate synthetic aspects of the cyber environment, including generation of network topologies, users, information, services, and profiles. This research will provide additional cyber defense capabilities enabling better understanding of adversarial intent and capabilities as well as enhanced strategies to mitigate the impact of adversarial attacks. (RCs 4, 5, 6, 20, 23, 31, 32, 33, 34)

(s) Research into vulnerability assessments of large, complex networks of heterogeneous systems will support adaptive protection of Army cyber networks. This development will incorporate security/performance requirements and mission context, such as the complexity of the network, host, and programs and the potential attack surface it presents, into the intelligent monitoring of assets and vulnerabilities that can lead to devastating zero-day attacks. (RCs 4, 5, 6, 20, 23, 31, 32, 33, 34)

(t) Research into self-adaptive heterogeneous networking enhances protection against adversarial detection of presence through low probability of detection communications to conceal network, emissions, and applications. This research will enable military operations to demonstrate self-awareness, self-organization, self-healing, and self-protection against near-peer adversaries. (RCs 4, 5, 6, 20, 23, 31, 32, 33, 34)

(u) Research into multi-agent game theory and machine learning approaches will support the tactical protective deployment of several heterogeneous counter-measures / agents to orchestrate a cooperative defense at machine speed. This advancement will enable the coordinated use of multi-agents and counter-measures to intercept and disrupt coordinated multi-threat strikes. (RCs 4, 5, 6, 20, 23, 31, 32, 33, 34)

(v) Research into improved AI-driven broad-spectrum screening of personnel to achieve faster and more accurate medical readiness assessments. Reduction in post-mobilization medical requirements will increase personnel and force readiness and availability and reduce cost. (RCs 8, 13)

(w) Research into advanced synthetic biologicals for improved human performance. Improvements in cognition, endurance, strength, resistance to disease vectors, and other performance measures will increase personnel effectiveness and readiness. (RC 3)

(4) Cognitive protection.

(a) Research into advanced methods for continuous and ubiquitous detection of and response to adversary IWar activities in military and civilian communications and media such as "deep fakes" and other effects. The ability to detect and apply cyber and/or physical effects as a form of "reactive armor" will provide accurate SA, improve decision making, and protect military and civilian populations from adversary activities. (RCs 2, 3, 5, 23, 31, 32, 34, 43)

(b) Research into enhanced training protocols for instilling critical thinking and resiliency in military forces, which could also be used by the general population, to enable cognitive protection against adversary IWar. Military individual, institutional, and unit training, and supporting civilian training, with both including training in identification of and response to likely mis/disinformation, will provide both with more accurate SA, improved decision making, and increased protection of military and civilian populations from adversary activities. (RCs 2, 3, 23, 31, 32, 34, 43)

(c) Research, in conjunction with and in support of the Whole of Government, into an improved national standard for assessing and displaying information validity, similar to what is currently done with nutrition labels on food and indicators of web site trustworthiness. This capability, as a continuous and ubiquitous national and informational security measure, will provide accurate SA, improve decision making, and protect military and civilian populations from adversary activities. (RCs 2, 23, 31, 34)

(d) Research to characterize, model, and control the spread of misinformation or disinformation to enhance networked applications by suppressing misinformation to enable faster and more accurate shared situational awareness. This research will assist in filtering out potential misinformation to mitigate the impact of adversarial information on shared situation awareness and to also counter adversarial narratives and information shaping activities. (RCs 2, 3, 5, 23, 31, 32, 34, 43)

(e) Research in computational social science to create verifiable models of social networks and human behavior to understand and predict when coordinated social media actions will likely become real-world threats. Advancements in computational social science will enable public opinion forecasting and scenario testing of information operations. (RCs 2, 3, 5, 23, 31, 32, 34, 43)

(5) Enhanced materiel, modularity, interoperability, and repurposing.

(a) Research into enhanced massively interchangeable and integrated hardware and software which has plug-and-play capability, is nonproprietary, and is engineered for common connections, power supplies, communications network protocols, and other factors. This will reduce the integration and other burdens inherent in operations and sustainment and will reduce the logistical burden. (RCs 3, 4, 44)

(b) Research into advanced customizable shipping and packing containers and materials, designed for multiple uses and able to be shipped and carried on multiple platforms, enabling receiving or other unit to use, reuse, or recycle all components, including as construction material or bulk source material for local 3D printing of supplies and equipment. This will reduce the transportation and logistical burden, reduce waste, increase operational readiness rates, and increase speed of construction. (RCs 3, 4, 44)

(c) Research into advanced materials, optimized packaging, and reduction in size and weight. Reducing the weight and optimizing the form factors of equipment, vehicles, and supplies will reduce the transportation and logistical burden, cost, and waste. (RCs 3, 44)

(d) Research into remote, autonomous or automated construction methods that enable access and remove operators from the point of application. Capability will provide increased speed of construction and protection of personnel. (RCs 8, 12, 42, 44)

(e) Research into rapidly assessing damage with remote, autonomous or automated means, and repairing critical infrastructure (ports, airfields, supply depots, roads) that preserve access to strategic and operational CCAAs. Capability will provide increased speed of construction and protection of personnel. (RCs 11, 42, 43, 44)

(f) Research into technologies for rapidly repairing damage to vehicles and equipment, restoring structural integrity and functionality, such as the application of heat or light to epoxy welds or joins. Capability will provide increased functionality, mission effectiveness, and protection of personnel and critical systems. (RCs 8, 10, 44).

(g) Research into advanced automated remote 3D printer/manufacturing equipment for remote/onsite fabrication of repair parts, tools, and other materiel. This will reduce the transportation and logistical burden, reduce waste, and increase operational readiness rates. (RCs 3, 44)

(h) Research into enhanced networked, smart munitions capable of sensing and sending data and information through and to the communications network and to other munitions, including lethal and nonlethal applications, for terrain shaping or other denial operations. Capability will increase SA on area denial operations and of enemy activity and increase accuracy, precision, lethality, and proportionality of engagements. (RCs 4, 5, 24)

(i) Research into advanced explosives for use in munitions and terrain shaping applications. Capability will increase lethality, impact enemy movement and maneuver, and reduce friendly logistical burden. (RCs 19, 24)

(j) Research into advanced non-explosive obstacles for use in terrain shaping applications. Capability will impact enemy movement and maneuver and reduce friendly logistical burden. (RCs 19, 24)

(k) Research into improved synthetic biologicals to be used in self-healing concrete. The use of tailored or engineered organisms in concrete mixes will increase the durability and life of

emplaced concrete, reducing the cost and logistical burden and increasing the usable lifespan of constructed structures and facilities. (RCs 8, 10, 19, 42, 44)

(l) Research into improved sprayable synthetic biologicals for roads and runways. The use of novel materials for dust abatement and soil stabilization will increase the durability and life of constructed facilities; reduce wear in air and ground platform rotors, engines, and machinery; reduce health and safety risk from degraded visual environments; and reduce cost and logistical burden. (RCs 3, 42, 44)

(m) Research into improved sprayable synthetic biologicals for armor and building materials. The use of novel materials to harden structures and building materials will increase structure and material durability and life, reducing the cost and logistical burden; increasing the usable lifespan of constructed structures and facilities; increasing protection for personnel, material and facilities; and reducing the transportation and logistical burden and reducing cost. (RCs 3, 8, 10, 42, 44)

(n) Research into improved synthetic biologicals for improved waste stream management. The reduction in or repurposing of waste will reduce cost and the logistical burden. (RCs 3, 44)

(o) Research into improved synthetic biologicals for improved fuels and energetics. Scalable production of enhanced products without traditional chemistry and resource limitations will reduce cost and the logistical burden and enable missions of longer range and duration. (RCs 3, 42, 43, 44)

(p) Research into improved synthetic biologicals for small scale power. The use of low power but longer-lived power sources, potentially renewable through "recharging" with organic matter vs electric methods, will reduce cost and the logistical burden and enable missions of longer range and duration. (RCs 3, 42, 43, 44)

(q) Research into nuclear metastables (isomers), where the current focus on isomer depletion (switching) via the newly-discovered nuclear excitation by electron capture, will enable nuclear energy to be tapped without fission reactors thereby supporting the goal of moving beyond the chemical limit. The output power from this process can be converted to electricity or mechanical energy, offering an alternative to fossil fuels to reduce logistics demand and support long-duration-energy requirements. (RCs 3, 42, 43, 44)

(r) Research into improved synthetic biologicals for continuous fuel production. The onsite or onboard production of fuel will reduce cost and the logistical burden and enable missions of longer range and duration. (RCs 3, 42, 43, 44)

C-6. Conclusion

The science and technology solutions in this appendix provide Army forces with the capabilities to execute multi-domain protection operations from the SSA / homeland into the theater of operations. The solutions enable the preservation of CCAAs through enhanced SA derived from advanced sensors, data processing and the application of technologies such as synthetic biologicals. The solutions enable the denial of enemy freedom of action through detection and denial/counter of adversary ISR, IW, UW, and activities using physical, virtual, and cognitive

effects in all domains and environments. The solutions also enable the force to generate persistent access in the OE through robust application of advanced biologicals, advanced fuels and energetics, and improved computing and RAS/AI technologies. The application of these capabilities through the use of communications network and AI decision-support technologies and fleets of RAS will enable assets and capabilities to provide convergent multi-domain protection.

Appendix D
Dependencies

D-1. Introduction
This appendix identifies the dependencies on other functions required to perform the capabilities identified in this concept.

D-2. Protection dependencies on other warfighting functions and supporting activities

a. Aviation.

(1) Army aircraft contributions to the protection WfF include providing early and accurate warning of enemy operations, air movement of key personnel and supplies to support engineering and breaching efforts, and rapid transport of bridging equipment to enable wet gap crossings. Ensuring that Army aircraft target acquisition systems meet joint standards for probability of correct identification of friendly ground entities contributes to protection by reducing the risk of fratricide and collateral damage when attack aviation provides close support of friendly ground elements.

(2) Aviation dependencies upon the protection WfF include the security of airfields, assembly areas, forward arming and refueling points, the coordination for air defense, and CBRN contamination mitigation.

b. C2.

(1) The future Army C2 system contributes to protection primarily through the development of bold, agile, and innovative leaders with the expertise to think, plan, and conduct protection activities throughout all domains, the EMS, and the IE. Future Army commanders, supported by their staffs, are able to systematically consider CCAAs, determine risks, rapidly make quality decisions, and establish and disseminate priorities for their protection. Future Army forces rapidly form cohesive, multifunctional teams while combining their diverse knowledge, expertise, and capabilities across all 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 protection forces and capabilities to bear against threats to preserve the force, deny threat and enemy freedom of action, and enable access.

(2) The future C2 system modifies the Army's overarching operations process – plan, prepare, execute, monitor, and assess – to integrate seamlessly with a protection assessment. This enhanced

operations process allows commanders and their staffs to consider fully all domains and dimensions then innovatively converge joint, multinational, and interorganizational capabilities to create windows of superiority and open and maintain access to protected corridors in which to conduct cross-domain maneuver. Future knowledge management optimizes how information is collected, developed, and shared throughout the operations and protection assessment processes. Knowledge management ensures commanders and their staffs have the right information at the right time to assess risk to CCAAs and determine protection requirements and priorities.

(3) The future unified communications network provides the Army's non-stop, day-to-day communications needs and is flexible, tailorable, responsive, interoperable, and resilient enough to support the conduct of MDO with any set of mission partners and in any environment. The future communications network links leaders, Soldiers, Army civilians, and other mission 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. It enables Army forces and mission partners to collaborate and create all domain battlefield visualization and shared understanding of protection needs and interdependencies through a tailored operational picture based on common, standardized, shareable, and secure data. The future communications network capitalizes on AI to support protection decision making and battle management.

(4) Future protection capabilities are critical to ensuring the survivability of dispersed command nodes and maintaining continuity of command. These protection capabilities include the ability of command nodes to be aware of their own visual, thermal, radio frequency, acoustic, and seismic signatures and, as necessary, decrease, obscure, or otherwise manage and control these identifying signatures. Other protection capabilities include improved camouflage and concealment, greater tactical deception capabilities, and hardening and protecting command nodes from enemy and weather effects.

c. Cyberspace and electromagnetic warfare.

(1) Cyberspace and EW contribute to protection through cyberspace security and defense and electromagnetic protection. Cyberspace elements identify threats, maintain status, and recommend defensive measures in the cyberspace domain, EMS and the IE to ensure the future forces has the maximum use of these resources in MDO. Protection coordinates with the appropriate cyberspace and electromagnetic warfare element to deny enemy offensive use of the cyberspace domain, EMS and the IE against friendly forces.

(2) Cyberspace and electromagnetic warfare depend on protection to account for the overall scheme of protection, include assets on the prioritized protection list, and coordinate defensive activities with the appropriate cyberspace elements. Protection also accounts for physical security requirements for cyberspace infrastructure and coordinates hardening and survivability of the physical assets.

d. Fires.

(1) Fires support protection by delivering lethal and nonlethal effects across the MDO framework to preserve CCAAs, penetrate and dis-integrate A2/AD, open windows of opportunity to exploit and neutralize enemy integrated air defense system (IADS) and long-range artillery, and enable cross domain maneuver. Fires support denial of enemy freedom of action through countering enemy fires, AMD, cyberspace, space, information warfare, and providing short-range air defense for class I-III UAS. Fires provide AMD to defend critical assets.

(2) Fires forces, including both AMD and field artillery, require security, protection, and survivability of sensors, shooters, and command nodes. Protection also enables fires function through CBRN hazard contamination mitigation, cover and concealment, and situational understanding of the prioritized protection requirements at echelon for mission support.

e. Information.

(1) Information supports protection by denying all domain enemy information warfare to deny freedom of action, and by preserving CCAAs through the IE, including the home installation (Soldiers and Families).

(2) Protection enables information through dependencies on Army C2 systems; cyberspace security and internal defensive cyberspace operations; preserves friendly activities in the EMS; employs OPSEC in decisive action; and preserves and secures facilities, systems, and data. Protection staffs at echelon plan, prioritize, coordinate, and synchronize the preservation of CCAAs, to include information, and deny enemy actions to enable friendly force access.

f. Intelligence.

(1) Intelligence supports protection through collection from broad sources of information (such as, sensor, open source, coalition, and host nation) and conducts analysis fusing information and intelligence to produce specific products providing situational awareness of the environment and operations. Intelligence assists in identifying key threats, obstacles and hazards to counter and deny enemy freedom of action. Intelligence contributes to forensics and biometrically-enabled identity intelligence to support the understanding of irregular and criminal threats, hostile actors, and high value targets present in the OE and by facilitating policing and protection operations. Counterintelligence teams support force protection across the MDO framework through identifying and enhancing situational understanding against enemy infiltration, collection, targeting, and their assessment of friendly activities.

(2) Intelligence depends on protection for the preservation of physical systems and assured access to cyberspace, the EMS and the IE. Intelligence integrates with MP detention operations to facilitate the interrogation of prisoners of war, captured criminals, surrogates, and other nefarious actors.

g. Maneuver (BCT).

(1) The BCT contribution to protection is to disrupt and deny the enemy's ability to sense, detect, and target the force's capabilities and intentions. The BCT is also an option to secure and

preserve CCAAs when it is not engaged in decisive action. The BCT provides support with denying both conventional forces and irregular warfare in the close and tactical support areas. Cross-domain maneuver will require BCTs to understand the enemy in order to operate semi-independently. Organic CBRN formations will allow BCTs to understand CBRN threats when operating with organic cavalry squadrons conducting cross-domain reconnaissance and security.

(2) Through its assigned maneuver units, the BCT typically coordinates multi-domain defense support, layered protection of CCAAs, survivability and terrain shaping, security and mobility support, denying explosive hazards, detention operations, forensic and biometric enabled intelligence, CBRN reconnaissance and surveillance, contamination mitigation, EOD detachment support, cyberspace and EMS defenses and protection, FHP, populace and resource control, and operational, information and physical security. Protection reinforces the BCT's ability to accomplish its assigned mission.

h. Medical.

(1) Army medicine contributes to protection by preserving the force through force health protection. This includes establishing and sustaining a healthy and fit force; health promotion and nutrition programs; the identification of the health threat in all occupational, environmental, and health settings; the development and implementation of preventive medicine measures to reduce exposure to health hazards; and mitigating the adverse effects of the impact of health threats to military personnel.

(2) Medical relies on protection to prioritize accurately medical protection requirements to preserve CCAAs.

i. Space.

(1) Space and high-altitude capabilities contribute to protection by providing assured access to space effects, communications, ISR, PNT, and air and missile warning. Army space elements coordinate with the appropriate agency to counter enemy space effects (deny and degrade) in order to deny enemy freedom of action.

(2) Space depends on protection to secure and preserve critical orbital, high-altitude and ground segments and communication links; to enable tactical NAVWAR devices; and to coordinate for theater AMD and homeland GMD.

(3) Army space forces deny enemy space-based ISR and support forward commanders through tasking of assigned space ISR assets.

j. SOF.

(1) SOF contributes to protection by providing observation of the deep areas and identifying immediate threats that present danger to CCAAs denying enemy freedom of action. SOF elements detect and report CBRN hazards and first-seen munitions in the deep maneuver and fires area. SOF assists conventional forces denying special purpose forces, unconventional warfare, violent

extremist organizations, and proxies in the close and support areas. SOF performs CWMD operations with specially trained CBRN and EOD personnel.

(2) SOF requires home-station protection of families, installations, facilities, systems, logistics, and strategic transportation against cyber-attacks and information warfare in the strategic support area to enable reliable and rapid force projection and uninterrupted operations across the competition continuum.

(3) The organization of the Army special operations forces (ARSOF) health support system is determined by the Army and joint force missions, the threat, intelligence, anticipated number of patients, duration of the operation, the theater patient movement policy, available lift, medical logistics capabilities, FHP and hospitalization requirements. The TSOC / SOJTF commander coordinates conventional health service support (HSS) packages to augment the ARSOF organic medical capability using the organic surgeon section. This is critical, as ARSOF has no organic medical evacuation, Role 2, or Role 3 medical capabilities.

(4) ARSOF operational elements, at echelon, employ unmanned ground, air, and water-borne delivery and medical/casualty evacuation systems; leverage indigenous procurement mechanisms; and use additive manufacturing techniques as they become available, to meet medical sustainment demands at the point of need. ARSOF headquarters at echelon plan for medical considerations, such as medical/casualty evacuation, prolonged care, and challenges of medical care in the deep areas. The special operations advanced tactical practitioner is a highly trained special operations medic who delivers a selected level of medical care normally reserved for health care providers. Special operations medics provide point of injury care, forward resuscitation, and prolonged patient care capabilities.

(5) CA brings critical capability to protection through its inherent synchronization, coordination, and integration of the activities of interorganizational partners with military operations to achieve unity of effort. The only Army elements that routinely and deliberately seek out civil organizations and incorporate civil considerations into military operations are its CA forces. At all echelons, across the competition continuum and in coordination with interorganizational partners, CA forces execute civil network development and engagement, civil-military integration, and transitional governance operations. The design of the core competencies is to:

(a) Answer civil information requirements to provide expanded situational understanding and inform targeting and decision-making cycles as well as build and mobilize networks with capabilities that provide the supported commander with options for preservation of combat power, consolidation of gains, or denying enemy freedom of maneuver.

(b) Establish a civil information-sharing architecture, civil knowledge management processes, and civil-military integration centers that use the Army's communications network and other integrating processes to enable collaboration, integration and synchronization of interorganizational partner knowledge, capabilities, and resources with those of military forces to achieve projected outcomes.

(c) Provide governance expertise, support to civil administration of liberated areas, and transitional military authority in occupied territories as part of the whole of government approach to operations across the competition continuum.

k. Sustainment.

(1) Sustainment contributes to protection by providing all classes of supply, transportation, maintenance and personnel support; EOD capability; medical capabilities for HSS and installation and power projection through Army Materiel Command support; and U.S. Transportation Command support.

(2) Sustainment depends on protection for security and the preservation of CCAAs beyond unit capability such as sustainment nodes, transportation vehicles, sites along routes and lines of communications, personnel replacement, currency, and prepositioned stock.

Appendix E
Protection Across the Competition Continuum

E-1. Introduction
The U.S. Army in MDO must deter and defeat the threat in competition and in conflict. The Army Operating Concept describes the five operational problems of compete, penetrate, dis-integrate, exploit, and re-compete which are aligned to the three parts of the competition continuum and which the force must accomplish to achieve strategic objectives. Protection enables MDO across the competition continuum by preserving CCAAs, denying threat and enemy freedom of action, and enabling access. The following sections describe initially how protection enables MDO across the competition continuum. There is expectation that additional contribution may be identified through focused MDO learning and experimentation in the near future.

E-2. Competition

a. Army forces, as part of JIIM, compete with a near-peer adversary by defeating their operations below the threshold of armed conflict, expanding the competitive space, and deterring an escalation of violence. Protection in competition achieves four critical objectives: deter conflict, counter expansion of competitive space below armed conflict, enable rapid transition to armed conflict, and protect the force (preserve – deny – enable).

b. In competition, the force must train and prepare in many areas, including protection. Soldiers, commanders, and staffs train on protection procedures to support mission objectives. This includes individual techniques, collective procedures, and staff functions to assess risk to the force and prioritize requirements. The Army must also train with JIIM partners to ensure interoperability and build partner capacity.

c. The Army protects the force to ensure mission success. In competition, the protection staff must be able to see and understand the operating environment. It must be able to identify critical capabilities, assets, and activities that must be preserved to deter and defeat; understand the threat

and risk; and prepare protective and defensive measures for the force to operate below the threshold of conflict. Protection staffs prepare, integrate, and synchronize requirements and resources to enable friendly freedom of action.

d. The Army denies enemy stand-off. Information warfare and unconventional warfare are the enemy's primary means of stand-off in competition. The protection WfF tracks and monitors enemy information and unconventional warfare, coordinates mitigation actions, and preserves friendly force capability to operate across the MDO battlefield in all domains, the EMS, and IE. Protection staffs ensure there are no limitations due to enemy information and unconventional warfare prior to transitioning operations. Protection requirements synchronize with forward deployed Army special operations forces to support Theater Special Operations Command (TSOC) and Special Operations Joint Task Force (SOJTF) objectives.

e. FHP measures conducted in competition reduce casualties from disease and non-battle injuries, and ensure the maximum number of Soldiers is ready to conduct operations through medical functions that include COSC, dental services, veterinary services, operational public health, and laboratory services. FHP in competition requires coordinating with JIIM partners on developing, integrating, and executing FHP plans, procedures, and capabilities. FHP includes plans and operations to protect the force against novel or unexpected health threats for which available medical prophylaxis, treatment, and control measures are minimal or ineffective.

f. The Army employs deception to protect friendly force operations in competition. The Army uses multiple methods to cover and conceal friendly force intentions. As part of deception, implementing OPSEC in competition eliminates, reduces, and conceals unclassified indicators that could compromise both classified information as well essential elements of friendly information (EEFI) to enemies and adversaries. This requires maintaining focus and awareness of steady-state operations and the operational timeline; coordinating with JIIM partners to integrate and execute OPSEC in all operation planning, preparation, operational contract reviews, and transition activities; utilizing the military decision-making process (MDMP) to identify and prioritize CCIR and EEFI to mitigate risk; and developing measures to minimize indicators of EEFI. Ultimately, this prevents the adversary from collecting, interpreting, and exploiting information in time to be useful to threat forces.

g. The Army preserves facilities, installations, infrastructure, movement modes, and headquarters in competition in MDO. Activities as part of the APP and protection WfF will intersect each other in future MDO operations as competition expands into day-to-day operations in the American homeland and facilities around the world. A unified effort is required to build combat power, project forces from the SSA / homeland to the operational support area, and sustain operations.

h. Army protection posture in MDO should enable the rapid transition to armed conflict as the escalation of tensions between friendly forces and the threat increases. Competition provides the continuous opportunity for the Army to see, understand, and shape the environment for combat operations.

i. Calibrating the protection force posture in competition develops the appropriate balance of capabilities across the total force with forward presence forces and the ability to deploy expeditionary forces to meet requirements. There are dependencies leveraged with JIIM partners to protect the force in MDO across the operating area.

E-3. Armed conflict

a. When competition fails and operations transition to armed conflict, the Army seeks to rapidly defeat aggression through calibrated force posture, multi-domain formations, and converging capabilities. In armed conflict, friendly forces penetrate threat stand-off, dis-integrate A2/AD, and exploit freedom of maneuver to win quickly and decisively. Protection enables the force in armed conflict to preserve, deny A2/AD, and enable access.

b. In conflict, protection provides critical capabilities that enable the Army to penetrate enemy stand-off, dis-integrate threat A2/AD, and exploit achieved freedom of maneuver. The Army does this through mobility support, clearing and maintaining routes and lines of communications for strategic and operational maneuver. Protection elements secure and protect CCAAs in the rear areas at echelon so maneuver commanders can focus on decisive actions. The protection staff ensures the force disperses adequately across the operating area to prevent vulnerabilities to enemy fires. Commanders employ countermobility activities to block and restrict enemy freedom of maneuver. Protection enhances survivability of critical CCAAs and ensures the force has the ability to maintain momentum as required to meet mission objectives.

c. The Army sees and understands the threat in MDO and characterizes the risk to the force as part of the protection assessment process. The staff develops the protection prioritization list based on risk and inputs from joint requirements through the critical asset list and defended asset list, and expands to include subordinate ground all-domain protection requirements. The Army continuously assesses and updates protection requirements throughout operations. The protection staff visualizes protection requirements to commanders and recommends conditions that should be met prior to transitioning.

d. Coordinate and conduct AMD to preserve CCAAs during conflict. The protection cell coordinates with appropriate air defense artillery and AMD units to provide defense against enemy missile, UAS, and fixed and rotary wing aircraft at echelon. They ensure essential assets on the critical asset list and the prioritized protection list have AMD coverage.

e. The Army continuously consolidates gains, secures those gains, and enables maneuver elements to focus on decisive operations. Commanders employ allocated protection forces to free up BCTs to expand access in denied areas, maintain momentum, and take advantage of windows of superiority against the threat.

f. The protection cell will track the C2 network, the EMS, and IE as critical assets that must be defended and protected at all times to enable MDO operations in conflict and competition. Cyber defense teams conduct Department of Defense Information Network-Army operations for internal defense against threat attacks, and provide alternate means to send data during degraded operations. Cyber-Electromagnetic Activities will ensure protection of the EMS and assure access

to the IE to meet the commander's objectives. Electromagnetic warfare elements will conduct electromagnetic protection by monitoring signatures during operations and recommend changing operating procedures when signatures present high risk of attack.

g. The Army denies enemy A2/AD by identifying threat systems or activities that present high risk to friendly forces, and by characterizing and mitigating the threat. Friendly forces recommend targets through the dynamic targeting process to reduce the risk to CCAAs. The force also coordinates countering activities against specific threats to reduce risk to the force (e.g. counter UAS, counter IW, counter cyberspace).

h. In the event personnel become isolated in hostile areas, the Army conducts personnel recovery of friendly forces in order to save lives. Stranded personnel will perform basic survive, evade, resist, or escape (SERE) procedures to move toward recovery units while avoiding the adversary. Recovery units will coordinate closely with the host nation and other JIIM partners for unity and priority of effort to recover personnel.

i. The Army conducts deception in conflict to defend CCAAs and enable penetration, dis-integration, and onward movement. Future forces will employ camouflage, cover, concealment, decoys, multi-domain obscuration, and conduct OPSEC to prevent the adversary from accurately observing friendly operations; to disrupt enemy information collection; to slow the adversary decision cycle; and to degrade the quality of the enemy's decisions.

j. The Army coordinates space, aerial, and high altitude surveillance capabilities to monitor areas for threat activities that are high risk to friendly operations. Implementing these capabilities allows the force to prioritize employment of protection resources, passively monitor large areas of operations, and maintain focus on high priority decisive operations. Once forces detect activity in surveilled areas, they send response forces to terminate the threat.

k. Protection elements converge multi-domain capabilities to preserve CCAAs against threats in all-domains. Protection capabilities enable the force, while penetrating and dis-integrating, to converge the abilities to see, deceive, and maneuver in windows of superiority, breaking the physical, virtual, and cognitive cohesion of enemy formations and systems leading to their defeat.

E-4. Return to competition

a. Friendly forces consolidate strategic gains and return to competition under favorable military and political conditions. This includes deterring the threat's return to armed conflict and assisting partner forces in restoring order. Protection enables transition back to competition by securing the initiative and maintaining operational contact in all domains, the EMS and the IE.

b. Friendly forces will secure key terrain across the area through security operations to deter escalation back to full armed conflict. Army forces will remove all remaining enemy systems through direct contact, and as the situation permits, control will transition to the host nation. Friendly combat forces redeploy out of the area and police and security units take over. The Army secures the population by resettling displaced persons, identifying and removing SPF, surrogates, criminals, and other irregular actors conducting nefarious activities. Army forces transfer

prisoners and displaced personnel to designated organizations who will process, prosecute, or resettle as required.

c. The Army collaborates with the host nation to repair essential services and mitigate remaining hazards in the area. The force repairs critical infrastructure such as water, sewer, roads, government facilities, and hospitals, to stabilize the region and lower the likelihood of additional armed conflict. Friendly forces establish the rule of law by collaborating with law enforcement organizations, conducting joint policing activities, and removing disruptive forces from the consolidation areas. Friendly forces expand influences in all domains, the EMS, and the IE to control the narrative, reduce the likelihood of return to conflict, and expand capability to quickly respond and preserve CCAAs.

d. The force rapidly builds partner capacity, reconstitutes capability in all domains, and transitions authority to host nations as quickly as possible to consolidate strategic gains under favorable friendly conditions. Combat forces transition to lighter security forces that are quicker to respond to any incident. The presence of U.S. security forces sends a clear message to the enemy to discontinue armed conflict. Security forces control terrain, respond with the appropriate firepower, and integrate other activities to preserve CCAAs, deny enemy freedom of action, and enable unrestricted access.

e. The future force conducts activities to deny enemy freedom of action and to preserve CCAAs. The enemy will continuously attempt to destabilize the region and friendly forces will deter these actions through counter information warfare and counter irregular warfare. Army forces conduct security cooperation activities with host nation and partners to preserve the consolidation and return to competition, and will build up partner capacity through security force assistance.

Appendix F
Protection Considerations of Unique Environments

F-1. Introduction

a. Army forces, as part of the joint force, execute operations globally in all environments. The Army must carefully weigh operational environmental considerations to maximize combat power and ensure mission success. Future enemies will choose to fight in environments that maximize their combat power and/or minimize ours. Future Army forces may operate in non-traditional and/or exotic environments, as technology allows global competitors to expand operational spaces.

b. Executing MDO in unique environments successfully requires three solution components: equipping the force to function in unique environments, training the force to operate in unique environments, and integrating environmental considerations into planning tools and processes at all unit echelons.

(1) Equipping the force. To be successful, the Army must equip Soldiers and units with equipment and vehicles designed and built to withstand the hazards unique to the environments in which they are operating. As each unique environment may require unique fielding, training, and planning solutions, future Army units may require organizational tailoring, with specific modified tables of organization and equipment for units that are force-calibrated or aligned to specific areas.

(2) Training the force. Each encountered environment poses unique protection challenges and risks that require additional specific Soldier and unit training to overcome and mitigate. Soldiers must understand that the environment affects everyone. Soldiers' preparation and training to live and fight in harsh environments beforehand will determine their unit's success or failure.

(3) Planning and executing operations. Each environment poses unique protection challenges for commanders to consider during operational planning and mission execution.

F-2. Dense urban terrain (DUT)

a. The MDO concept specifically highlights the challenges of operating in DUT. Operating in a megacity environment, with all the unique challenges it presents, requires future capabilities that define required materiel solutions and pertinent investment areas allowing the Army to successfully operate in this increasingly complex environment. Currently more than 50 percent of the world's population lives in urban areas and this is likely to increase to 60 percent by 2050, making military operations in cities both inevitable and the norm. Threats operating in DUT may consist of conventional military forces, unconventional militias or guerilla forces, terrorists, criminal organizations or gangs, or opposing political groups. DUT presents challenges such as civil unrest, loss of communications, narrow and/or congested roadways and minimal line of sight. Urban areas vary in terms of population density, construction, culture, and many other factors. The dynamic variety of natural and man-made features in urban areas presents commanders with a multitude of challenges.

b. Protection equipping considerations. Future Army forces operating in DUT require highly specialized equipment given the unique aspects and density of urban terrain and the populations living within it.

(1) Enemy, insurgent, and criminal organizations operating in DUT are likely to capitalize on the complexity of the urban terrain to attack and surprise friendly forces. This complexity will require that future Army forces operating in DUT have optimized sensors and AI-enabled analysis tools that generate 3D data, map interior structures, map and sense subterranean complexes, and analyze urban and adjoining maritime terrain. Future Army forces will require advanced data analysis tools to provide rapid situational assessments and a common operational picture to leaders and Soldiers.

(2) Enemy, insurgent, and criminal organizations operating in DUT are likely to employ unmanned vehicles to conduct intelligence-gathering activities and to attack friendly forces, requiring that future Army forces operating in DUT have the ability to detect, identify, and neutralize UAS and UGV threats.

(3) Future Army forces require specialized equipment to secure and protect DUT maritime space. Watercraft, UASs, UGVs, and unmanned naval surface and subsurface vehicles offer future Army forces the ability to conduct operations more efficiently through remote means, and to preserve combat power by reducing the risk to Soldiers.

(4) Enemy forces operating in DUT often utilize manmade subterranean complexes for convenient weapon caches, bases, and rally points. The dynamic nature of earth movement and the threats associated with confined spaces make DUT subterranean areas extremely dangerous. Future Army forces require optimized UASs and UGVs for subterranean operations in DUT to avoid unnecessary casualties. Future Army forces require specialized communications equipment for operating in subterranean environments. Units deploying to any terrain that supports underground spaces require gas detectors capable of identifying oxygen and carbon monoxide levels. To meet the challenges of a subterranean environment, the Army must find materiel solutions, such as robotics, which enable expedient search, navigation and mapping of the encountered or expected underground environments. Likewise, the use of man-portable lightweight ground sensors, ground penetrating radar or an equivalent capability, and improved aerial terrain imaging and analysis will support identifying subterranean threats. Individual units will need a wide spectrum of advanced sensors to peer through degraded visual environments, breaching tools, communication and navigation systems, and air quality monitors to operate successfully.

(5) Urban environments pose heightened CBRN risks due to the presence of industrial areas and activities. Chemical plants, food processing facilities, manufacturing facilities, and power generation plants all require the usage and storage of commercial hazardous chemicals and other dangerous materials. Future Army forces require real time understanding of the CBRN environment, including the ability to sense, analyze, and communicate situational awareness. Future Army forces require advanced inherent survivability capabilities to protect against CBRN hazards and enemy weapons in DUT. Future Army forces require advanced decontamination and mitigation capabilities to operate within urban environments and protect military forces and civilian populations.

(6) Urban environments present unique challenges to future Army forces in maintaining civilian order and population control. Future Army forces employ UASs, UGVs, and other advanced sensor platforms to detect, identify, and analyze criminal, insurgent, and other threats to civilian order.

(7) Enemy, insurgent, and criminal organizations operating in DUT are likely to employ mines, IEDS, and advanced UAS vehicle-borne IEDs against future Army forces. Stand-off and remote explosive threat detection and neutralization are essential in defeating this threat and mitigating risks to military and civilian forces.

(8) Urban environments present unique challenges for search, rescue, and evacuation of Soldiers and wounded civilians. Injured Soldiers and civilians are likely to be trapped in rubble from large buildings, and high above the ground in damaged skyscrapers, requiring specialized search and rescue equipment, personnel, and evacuation means to locate and extricate them.

c. Protection training considerations. Soldiers and units require specific training in DUT environments prior to deploying to combat operations in them. Units committed to urban operations may have to fight as soon as they arrive in the operational area. Commanders must make the best use of the preparation time available. Advanced simulators are essential in training Soldiers on the unique aspects of fighting in a dense urban environment. Units require training and preparation to conduct tasks in a DUT. Such operations include non-combatant evacuations, humanitarian assistance disaster relief missions, raids, denial of adversary objectives, countering WMD operations, conducting military operation and security cooperation, providing a global stabilizing presence, providing support to civil authorities, counterterrorism and counterinsurgency missions.

d. Protection planning considerations. Successful operations require identifying then mitigating threat capabilities and the variables present in the operational environment. Urban operations often reduce the relative advantage of technological superiority, weapons ranges, and firepower of military units. They have historically demanded large amounts of manpower, are usually more time-intensive, and require more decentralized C2. Moreover, because there is risk of high civilian casualties, commanders must consider protecting civilians, rendering aid, and minimizing damage to infrastructure. Tactically mobile mutually supporting units are critical to success in complex urban terrain. Having cyber and information operations support to monitor social media is essential to understanding civil populations. Likewise, understanding the socio-economic and political standing of a given region helps commanders with forward planning in anticipation of potential outside nation support.

F-3. Jungle environments (FM 90-5)

a. Jungles in various forms are common in tropical areas, mainly Southeast Asia, Africa, and Latin America. Jungle environments pose unique challenges to protecting Soldiers and equipment. Jungle environments include hot and cold weather extremes; wet monsoons and dry seasons; insects, leeches, snakes, and other dangerous wildlife; malaria and other tropical diseases; and poisonous vegetation. Jungles also offer unique opportunities for cover and concealment to protect forces operating within them.

b. Protection equipping considerations.

(1) Future Army forces operating in jungle environments are likely to be most successful when designed to be light and airmobile. Clothing and equipment designed for jungle environments should be lighter and faster to dry and should provide excellent ventilation. Soldiers utilize insect repellent and mosquito netting to mitigate the risks of insect-borne disease. Night vision devices, multispectral sensors, and ground sensors are likely very effective in detecting threats, while visual-spectrum video capture devices are less likely to be effective given the enhanced cover and concealment offered by the terrain and local biology. Wet and marshy soil and terrain seriously impair heavy armored vehicle mobility making their usefulness in the jungle environment questionable.

(2) Enemy forces operating in jungle environments often utilize natural and manmade subterranean complexes for convenient weapon caches, patrol bases, and rally points. The

dynamic nature of earth movement and the threats associated with confined spaces make jungle subterranean areas extremely dangerous. Future Army forces require optimized UASs and UGVs for subterranean operations in jungle environments to avoid unnecessary casualties. Future Army forces require specialized communications equipment for operating in subterranean environments. Units deploying to any terrain that supports underground spaces require gas detectors capable of identifying oxygen and carbon monoxide levels.

c. Protection training considerations. Soldiers and units require specific training in jungle environments prior to deploying to combat operations in them. Units committed to jungle operations may have to fight as soon as they arrive. Commanders must make the best use of the preparation time available. The first priority in preparation for jungle warfare is acclimation. Troops not conditioned properly will not perform jungle warfare tasks reliably. Swimming is also a vital skill for the jungle fighter. Falling into a jungle pool or river can be a dangerous experience, especially for a non-swimmer. Training to conceal Soldiers and equipment from ground and air observation is equally important and will help to make up for an enemy's superior knowledge of the jungle area. Training must emphasize small unit tactics and operations with Army aviation. Since night operations, especially ambushes, are common in jungle fighting, units must emphasize night training. Advanced simulators are essential in training Soldiers on the unique aspects of fighting in a jungle environment.

d. Protection planning considerations. Much of a conventional jungle enemy's effectiveness depends on familiarity with the terrain. In general, this means that forces native to a battlefield area will be more effective than forces from outside. Even if these outside forces have a greater amount of firepower than the native forces, the lack of terrain familiarity may limit their ability to use that firepower. The thick foliage and rugged terrain of most jungles limit fields of fire and speed of movement. Lack of line of sight and clearance may prevent visual contact between units, and hinder direct and indirect fires support.

F-4. Desert environments (FM 90-3)

a. Arid regions make up about one-third of the earth's land surface, more than any other type of climate. Desert operations demand adaptation to the environment and to the limitations imposed by terrain and climate. Environmental effects on personnel, equipment, and tactics because of extreme temperature variance, wind conditions, lack of natural water sources, and terrain features characteristic of a dry, barren landscape require special consideration before operating in desert environments. Success depends on an appreciation of the physical and/or psychological effects of arid conditions on Soldiers, equipment, facilities, and operations.

b. Protection equipping considerations. Future Army forces employed in desert environments are most likely to be successful when designed for high mobility. Optimization in desert environments requires highly maneuverable aviation, armored, and wheeled formations that can target, attack, and fight deep operations simultaneously.

(1) Desert environments pose unique challenges to future Army forces. Equipment requires adaption to a dusty, rugged landscape where temperatures vary from extreme highs to freezing lows and where visibility can change from 30 miles to 30 feet in a matter of minutes.

(2) The lack of water is the most important single characteristic of the desert. Future Army forces operating in desert environments require advanced water conservation capabilities and water point production and purification capabilities to protect Soldiers and maximize combat power.

(3) Conditions in arid environments can damage military equipment and facilities. Future Army forces require equipment designed to counter the effects of temperature, dryness, and dust. Vehicles, aircraft, sensors, and weapons are all affected. Rubber components such as gaskets and seals become brittle, and oil leaks are more frequent.

(4) Future Army forces require an integrated network architecture that collects sensor data; conducts large data analysis utilizing AI-enabled algorithms, and provides a cogent and real-time common operational picture to formations and headquarters.

c. Protection training considerations. Soldiers and units require specific training in desert environments prior to deploying to combat operations in them. Units sent to desert operations may have to fight as soon as they arrive. Commanders must make the best use of the preparation time available. The first priority in preparation for desert warfare is acclimation. Troops not conditioned properly will not perform desert warfare tasks reliably. Training to conceal Soldiers and equipment from ground and air observation is important, given the lack of natural cover and concealment in desert environments. Individuals require training on hot and cold weather injuries, hygiene and sanitation, and insect borne disease prevention. Individual and unit level training for desert environments should include first aid; driver; SERE; continuous field training; navigation; and specific technical aptitudes required for specific tools and mission sets in this unique environment. Advanced simulators are essential in training Soldiers on the unique aspects of fighting in a desert environment.

d. Protection planning considerations. Knowing how the desert environment affects tactical, offensive and defensive operations will aid commanders in the decision-making process. Mobility and logistics are critical to success in the desert. Commanders make protection decisions based on terrain data gathered when using the IPB process to help mitigate threats. Understanding and planning for the geography, weather and its effects on troops and equipment are essential. Cover and concealment are generally scarce in the desert, making enemy air attack and reconnaissance very effective. Maximizing natural and man-made obstacles to hinder enemy cross-country movement is critical, and sandy soil is optimal for employing terrain-shaping obstacles.

F-5. Maritime environments

a. Maritime space, littorals and waterways include oceans or seas, large lakes, and major rivers. In 2013, more than 80 percent of the world's population lived within 60 miles of a coast, while 75 percent of large cities were on a coastline. Maritime environments provide key friendly and threat avenues of approach or essential lines of communications for urban areas that border these large bodies of water. As part of the joint force, Army Soldiers and units are likely to employ to support Navy and Marine forces conducting maritime operations. Maritime environments that future Army forces are likely to be employed in include coastal cities and ports, aboard naval vessels

during fires support operations, conducting aviation missions or in other capacities utilizing Army vehicles and equipment, conducting Army watercraft operations; supporting riverine operations, in support of or sustaining amphibious operations in littorals and ashore, ashore as part of a multi-domain task force providing fires and protection to the joint force, and on beaches supporting sustainment and joint logistics over-the-shore operations.

b. Protection equipping considerations. Maritime environments pose unique challenges to Army equipment and vehicles. The combination of moisture, oxygen and salt, especially sodium chloride, damages metal worse than rust does. Saltwater corrodes metal five times faster than fresh water does and the salty, humid ocean air causes metal to corrode 10 times faster than air with normal humidity.

c. Protection training considerations. Army forces working in the maritime environment require specific training prior to deployment. Army units should train in a joint environment alongside both Marine and Navy personnel to simulate real world operations. Understanding the communication paths and requirements of air and naval gunfire support will allow Army units to effectively call for fire or otherwise utilize the naval assets available in a joint environment. Future Army forces require additional training on water survival and unit-specific training in joint logistics over-the-shore, emphasizing training on joint interfaces for various systems or technologies used to achieve both the distribution of supplies and equipment as well as those systems used for joint C3. The Navy or Marines may provide specific training when working as part of a Joint task force. Advanced simulators are essential in training Soldiers on the unique aspects of fighting in a maritime environment.

d. Protection planning considerations. MDO calls for Army forces to be able to operate across all domains and environments. Effective Joint support and operations will be a staple of MDO. Ensuring troops and units are prepared for joint level training and operations aboard a ship or shoreline will enhance overall confidence in their ability to complete the mission in an unfamiliar environment. Future Army forces operating in a maritime environment with JIIM partners require the ability to share information and integrate with their C2 systems. To facilitate this function, future Army forces require specialized or dedicated equipment, specially trained Soldiers, and specially modified organized units (such as the MDTF) optimized for maritime operations and JIIM integration.

F-6. Mountainous and cold weather environments (ATP 3-90.97)

a. Mountainous regions are located throughout the world. Additionally, based upon projections of the opening of Arctic shipping lanes due to climate change, the likelihood increases for potential cold weather operations in the Arctic. When conducting military operations in mountains or cold weather environments, leaders and Soldiers must plan to fight both the environment and the opposing force. Despite the difficulties that mountains and cold weather pose, there are armies that can conduct large-scale, sustained operations in them. In contrast, few U.S. military units or personnel have trained extensively in mountain and cold weather operations. While a mountainous environment is challenging, expeditionary forces operate effectively with proper training, equipment, and organization. Given the highly specialized nature of operations in mountainous

and cold weather environments, future Army forces are likely to require dedicated mountain and Arctic-focused organizations.

b. Protection equipping considerations. Future Army forces operating in mountainous and cold weather environments are likely to be most successful when designed to be light and airmobile. Assault support aircraft are essential to rapid movement of forces and equipment in the mountains. Terrain, infrastructure, and weather hamper armored and Stryker operations in complex and compartmentalized terrain. Narrow roads and movement corridors will limit vehicle traffic to predictable patterns. Generally, mountainous terrain above the valley floor limits movement of wheeled vehicles and is too restricted for tracked vehicles.

(1) In cold weather, special equipment requirements include snowshoes, boot crampons, avalanche beacons, avalanche probes, skis, skins, ski wax, backpacking stove and fuel, candles, ice axes, snow shovels, matches, 100 percent ultraviolet protection glacier glasses, sunscreen, special fuel containers, tire chains, and winterization kits.

(2) Future Army forces require specialized vehicles and equipment for personnel to maximize combat power in mountainous and cold weather environments. In cold weather, preferred clothing consists of loose-fitting layers and insulated clothing designed to wick away moisture and ensure perspiration does not accumulate close to the body. Economizing the individual combat load is essential for conducting dismounted operations in the mountains. Lighter weight ammunition and body armor, and lightweight water purification equipment, are essential to reducing individual loads. Improved sustainment utilizing UASs during operations can further reduce individual loads. Casualty evacuation in the mountains is resource-intensive in manpower, equipment, and time. UASs have the potential to greatly improve casualty evacuation times in mountainous and cold weather environments.

(3) In a mountainous environment, the terrain favors the enemy's use of mines and IEDs as standalone weapons and in the initiation of ambushes. In the mountains, using mechanical mine plows and rollers or other standard route clearance vehicles, such as the vehicle mounted mine detection system (Husky) and mine protected clearance vehicle (Buffalo) is frequently impossible due to the lack of roads and trails and the low trafficability of those that do exist. Future Army forces require lightweight and Soldier-borne mine detectors, UASs, and UGVs to conduct counter-IED and mobility operations in mountainous and cold weather environments.

(4) Mountains present natural and manmade subterranean complexes for convenient weapon caches, patrol bases, and rally points. The dynamic nature of earth movement and the threats associated with confined spaces make mountainous subterranean areas extremely dangerous. Future Army forces require optimized UASs and UGVs for subterranean operations in mountainous and cold weather environments to avoid unnecessary casualties. Future Army forces require specialized communications equipment for operating in subterranean mountainous environments. Units deploying to any terrain that supports underground spaces require gas detectors capable of identifying oxygen and carbon monoxide levels.

c. Protection training considerations. Individual and collective unit mountain and cold weather training is essential prior to conducting operations in these environments. Commanders will make

every effort to maximize the training capabilities of the Army Mountain Warfare School, the Northern Warfare Training Center, and the Marine Corps Mountain Warfare Training Center in order to enhance the units' warfighting capability in these challenging environments. Advanced simulators are essential in training Soldiers on the unique aspects of fighting in a mountainous and cold weather environment.

d. Protection planning considerations. Operating and maneuvering in a mountainous environment requires centralized planning and decentralized execution. The dispersion of forces is useful when conducting offensive, defensive, and stability operations in the mountains. Information collection planning in mountainous areas must consider an increased reliance on aerial collection assets and degraded target acquisition and early warning and collection capabilities of intelligence systems. In harsh mountainous terrain or cold weather environments, time is a greater planning factor for troop movements. Compartmentalized terrain, expansive areas of operation and severe environmental conditions limit communications systems and challenge C2. Leaders consider and mitigate significant environmental impacts to ensure command post nodes remain functional despite cold temperatures, high winds, and the effects of altitude.

F-7. CBRN environments (JP 3-11)

a. The end state of implementing CBRN defense measures is to provide the best possible protection against CBRN threats and hazards, to improve survivability by avoiding contamination, to continue the mission, and to reestablish the readiness of forces. The CBRN environment includes CBRN threats and hazards and their potential effects on operations. These effects are the result of intentional or unintentional releases of CBRN materials. Chemical hazards include any toxic chemical manufactured, used, transported, or stored that can cause death or other harm through exposure. Biological hazards include any organism or substance derived from an organism that poses a threat to the health of any living organism. Radiological hazards include ionizing radiation that can cause damage, injury, or destruction from either external irradiation or radiation from radioactive materials within the body. Nuclear hazards are those dangers associated with the overpressure, thermal, and radiation effects from a nuclear explosion.

b. Protection equipping considerations. Future Army forces require equipment to protect against CRBN threats and hazards to include protective suits and masks for individual Soldiers, vehicles with designed or additive CBRN protection capabilities, field facilities such as tents and command posts with designed or additive CBRN protection capabilities, detection and warning equipment integrated with communications systems, CBRN decontamination systems, and CBRN medical treatment capabilities.

c. Protection training considerations. Soldiers and units must train to proficiency on CBRN-related tasks in replicated CBRN environments. Advanced simulators are essential in training Soldiers on the unique aspects of fighting in a CBRN environment.

d. Protection planning considerations. Future Army forces require CBRN staff organizations and units that can characterize the CBRN hazard; develop a clear understanding of the current and anticipated CBRN situations; and collect and assimilate information from intelligence, health, and specific CBRN reconnaissance and surveillance sources in near real time.

F-8. Space and non-terrestrial environments

a. Army forces utilize the space domain to facilitate command, control, communication, computers, cyber, intelligence, surveillance, and reconnaissance functions. Satellites collect data, facilitate communications, enable navigation, and support meteorology. Future Army forces may participate more extensively in the space environment as technology allows.

b. Protection equipping considerations. There are no current plans to employ Army soldiers in space. The space environment is unlike any earth environment, as it is inherently deadly to any living organism not protected within an artificial terrestrial environment. Future Army forces, if required to operate in space, would require protections against radiation, exposure to vacuum, and the myriad effects on the human body from lack of gravity.

c. Protection training considerations. There are no current plans to employ Army Soldiers in space. Future Army forces, should they be required to operate in space, would require advanced simulators for training Soldiers on the unique aspects of fighting in a space environment.

d. Protection planning considerations. Future Army forces operating in a space environment with JIIM partner capabilities would require the ability to share information and integrate with their C2 systems. To facilitate this function, future Army forces require specialized or dedicated equipment, Soldiers, or even units.

Glossary

Section I
Abbreviations

2D	two dimensional
3D	three dimensional
A2	antiaccess
AC-P	Army Futures Command Concept for Protection
AD	area denial
ADP	Army doctrine publication
AFC	Army Futures Command
AHS	Army health system
AI	artificial intelligence
AMD	air and missile defense
AME	Army modernization enterprise
AML	adversarial machine learning
AOC	Army operating concept
APP	Army protection program
APS	Army pre-positioned stock
AR	Army regulation
ARSOF	Army special operation forces

BCT	brigade combat team
C2	command and control
CA	civil affairs
CBRN	chemical, biological, radiological, nuclear
CBRN R&S	chemical, biological, radiological, nuclear reconnaissance and surveillance
CCAA	critical capabilities, assets, and activities
CCIR	commander's critical information requirements
CEMA	cyberspace electromagnetic activities
CFT	cross-functional team
CI	counterintelligence
CONUS	continental United States
COP	common operational picture
COSC	combat and operational stress control
CP	command post
CUAS	counter unmanned aircraft system
CWMD	counter weapon of mass destruction
DCA	defensive counter air
DEW	directed energy weapon
DIMEFIL	diplomatic, informational, military, economic, financial, intelligence, and legal
DOD	Department of Defense
DODD	Department of Defense Directive
DODIN-A	Department of Defense Information Network-Army
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy
DSCA	defense support of civil authorities
DUT	dense urban terrain
EA	electromagnetic attack
EAB	echelons above brigade
EABC	Echelons Above Brigade Concept
EEFI	essential element of friendly information
EMP	electromagnetic pulse
EMS	electromagnetic spectrum
EO	electro-optical
EOD	explosive ordnance disposal
EW	electromagnetic warfare
FCC	Futures and Concepts Center
FHP	force health protection
FM	field manual
GMD	ground-based midcourse defense
GPS	global positioning system
HAU	hazard awareness and understanding
HSI	hyperspectral imaging
HSS	health service support
IADS	integrated air defense system
IE	information environment

IED	improvised explosive device
IPB	intelligence preparation of the battlefield
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
IW	irregular warfare
IWar	information warfare
JIIM	joint, interagency, intergovernmental, multinational
JOA	joint operating area
JOES	joint operating ecosystem
JP	joint publication
LIDAR	light detection and ranging
LOC	lines of communication
LSCO	large-scale combat operation
MDCOP	multi-domain common operational picture
MDMP	military decision-making process
MDO	multi-domain operations
MDTF	multi-domain task force
MILDEC	military deception
ML	machine learning
MP	military police
MSI	multispectral imaging
NAVWAR	navigation warfare
OE	operational environment
OPSEC	operations security
PIO	police intelligence operations
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
PNT	positioning, navigation, and timing
PPE	personal protective equipment
PTSD	post-traumatic stress disorder
RADAR	radio detection and ranging
RAS	robotic and autonomous systems
RC	required capability
RF	radio frequency
SA	situational awareness
SAR	synthetic aperture radar
SERE	survival evasion resistance escape
SOF	special operations forces
SOJTF	special operations joint task force
SPF	special purpose forces
SSA	strategic support area
SWaP	size, weight, and power
TP	U.S. Army Training and Doctrine Command pamphlet
TSOC	theater special operations command
UAS	unmanned aircraft system
UGV	unmanned ground vehicle

U.S.	United States
USA	U.S. Army
WfF	warfighting function
WMD	weapon of mass destruction
WME	weapon of mass effect

Section II
Terms

active defense
The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy. (JP3-60)

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. (TP 525-3-3 and adapted from ADP 6-22 mental agility description)

air domain
The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible. (JP 3-30)

antiaccess
Action, activity, or capability, usually long-range, designed to prevent an advancing enemy force from entering an operational area. Also called **A2**. (JP 3-0)

area denial
Action, activity, or capability, usually short-range, designed to limit an enemy force's freedom of action within an operational area. Also called **AD**. (JP 3-0)

area of influence
A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. (JP 3-0)

area of interest
That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. (JP 3-0)

area of operations
Operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. (JP 3-0)

area of responsibility
Geographical area associated with a combatant command within which a geographic combatant commander has authority to plan and conduct operations. (JP 1)

area security
A security task conducted to protect friendly forces, installations, routes, and actions within a specific area. (ADP 3-0)

armed conflict
When the use of violence is the primary means by which an actor seeks to satisfy its interests. (JCIC)

Army design methodology
Applying critical and creative thinking to understand, visualize, and describe unfamiliar problems and approaches to solving them. (ADP 5-0)

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

attack
An offensive task that destroys or defeats enemy forces, seizes and secures terrain, or both. (FM 3-0)

authority
Delegated power to judge, act, or command. (ADP 3-0)

battlefield
The area where military operations are conducted to achieve military goals consisting of all 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, and terrain within the operational areas and areas of interest. (TP 525-3-1)

biometrics
Process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 2-0)

boundary
A line that delineates surface areas for the purpose of facilitating coordination and de-confliction of operations between adjacent units, formations, or areas. (JP 3-0)

calibrated force posture
The combination of position and the 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. (TP 525-3-1)

campaign
Series of related major operations aimed at accomplishing strategic or operational objectives within a given time and space. (JP 5-0)

capabilities development
Identifying, assessing, and documenting changes in DOTMLPF that collectively produce the force capabilities and attributes prescribed in approved concepts, concept of operations, or other authoritative sources. (TP 71-20-3)

capability
Ability to achieve a desired effect under specified standards and conditions through a combination of means and ways across DOTMLPF to perform a set of tasks to execute a specified course of action. (DODD 7045.20)

capacity
Capability with sufficient scale to accomplish the mission; actual or potential ability to perform. (TP 525-3-1)

center of gravity
The source of power that provides moral or physical strength, freedom of action, or the will to act. (JP 5-0)

close area
Where friendly and enemy formations, forces, and systems are in imminent physical contact and contest for control of physical space in support of campaign objectives. (TP 525-3-1)

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

combatant command
Unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. (JP 1-0)

combined arms
Synchronized and simultaneous application of all elements of combat power that together achieve an effect greater than if each element was used separately or sequentially. (ADP 3-0)

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)

competition
Exists when two or more actors in the international system have incompatible interests but neither seeks to escalate to open armed conflict. While violence is not the adversary's primary instrument in competition, challenges may include a range of violent instruments including conventional forces with uncertain attribution to the state sponsor. (JCIC)

complex terrain
Geographical area consisting of an urban center larger than a village and/or of two or more types of restrictive terrain or environmental conditions occupying the same space. Restrictive terrain or environmental conditions include, but are not limited to, slope, high altitude, forestation, severe weather, and urbanization. (ATP 3-34.80)

conduct
Direct or take part in the operation or management of an organization, unit, mission, task, or activity. (Adapted from TP 350-70-1 definition.)

consolidate gains
Activities to make enduring any temporary operational success and set the conditions for a stable environment allowing for a transition of control to legitimate authorities. (ADP 3-0)

consolidation
The organizing and strengthening of a newly captured position so that it can be used against the enemy. (FM 3-90-1)

contested spaces
Those areas where U.S., allied, or coalition forces can challenge the adversary's denial measures, maintain some degree of friendly freedom of action, and potentially deny adversary freedom of action. (TP 525-3-1)

control
The regulation of forces and warfighting functions to accomplish the mission in accordance with the commander's intent. (ADP 3-0)

control measure
A means of regulating forces or warfighting functions. (ADP 3-0)

conventional forces
Forces capable of conducting operations using nonnuclear weapons and forces other than designated special operations forces. (JP 3-05)

convergence
Rapid and continuous integration of capabilities in all domains that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative. (TP 525-3-1)

course of action
Scheme developed to accomplish a mission. (JP 5-0)

critical capabilities, assets, and activities*
Mission and objective-related readiness, force projection, combat power and formations, access to spaces, decisive points and connections, assets, facilities, information, understanding, infrastructure (not all inclusive) e.g., those things a commander deems essential to mission assurance (performing missions or achieving objectives).

cross-domain
Having an effect from one domain into another. (TP 525-3-1)

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 EMS, and the IE. Cross-domain maneuver creates synergistic effects in the physical, temporal, virtual, and cognitive realms that increase relative combat power and provide the overmatch necessary to destroy or defeat enemy forces, control land areas and resources, and protect populations. (The U.S. Army Concept for Brigade Combat Team Cross-Domain Maneuver 2028)

cross-domain synergy
The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others – to establish superiority in some combination of domains that will provide the freedom of action required by the mission. (Capstone Concept for Joint Operations, JOAC)

cyberspace
A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

cyberspace operations
Employment of cyberspace capabilities where the primary purpose is to achieve military objectives in or through cyberspace. (JP 3-0)

data
Unprocessed signals communicated between any nodes in an information system, or sensing from the environment detected by a collector of any kind. (ADP 3-0)

decisive operation
The operation that directly accomplishes the mission. (ADP 3-0)

decisive point
A geographic place, specific key event, critical factor, or function that, when acted upon, allows commanders to gain a marked advantage over an adversary or contribute materially to achieving the operation's purpose. (JP 5-0)

decisive space
Conceptual geographic and temporal location 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. (TP 525-3-1)

deep fires areas
Areas beyond the feasible range of movement for conventional forces, but where joint fires, SOF, information, and virtual capabilities can be employed. (TP 525-3-1)

deep maneuver area
Area where maneuver forces can go (beyond the close area) but is so contested that maneuver still requires significant allocation and convergence of multi-domain capabilities. (TP 525-3-1)

defensive cyberspace operations
Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 3-12)

denied spaces
Areas where the adversary can severely constrain U.S. and allied forces' freedom of action through A2/AD and other measures. (TP 525-3-1)

dense urban terrain
Areas characterized by extraordinarily closely-packed manmade infrastructure and high population density, potentially including concentrations of high-rise buildings, subterranean features, and densely packed slums. (TP 525-3-1)

depth
The extension of operations in time, space, or purpose, to achieve definitive results. (ADP 3-0)

destroy
Tactical mission task that physically renders an enemy force combat-ineffective until it is reconstituted. Alternatively, to destroy a combat system is to damage it so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt. (FM 3-90-1)

deterrence
The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits. (JP 3-0)

directed energy
Umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. (JP 3-85)

disciplined initiative
Duty and willingness to act in the absence of orders, when existing orders no longer fit the situation, or when unforeseen opportunities or threats arise. (ADP 3-0)

dispersion
Deliberate or accidental reaction to enemy or 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. (TP 525-3-1)

dis-integrate
Break the coherence of the enemy's system by destroying or disrupting its subcomponents (such as command and control means, intelligence 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. (TP 525-3-1)

domain
Area of activity within the operational environment (land, air, maritime, space, and cyberspace) in which operations are organized and conducted. (TP 525-3-1)

electromagnetic spectrum
The range of frequencies of electromagnetic radiation from zero to infinity. For convenience the DOD divides into 26 alphabetically designated bands. (AR 5-12)

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)

end state
Set of required conditions that defines achievement of the commander’s objectives. (JP 3-0)

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

engagement
The combination of physical, informational, and psychological actions taken to build relationships or influence actors' decision making (moral and mental). (TP 525-3-1)

expeditionary
Ability to deploy task-organized forces on short notice to austere locations, capable of conducting operations immediately upon arrival. (TP 525-3-1)

expeditionary force
An armed force organized to achieve a specific objective in a foreign country. (JP 3-0)

expeditionary forensics*
The multi-disciplinary, scientific process to generate knowledge and promote understanding of crimes, hazards, and threat organizations, capabilities, and methods gained through the collection, exploitation, and reporting of forensic material during multi-domain operations. (Army Expeditionary Forensics in 2028-2040 White Paper)

exploitation
Taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already created. (JP 2-01.3)

fait accompli
A type of attack intended to achieve military and political objectives rapidly, quickly consolidating gains, so any attempt to reverse the action would entail unacceptable cost and risk. (TP 525-3-1)

hyperactive
More active than usual or desirable; hyper-competitive during competition and hyper-violent in armed conflict. (TP 525-3-1)

information environment
The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (TP 525-3-1)

information operations
Integrated employment, during military operations, of information related capabilities (IRC) in concert with other lines of operation to influence, deceive, disrupt, corrupt, or usurp the decision making of enemies and adversaries while protecting our own. (JP 3-85)

information warfare
Employing information capabilities in a deliberate disinformation campaign supported by actions of the intelligence organizations designed to confuse the enemy and achieve strategic objectives at minimal cost. (TP 525-3-1)

intelligence, surveillance, and reconnaissance
An integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. Also called ISR. (JP 2-01)

intent
Leader's clear, concise, and personal expression of the end state that describes the desired conditions of the friendly force in relationship to the enemy, terrain, or civil considerations. The intent provides focus and helps subordinates and supporting leaders act to achieve the desired results without further direction, even when the plan does not unfold as designed. (JP 3-0)

interoperability
Ability of two or more organizations to operate together effectively and efficiently as an integrated team to accomplish a common goal. Interoperability includes human, procedural, and technical considerations. (TP 525-3-3 and adapted from JP 3-0 and JP 6-0 definitions, and NATO Pub 06)

irregular warfare
A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Also called IW. (JP 1) [Note: Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, to erode an adversary's power, influence, and will.] (TP 525-3-1)

isolate
Tactical mission task that requires a unit to seal off—both physically and psychologically—an enemy from sources of support, deny the enemy freedom of movement, and prevent the isolated enemy force from having contact with other enemy forces. (FM 3-90-1)

kinetic
A weapon (action or capability) that after transiting to a designated target employs the dynamic transfer of energy (chemical, explosive, lethal, nonlethal effects) to defeat, destroy, or incapacitate personnel, platforms, and systems. (The U.S. Army Concept for Brigade Combat Team Cross-Domain Maneuver 2028)

land domain
The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals. (JP 3-31)

lethal
A weapon (or capability) that is explicitly designed and employed to produce effects that result in great harm, death, or destruction in designated targets within acceptable levels of collateral damage to property, personnel, and the environment. (The U.S. Army Concept for Brigade Combat Team Cross-Domain Maneuver 2028)

littoral
The littoral comprises two segments of the operational environment: 1. Seaward: the area from the open ocean to the shore, which must be controlled to support operations ashore. 2. Landward: the area inland from the shore that can be supported and defended directly from the sea. (JP 2-01.3)

major operation
Series of tactical actions (battles, engagements, strikes) conducted by combat forces of a single or several services, coordinated in time and place, to achieve strategic or operational objectives in an operational area. (JP 3-0)

maneuver
Employment of forces in the operational area through movement in combination with fires to achieve a position of advantage with respect to the enemy. (JP 3-0)

maritime domain
The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. (JP 3-32)

mesh
To connect devices directly, dynamically, and non-hierarchically to as many other devices as possible allowing them to relay critical data without interruption and cooperate, self-organize, and self-configure to accomplish tasks collectively despite individual device degradation or destruction. (TP525-3-8)

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)

multi-domain
Dealing with more than one domain at the same time. (TP 525-3-1)

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. (TP 525-3-1)

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. (TP 525-3-1)

near-peer adversaries
Nation states with the intent, capabilities, and capacity to contest U.S. interests globally in most or all domains and environments. (TP 525-3-1)

neutral
Party identified as neither supporting nor opposing friendly, adversary, or enemy forces. (ADP 3-0)

neutralize
A tactical mission task that results in rendering enemy personnel or materiel incapable of interfering with a particular operation. (FM 3-90-1)

nonkinetic
A weapon (action or capability) that generates negative systematic effects to personnel, platforms, or system(s) remotely that degrades, disrupts, defeats, or incapacitates the designated target. (The U.S. Army Concept for Brigade Combat Team Cross-Domain Maneuver 2028)

nonlethal
A weapon (or capability) that is explicitly designed and primarily employed to produce effects that are intended to incapacitate or redirect personnel or materiel from interfering with military operations, while minimizing fatalities, permanent injury to personnel, and undesired damage or disruption to activities, property and the environment. (The U.S. Army Concept for Brigade Combat Team Cross-Domain Maneuver 2028)

nonlethal effects
Effects that limit collateral damage, reduce risk to civilians, and may reduce opportunities for enemy or adversary propaganda. They may also reduce the number of casualties associated with excessive use of force, limit reconstruction costs, and maintain the good will of the local populace. In addition, effects in non-physical domains that are likely to not result in death. (JP3-0)

offensive cyberspace operations
Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 3-12)

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

operational maneuver
Maneuver that supports operational level objectives; usually occurs within a theater of operations (intra-theater). (TP 525-3-1)

operational reach
Distance and duration across which a joint force can successfully employ military capabilities. (JP 3-0)

operational support area
The area of responsibility from which most of the air and maritime capabilities derive their source of power, control, and sustainment as well as where ground forces enter theater, organize, and prepare for rapid onward movement and integration. (TP 525-3-1)

operations security
Process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. (JP 3-13.3)

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. (TP 525-3-1)

passive defense
Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative. (JP 3-60)

planning
Art and science of understanding a situation, envisioning a desired end future, and laying out effective ways of bringing that future about. (ADP 5-0)

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.

protection warfighting function
The related tasks and systems that preserve the force so the commander can apply maximum combat power to accomplish the mission. (ADP 3-0)

reset
A set of actions to restore equipment to a desired level of combat capability commensurate with a unit's future mission. (JP 4-0)

resilience
The ability for Army formations and systems at all echelons to operate in contested spaces against a capable adversary. (TP 525-3-1)

shaping operation
An operation that establishes conditions for the decisive operation through effects on the enemy, other actors, and the terrain. (ADP 3-0)

special operations
Operations requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk. (JP 3-05)

special operations joint task force
A SOJTF is a deployable, JTF-capable, headquarters that supports joint all domain operations and Army MDO. The SOJTF can be tailored for a range of operations from crisis response or limited contingency during competition to a joint force special operations component command (JFSOCC) for armed conflict. In future competition, the SOJTF could have a role in serving as an integrating headquarters for specific whole of government solutions designed to accomplish campaign plan objectives. (JP 3-05)

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. (TP 525-3-1)

strategic maneuver
Maneuver that supports strategic level objectives; usually occurs across more than one theater of operations (inter-theater) (TP 525-3-1)

strategic support area
Area of cross-combatant command coordination, strategic sea and air lines of communications, and the homeland. (TP 525-3-1)

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

system
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. (TP 525-3-3)

tactical support area
Area that directly enables decisive tactical operations in the close area and extension of capabilities into the deep maneuver and deep fires areas. (TP 525-3-1)

taggant
A nonreactive substance added to an explosive that may be traced if the explosive is used for unlawful purposes.

targeting
Process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

threat
Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADP 3-0)

unconventional warfare
Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area. Also called UW. (JP 3-05.1)

warfighting function
A group of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives. (ADP 3-0)

weapons of mass destruction
Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. Also called WMD. (JP 3-40)

weapons of mass effect*
Nonlethal or nondestructive weapons capable of a high order effect causing grave infrastructural, psychological, and economic damage at any point along the competition continuum and across the battlefield to achieve physical, cognitive, virtual or temporal positions of advantage.

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. (TP 525-3-1)

Section III
Special terms
N/A

* Proposed definition