Army Futures Command Concept for Special Operations 2028

18 September 2020

This page intentionally left blank

Foreword

From the Director
U.S. Army Futures Command Futures and Concepts Center

Our near-peer competitors, leveraging emerging trends in science, technology, and the information environment, have invested in strategies and capabilities to challenge the U.S. and remake the global order. They employ innovative approaches to contest U.S. and allies' interests in all domains, the electromagnetic spectrum, and information environment. They often seek to attain their goals through ambiguous actions taken below the threshold of armed conflict. In armed conflict, advances in weapons technology, sensors, communications, and information processing allow these adversaries to generate stand-off intended to separate the joint force in time, space, and function. To address these challenges and fulfill the U.S. Army's landpower roles in protecting the Nation and securing its vital interests, the Army is adapting the way it organizes, trains, educates, mans, and equips to fight these future threats structured around the Multi-Domain Operations (MDO) concept.

Throughout the competition continuum, Army Special Operations Forces (ARSOF) support MDO by providing unique capabilities to advance partnerships, influence adversarial behavior, execute special operations, and respond to crisis. ARSOF provide unique modes of employment, tactical techniques, equipment, and training often conducted in hostile, denied, or politically sensitive environments and characterized by time sensitivity, the need for clandestineness, operating in low visibility, conducting operations with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk. Additionally, ARSOF's geographically calibrated force posture provides the capability to quickly understand the operational environment and wield influence through persistent relationships with local partner forces, resident populations, government institutions, and interorganizational partners to leverage military and civilian networks that improve real-time situational understanding, amplify operational effects, and disrupt an adversary's communication capabilities and decision-making process.

This concept describes the key challenges, solutions, and supporting capabilities required to enable ARSOF to support MDO across the competition continuum against near-peer competitors to accomplish campaign objectives and protect U.S. national interests. It serves as a basis for modernization actions for ARSOF organizations and capabilities. This concept also identifies implications for other supporting and enabling functions. It will inform development of other concepts, experimentation, capabilities development activities, and other future force modernization efforts to achieve the MDO AimPoint Force.

EDMOND M. BROWN
Brigadier General, U.S. Army
Acting Director, Futures and
Concepts Center

This page intentionally left blank

Preface

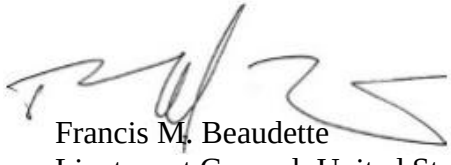
From the Commanding General
U. S. Army Special Operations Command

We live in a world where our adversaries weaponize information and technology at speed against us. They intend to isolate the U.S. from our partners and offset the joint force's ability to integrate capabilities and project power globally. Strategic competitors like Russia and China blur the distinction between peace and war. They do so below the threshold of armed conflict, contesting our advantage and national interests while provoking dissent and challenging the international order. The Army's Multi-Domain Operations (MDO) concept describes how U.S. Army forces, as part of the Joint Force, will militarily contend with our adversaries in the future across all domains.

The Army Special Operations Forces (ARSOF) operating concept integrates ARSOF into MDO. Our ARSOF Women and Men will mitigate risk and deter armed conflict by capitalizing on our strengths and skills: building partner capacity, advancing relationships, and countering malign influences. If deterrence fails, we are the initial crisis response force who will take the fight to our enemies. Our unique capabilities combined with our forward physical and virtual presence provide a natural transition to Large Scale Combat Operations. We will prevail and we will consolidate gains to deny the enemy's ability to prolong conflict and spoil peace.

Our great Nation demands much from us. It will undoubtedly continue to do so in the future as we work with the Army and the Joint Force to solve our country's most challenging military problems. ARSOF must posture for competition while building the capability and capacity to infiltrate, sustain, and maneuver across all domains. If our adversaries' cross the threshold of armed conflict, we will be the first to answer the Nation's call in the most demanding, complex, and uncertain environments imaginable. Now is the time for ARSOF to sharpen our competitive edge as we prepare for the scale, tempo, lethality, and complexity of the multi-domain battlefield beyond 2028.

ARSOF will be a vital component of multi-domain operations. The stakes are high and the sacrifices can be steep. Regardless of the conditions, it is our sacred oath to provide the Nation with the world's most capable special operations forces. The Army Futures Command Concept for Special Operations, 2028 is the initial Army concept focused on special operations. This concept will guide the preparation our elite forces in support of MDO.



Francis M. Beaudette
Lieutenant General, United States Army
Commanding

Army Special Operations in Multi-Domain Operations

Operational Environment

- Near-peer threats
- Contested in all domains
- Increasingly lethal, expanded battlefield
- Increasingly complex environment
- Challenged deterrence
- Terrorists & criminal organizations
- Dense urban areas
- Subterranean

Chinese and Russian Threat Capabilities

Competition

Creating stand-off by separating the U.S. and partners politically with…

- National- and district-level forces
- Conventional forces: Long-, mid-, and short-range systems
- Irregular warfare, proxy warfare and subversion
- Information warfare including cyberspace activities

…to fracture alliances and win without fighting

Armed Conflict

Creating stand-off by separating the Joint Force in time, space, and function with…

- National- and district-level forces
- Conventional forces: Long-, mid-, and short-range systems
- Information, cyberspace, space and electronic attack
- CBRNE and WMD

…to win quickly with a surprise, fait accompli campaign

Military problem: How do Army special operations advance U.S. interests in great power competition against China and Russia while denying violent extremist organizations (VEO) freedom to attack the homeland or threaten vital interests; enable the joint force to penetrate and dis-integrate great power standoff systems in armed conflict; and then consolidate gains and return to competition?

Army Special Operations Central Idea and Contributions in MDO

Central Idea: ARSOF conduct special operations during competition and conflict, as part of the joint force commander's campaign plan to mitigate risk, deter, disrupt, or defeat hostile aggression, and gain time in order to set up strategic and operational options. By expanding partnerships with local irregular forces, Army special operations allow the joint force to sense and create a picture of the adversary's layered standoff system. When directed, ARSOF penetrate denied areas to dis-integrate enemy anti-access and area denial systems by producing multiple physical, virtual, and cognitive dilemmas. This allows the joint force commander to consolidate operational gains and achieve the strategic objectives to return, under favorable terms, to a competitive environment.

Contributions:

- Forward presence campaigning throughout competition
- Physical, virtual and cognitive disruption / defeat of enemy activities in the operational and strategic deep fires areas
- Deep sensing / informational understanding and knowledge across the battlespace
- Global SOF network builds partner capacity while attracting new allies and partners
- Special operations headquarters capable of serving as a JTF - C2 in competition and conflict
- Precision targeting / irregular warfare / counter WMD

Gain Time ← **ARSOF in MDO** → **Extend Reach**

Strategic Support Area	Operational Support Area	Tactical Support Area	Close Area	Deep Maneuver Area	Operational Deep Fires Area	Strategic Deep Fires Area

Army special operations gain <u>time,</u> extend the joint force's <u>reach</u>, and <u>expand strategic options</u>.

Convergence at Echelon

XXXX Theater Army

- Provides AOR-tailored capability
- Maintains enduring initiative
- Sets the theater
- Enables expeditionary maneuver
- Responds immediately to regional emergencies
- Protects bases, key nodes, and networks

XXXX Operational HQ

- Executes competition against a near-peer
- Conducts all-domain operational preparation of the environment
- Provides credible deterrence
- Commands multiple corps
- Enables partners and SOF
- Employs long-range fires

XXX Corps

- Tailors to multiple missions and roles (e.g., Joint Task Force)
- Coordinates deep cross-domain maneuver
- Commands multiple divisions
- Shapes close areas: enemy mid-range fires and IADS
- Defeats long-range fires

XX SOJTF

- Commands joint SOF, CF and multinational air, ground and maritime forces
- Executes deep cross domain maneuver
- Enables defeat of A2/AD mid-long-range fire systems
- Plans, integrates, and conducts special operations
- Executes operations in the information environment

Contributions to Competition, Armed Conflict, and Return to Competition

<u>Compete</u>

- Campaigning in competition
- Global force posture
- Harden the environment
- Expand SOF networks
- Reinforce partners and allies
- Deep area preparation

<u>Penetrate, Dis-integrate, Exploit</u>

- Deep and denied area sensing
- Enable deep area fires
- Enable the dis-integration of A2/AD systems
- Deep area irregular force maneuver
- Support to CF in close fight
- Enable convergence through SOF command and control

<u>Re-compete</u>

- Consolidate gains
- Assure partners/allies
- Secure terrain and population
- Re-calibrate force posture
- Retain position of advantage
- Re-posture in a reframed security environment

Figure 1. Logic Map

U.S. Army Futures Command
Futures and Concepts Center
Fort Eustis, VA 23604

18 September 2020

Force Management

ARMY FUTURES COMMAND CONCEPT FOR SPECIAL OPERATIONS 2028

FOR THE COMMANDER:

OFFICIAL:

EDMOND M. BROWN
Brigadier General, U.S. Army
Acting Director, Futures and
Concepts Center

JONATHAN PHILLIPS
IT Resources Chief, G6

History. This document is a new U.S. Army Futures Command (AFC) pamphlet.

Summary. This pamphlet describes how Army Special Operations Forces (ARSOF) operate throughout the competition continuum to support the Army's conduct of Multi-Domain Operations (MDO).

Applicability. This concept guides future force development and supports the Joint Capabilities Integration and Development System process. It also supports Army capabilities development processes described in the U.S. Army Futures and Concepts Center (FCC) Concepts and Capabilities Guidance, and functions as the conceptual basis for developing affordable options for the future force pertaining to Army special operations across the realms of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P). This concept applies to all Department of Army (DA) activities that develop DOTMLPF-P requirements.

Proponent and exception authority. The proponent of this pamphlet is the Director, Futures and Concepts Center. 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 (FCFC-CE), 950 Jefferson Avenue, Fort Eustis, VA 23604.

Suggested improvements. Users are invited to submit comments and suggested improvements via DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Director, Futures and Concept Center (FCFC-CE), 950 Jefferson Avenue, Fort Eustis, VA 23604-5763.

Availability. This pamphlet is available on the FCC homepage at https://fcc.army.mil/resource-library.

Summary of Change

AFC Pamphlet 71-20-4
Army Futures Command Concept for Special Operations

This revision, dated 18 Sep 2020:

o Describes the operational environment (OE) as it pertains to special operations.

o Describes the military problem and provides a detailed description of how ARSOF can contribute to joint force efforts in competition, armed conflict, and in the return to competition.

o Discusses the importance of building and maintaining relationships with allies and partners to build the networks and mechanisms required to deter aggression in competition, disrupt the potential transition to conflict, and defeat the enemy in armed conflict.

o Emphasizes ARSOF's ability to extend the joint force commander's reach by working with and through local populations to see, sense, and stimulate components of the enemy's system.

o Identifies the capabilities envisioned by this concept to conduct special operations in MDO.

o Explains science and technology capabilities that currently are under development and how ARSOF intends to leverage these in the future.

Contents

Foreword iii
Preface v
Contents 3

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. Linkage to The U.S. Army in Multi-Domain Operations 2028 7
1-6. Background on special operations 7
1-7. The mission of Army special operations forces 8

Chapter 2 Operational Environment 9
2-1. The future operational environment 9
2-2. Implications for Army special operations in multi-domain operations 11

Chapter 3 Conducting Special Operations in MDO 12
3-1. Military problem 12
3-2. Central idea 13
3-3. Solution synopsis 13
3-4. Contributions in competition 14
3-5. Contributions in armed conflict 19
3-6. Contributions to the return to competition 26
3-7. Supporting ideas 27

Chapter 4 Conclusion 33

Appendix A References 34
Section I. Required References 34
Section II. Related References 34

Appendix B Key Required Capabilities 37
B-1. Introduction. 37
B-2. Warfighting Functions RCs 37

Appendix C Science and Technology 41
C-1. The ARSOF Approach 41
C-2. Part I Foundational Research Explored and Addressed 45
C-3. Part II: Advanced Research and Technology 49
Annex 1 – Technology Readiness Levels 60
Annex 2 – Enhanced Reality 61

Glossary 65
Section I. Abbreviations 65
Section II. Terms 68

End Notes 72

Figure List

Figure 1. Logic Map vi
Figure C-1. Exponential Convergence 42
Figure C-2. ARSOF will converge technologies to attack adversary 42
Figure C-2-1. Oculus Rift 61
Figure C-2-2. Google Glass 61
Figure C-2-3. Microsoft HoloLens 61
Figure C-2-4. Virtual Reality image source 62
Figure C-2-5. Augmented Reality image source, Mixed Reality environment 62
Figure C-2-6. Virtual Reality employs a fully digital environment 62
Figure C-2-7. Augmented Reality environment, Mixed Reality environment 63
Figure C-2-8. Perspective in Virtual Reality matches that of the user in virtual world 63
Figure C-2-9. In Virtual Reality and Mixed Reality perspective matches user in real world ... 63
Figure C-2-10. Example of Virtual Reality presence 64
Figure C-2-11. Presence examples for Augmented Reality and Mixed Reality 64
Figure C-2-12. Floating text Augmented Reality allows user to identify virtual elements 64
Figure C-2-13. Perfectly rendered images, whether in Virtual Reality or Mixed Reality 65

Table List

Table C-1. Foundational Technologies for Future ARSOF ..... 45 - 48
Table C-2. Advanced Technologies for the Future ARSOF ..... 49 - 59
Table C-2-1. Technology Readiness Levels 60

Chapter 1
Introduction

1-1. Purpose

a. The *Army Futures Command Concept for Special Operations* describes how Army Special Operations Forces (ARSOF) operate throughout the competition continuum to support the Army's conduct of Multi-Domain Operations (MDO). *TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028, dated 6 December 2018,* proposes solutions to the specific problems posed by the militaries of post-industrial, information-based states like China and Russia. While this special operations concept supports the Army's MDO concept by focusing on China and Russia, it also introduces ideas that apply to other competitors and threats who seek subversive means to compete below the level of armed conflict.

b. This is the first supporting concept included in the Army's family of concepts that focuses on Special Operations. It is also the first ARSOF concept following the inclusion of Special Operations as an Army core competency as defined in *Army Doctrine Publication 1, The Army*. Its ideas expand upon traditional ARSOF approaches to defeat United States (U.S.) adversaries. Defeating national adversaries requires a nuanced, whole of government approach in competition however; it requires defeat of their entire warfighting system during large-scale combat operations (LSCO). It includes defeating their physical capabilities such as personnel, command and control (C2) architecture, strategic intelligence, logistics base, and the means by which they acquire and use data as well as having virtual and cognitive effects on their ability to wage war.[1] The systematic defeat of an enemy demands an in-depth understanding of the system's strengths and vulnerabilities. Defeating an enemy's system requires defeating its logic—the reason the system functions the way it does. Therefore, ARSOF must see, sense, stimulate, and strike critical parts of the enemy's stand-off system across all domains to enable the joint force to disrupt the enemy's logic and defeat the way they intend to fight. This concept describes the ARSOF role in MDO in competition, conflict—including LSCO, and in the return to competition on terms favorable to National interests.

(1) The 2017 National Security Strategy (NSS) and the 2018 National Defense Strategy (NDS) have reoriented ARSOF focus on great power competition and near-peer threats. In this new era of great power competition, our nation's adversaries seek to achieve their strategic aims while avoiding armed conflict under the protection of a layered stand-off system. Stand-off in the political, military, and economic realms isolates the U.S. from its allies and partners, creates strategic ambiguity, and facilitates *fait accompli* such as that which occurred in Crimea. Adversaries will employ multiple layers of stand-off in all domains—land, maritime, air, space, cyberspace, the electromagnetic spectrum (EMS), and the information environment—to separate the U.S. joint force and its allies in time, space, and function.

(2) The ideas in this concept include the results of rigorous and ongoing experimentation. The U.S. Army Special Operations Command (USASOC) integrates these ideas into joint and Army experimentation venues and assesses them during on-going global operations. ARSOF participation in these events helps the Army envision new ways for conventional forces (CF) and special operations forces to achieve operational synergy in competition and conflict.

(3) This concept acknowledges the Global Operating Model, set forth in the 2018 NDS, and explores the possibilities of operating physically, virtually, and cognitively within it.[2] The NDS Global Operating Model is a strategic construct that "describes how the Joint Force will be postured and employed to achieve its competition and wartime missions." The model has four "layers:" *contact*, *blunt*, *surge*, and *homeland*. Briefly, the contact layer is where U.S. forces routinely confront adversaries in competition below the level of armed conflict; the blunt layer is where U.S. forces delay, degrade, or deny adversary aggression in the transition to conflict; in the surge layer, war-winning forces defeat fielded enemy forces in combat; finally, U.S. forces continuously defend the Nation in the homeland."[3]

c. Chapter 2 describes the operational environment (OE) as it pertains to special operations. Chapter 3 describes the military problem and provides a detailed description of how ARSOF contributes to joint force efforts in competition, armed conflict, and in the return to competition.[4] Chapter 4 is the conclusion that emphasizes key themes of the concept. Appendix A details the required and related sources for this concept. Appendix B identifies the capabilities envisioned by this concept to conduct special operations in MDO. Appendix C explores capabilities that currently are under development and which ARSOF intend to leverage in the future.

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 this pamphlet.

1-4. Assumptions

a. As with any concept, the special operations concept is aspirational and a vision for how ARSOF may fight in 2028. While it is resource informed, an unconstrained approach underpins an overarching assumption, specifically with respect to SOF-unique resources, formations, capabilities, strategy, policy, and authorities. The central idea—that Army special operations will enable the joint force to mitigate risk, gain time, extend reach, and expand strategic options—is predicated on the four interrelated assumptions below. A change to any of the following assumptions demands a reassessment of this concept's central idea.

b. In spite of enemy layers of stand-off, special operations forces will be able to penetrate through portions of the enemy's anti-access and area denial (A2/AD) systems using specialized means.

c. Conventional forces and special operations forces operating systems will be compatible, cross-functional, and their information protocols will share relevant information.

d. Local partners and regular and irregular forces will share similar or related U.S. campaign objectives and demonstrate their resolve by providing appropriate resources.

e. 1st Special Forces Command (Airborne) will have the resources, command and staff structure, capabilities and authorities, to plan, prepare, and execute campaigning activities as a special operations joint task force (SOJTF) during competition and conflict.

1-5. Linkage to The U.S. Army in Multi-Domain Operations 2028

a. The *U.S. Army in Multi-Domain Operations 2028* depicts the future operational environment as increasingly complex and contested in all domains. An increasingly lethal and hyperactive expanded battlefield will make it harder for nation-states to impose their will in a politically, culturally, technologically, and strategically complex environment. Near-peer states will more readily compete below armed conflict making deterrence more challenging. China and Russia will continue to leverage these trends to create tactical, operational, and strategic stand-off. Army forces conduct MDO to prevail in competition; and if necessary, penetrate and dis-integrate enemy anti-access and area denial systems and exploit the resultant freedom of maneuver to achieve strategic objectives and force a return to competition on favorable terms.

b. The *Army Futures Command Concept for Special Operations* supports the MDO concept by providing a conceptual foundation that describes how Army special operations forces will compete to prevail in competition; penetrate into the operational and strategic deep fires areas in conflict; and enable the dis-integration of enemy anti-access and area denial systems. ARSOF will enable the joint force to exploit opportunities in the deep areas to delay, disrupt, or attrite enemy forces supporting the close fight, and assist the joint force as it consolidates gains and re-competes in the reframed security environment.

1-6. Background on special operations

a. According to Joint Publication 3-05, *Special Operations*, special operations are operations requiring unique modes of employment, tactical techniques, equipment and training conducted in hostile, denied, or politically sensitive environments. One or more of the following often characterize special operations: time sensitive, clandestine means, low visibility, conducted with and through local irregular forces, requiring regional expertise, and a high degree of risk. Additionally, Title 10 U.S. Code, Section 167 specifies ten special operations activities insofar as each of them relate to special operations:

- Direct action.
- Strategic reconnaissance (SR).
- Unconventional warfare (UW).
- Foreign internal defense (FID).
- Civil affairs (CA).
- Military information support operations (MISO).
- Counterterrorism (CT).
- Humanitarian assistance (HA).
- Theater search and rescue (SAR).
- Such other activities as may be specified by the President or the Secretary of Defense.

b. ARSOF are specially organized, trained, and equipped military forces. ARSOF can operate as small teams or task forces to develop and execute discreet, precise, and scalable special operations in permissive, uncertain, and hostile environments. ARSOF develop and execute diplomatically sensitive missions using the principle of discretion. In diplomatically sensitive conditions, special operations forces create effects of a magnitude disproportionate to their small footprint. ARSOF support objectives that deter, prevent, or resolve trans-regional, cross-domain threats, as well as support Army operations over a multi-domain extended battlefield.[5] ARSOF conduct core activities using unique capabilities derived from specialized training, equipment, organizations, and authorities. The ARSOF core activities, derived from those outlined in Title 10, U.S. Code and directed by U.S. Special Operations Command, include:

- Unconventional warfare (UW).
- Foreign internal defense (FID).
- Counterinsurgency (COIN).
- Counterterrorism (CT).
- Countering weapons of mass destruction (CWMD).
- Security force assistance (SFA).
- Direct action.
- Special reconnaissance (SR).
- Military information support operations (MISO).
- Civil affairs operations (CAO).
- Preparation of the environment (PE).
- Hostage rescue and recovery (HRR).
- Foreign humanitarian assistance (FHA).

c. The Army forces that conduct special operations include special forces, civil affairs, psychological operations, special operations aviation, Rangers, special operations logistics units and special mission units. Special operations forces are capable of operating geographically dispersed in small elements when conducting a particular activity. Special forces are ideally suited for unconventional warfare. Psychological operators are experts in influence and shaping operations. Civil affairs operators engage the civil component of the OE and provide civil considerations expertise. Rangers specialize in direct action and crisis response. Army special operations aviation units provide responsive, special operations aviation capability. Special operations logistics units provide tailored logistics, signal support, medical care and military intelligence support for ARSOF worldwide. In practice, ARSOF rarely operate piecemeal and instead conduct integrated campaigning in support of the JFC as a special operations combined arms team. ARSOF function as part of a joint special operations component under the geographic combatant commander (GCC) or a subordinate JFC.

1-7. The Mission of ARSOF

a. Army special operations forces prepare for all types of conflict and arm the joint force with the world's premier ARSOF. ARSOF provide value to the Nation through their unique capabilities to advance partnerships, influence adversarial behavior, execute special operations, and respond to crisis.

b. During competition and conflict, ARSOF's geographically calibrated force posture provides the JFC with a capability to quickly understand the OE and wield influence in the contact and blunt layers with near-peer adversaries or irregular threats. ARSOF maintain an advantage in the virtual and cognitive dimensions through sustaining and building persistent relationships with local partner forces, resident populations, government institutions, and interorganizational partners. These relationships allow the JFC to leverage military and civilian networks that improve real-time situational understanding, amplify operational effects, and disrupt an adversary's communication capabilities and decision-making process.

c. ARSOF attract, train, and retain the best talent available to conduct the full range of specialized activities. People are ARSOF's platform and will always be the first priority. ARSOF are the relationship enablers of the joint force who capitalize on trust and professionalism with strategic partners. ARSOF execute enterprise-wide 21st century talent management techniques to produce empowered Soldiers who prevail in high intensity combat, thrive in chaotic complexity, integrate rapidly changing technology and embody the ARSOF culture of lethality, agility and survivability.

Chapter 2
Operational Environment

2-1. The Future Operational Environment

a. The 2018 NDS specifically recognizes the "central challenge to U.S. prosperity and security is the *reemergence of long-term strategic competition*."[6] Furthermore, it identifies the need for "new concepts of warfare and competition that span the entire spectrum of conflict" to address the new reality.

b. The *Joint Operating Environment 2035* predicts that U.S. national interests will face challenges from both persistent disorder and states contesting international norms. Great power competition and conflict are the context of this concept. Additionally, an important characteristic of the emerging OE is its urban nature. The strategic importance of cities suggests that Army forces must be able to conduct operations within dense urban terrain.

c. This concept focuses on great power challenges, but it also accounts for an array of regional and non-state actor security challenges. This includes the ongoing fight against VEOs and criminal networks. VEOs and similar threats will confront the U.S. in ever evolving sophisticated ways. They will be dangerous, resilient, adaptive, and focus on long-term strategies. Additionally, the proliferation of chemical, biological, radiological, and nuclear weapons, and the means to deliver them into the hands of adversaries who think and act asymmetrically will threaten U.S. interests, the homeland, and international security.

d. The strength of the joint force lies in its ability to integrate capabilities and project power globally. Our adversaries intend to offset these abilities through layered stand-off in the political, military and economic realms to separate the U.S. from our partners. During conflict, they will employ multiple layers of stand-off in all domains—land, maritime, air, space and cyberspace—as well as the EMS and the information environment to separate U.S. forces and our allies in time,

space, and function to defeat us. Stand-off will provide adversaries strategic decision cycles with an advantage in respect to time and distance. To counter this adversary approach, the joint force must negate the effects that multiple stand-off layers create.

e. Among the states to contest international norms, China and Russia are the most capable.[7] Thus they are the focus of this concept. Both are pursuing capabilities and approaches to create operational and strategic stand-off. Russia has demonstrated the most effective combinations of systems and concepts to challenge the U.S. militarily in the near term. Russia's actions in Georgia, Ukraine, and Syria have demonstrated its pursuit of strategic objectives below the threshold of armed conflict. China possesses the vision and strategic depth to become the U.S.' most powerful competitor in time and possesses the economy and technological base to overtake the current Russian system overmatch in the next 10-15 years.[8]

f. Chinese and Russian attempts to create political, economic, and military stand-off challenges the joint force's ability to dominate all domains, the EMS, and the information environment. If successful, stand-off offers these near-peer competitors the strategic freedom of action to pursue objectives at the expense of the U.S. and its allies. China and Russia scale their offensive operations to avoid triggering a decisive U.S. response. They typically direct such operations at fault-line states.[9] China's and Russia's ability to rapidly transition to overt military action provides them the means to seize and maintain the initiative before the U.S. and partner forces can prepare a response.

g. Our adversaries will seek to expand the battlefield in four ways: time, domains, geography, and actors.[10] They will blur the distinctions between actions below armed conflict and during armed conflict to achieve strategic objectives short of what the U.S. traditionally considers war. The expanded battlefield will include space, cyberspace, electronic warfare, and information operations as key components of adversary operations.[11] They will also seek to expand the battlefield geographically. The cumulative effect of their multi-domain capabilities will extend the range at which they can effectively engage joint force formations. Finally, they will increasingly pursue their objectives through non-traditional actors, including proxies and surrogates.

h. In competition, Russia will attempt to separate the U.S. and friendly states politically, limiting a coordinated allied response while destabilizing target states. To accomplish this task, Russia will execute coordinated campaigns employing national and district level capabilities, including irregular and conventional operations to achieve strategic objectives. Through this integrated approach during competition, Russia will seek to achieve objectives without risking armed conflict with the U.S.[12]

i. The operational center of gravity for Russian actions in competition will be their close integration of information warfare, proxy warfare, unconventional warfare, and other actions below the threshold of armed conflict.[13] Their ability to employ all elements in a coordinated manner provides Russia with an escalation advantage, in which any friendly reaction risks a more powerful response. Their demonstrated ability to accomplish a *fait accompli* will provide credibility to Russian narratives.[14] This combination of information warfare, proxy warfare,

unconventional warfare, and nuclear forces provides Russia with political and military stand-off within which it can secure strategic objectives short of armed conflict with the U.S.[15]

j. Russian long- and mid-range fires systems will be their operational center of gravity in armed conflict. Russian conventional forces will seek to increase physical stand-off by creating layers of anti-access and area denial systems designed to inflict unacceptable losses on U.S. and partner military forces. They aim to achieve campaign objectives within days, before the U.S. can effectively respond. The Russians will attempt to convince the U.S. that it has lost before it can react. If that fails, they will attempt to impose high costs early on to disrupt U.S. strategic and operational maneuver.

k. All-domain reconnaissance will enable Russian forces to operate in depth all the way from within the U.S. homeland to the area of operations. Empowered by extensive reconnaissance complexes, they can conduct simultaneous attacks throughout the depth of the battlefield. Russia will continue to design their systems to separate the joint force in time, space, and function.

l. China possesses the vision and strategic depth to become the U.S.'s most powerful competitor in time. Unlike Russia, China has the economy and technological base, such as an independent microelectronics industry and world-leading artificial intelligence (AI) development process that is sufficient to have overmatch with the current Russian system in the next 10-15 years. China is rapidly building a world-class military intended to project power globally. In the future, U.S. strategists assume that China will become the pacing threat for the joint force. The joint force must continuously assess the risks associated with this assumption to ensure their ability to adapt should China accelerate its capability development.[16]

2-2. Implications for Army Special Operations in Multi-Domain Operations

a. What current and emerging threats have in common is their intent and capability to challenge the U.S. by employing a variety of means to generate stand-off—exploiting political ambiguity, our strategic posture, and joint force operational predictability. Countering these threats will require a concept that converges capabilities from all domains, EMS, and the information environment to solve a wide array of problems in both competition and armed conflict.

b. The adversary's strategy to extend the battlefield in competition and conflict has direct implications for ARSOF by offering opportunities to undermine specific elements of adversary strategy. In competition, ARSOF can identify subversive activities, expose propaganda efforts, and counteract threat actions through irregular warfare beneath the level of armed conflict. Similarly, the adversary will be vulnerable when operating among populations that favor the U.S. where information and tailored operational activities can further limit adversary freedom of access and options. In conflict, ARSOF can attack vulnerable elements that underpin the enemy's strategy by targeting ground-based air defense, C2 nodes, long-range strike systems, WMD storage and delivery systems, and terrestrial space capabilities. As the adversary's strategy unfolds it will reveal possibilities for ARSOF to attack multiple elements of that strategy, thereby collapsing the extended battlefield and reducing the adversary's ability to achieve stand-off.

c. Advantages will accrue to those who act first and retain the ability to see, sense and fight deep. The special operations deep fight in the operational and strategic deep fires areas will rely on trans-regional collaboration and globally integrated operations to outpace enemy decision-making. The deep fight will require new and tailored approaches to the six warfighting functions—C2, movement and maneuver, intelligence, fires, sustainment and protection—and the integration of special operations with strike, reconnaissance, space, cyberspace and other capabilities. Ultimately, special operations in the deep fight will directly affect the tempo and momentum of the close fight. ARSOF activities in both the deep and close areas will help to retain Army brigade combat team (BCT) combat power and freedom of action required to win in the close fight.

d. U.S. adversaries have created decision space by using defenses in depth to their advantage. The joint force must penetrate through these layers, overcoming the challenges of time, space, and information to operate with a tempo that adversaries cannot match. One service alone will not be sufficient. It will take the entire joint force, including ARSOF, to achieve success in MDO.

e. ARSOF must penetrate multiple layers of stand-off to operate in denied areas, especially in the operational and strategic deep fires areas. This requires undetected access to denied areas using covert or clandestine infiltration techniques via government or commercial air, land, maritime, or space platforms. ARSOF will infiltrate denied areas using capabilities such as military free fall operations until future technologies emerge and become practicable.

f. Near-peer adversaries will conduct physical, virtual, and cognitive activities across all domains, sequenced over time to obtain a position of relative advantage in competition, prevent U.S. forces from moving strategically and gaining a lodgment during the transition to conflict, and to prevent U.S. or coalition elements from closing with their fielded forces in conflict. ARSOF will support MDO by providing a physical point of presence in the contact layer during competition and in the blunt and surge layers during conflict.

g. By converging SOF, space, cyberspace, intelligence, fires, and information capabilities the joint force will conduct operations in multiple domains within all four layers of the NDS Global Operating Model to see, sense, stimulate, and strike deep across all domains, the EMS, and in the information environment. Such a convergence of capabilities will create ‘multiple fronts’ that present the enemy with a myriad of compounding dilemmas thus, preventing the components of his system from cooperating effectively and paralyzing his decision-making processes.

Chapter 3
Conducting Special Operations in MDO

3-1. Military problem
How do Army special operations advance U.S. interests in great power competition against China and Russia while denying violent extremist organizations freedom to attack the homeland or threaten vital interests; enable the joint force to penetrate and dis-integrate great power stand-off systems in armed conflict; and then consolidate gains and return to competition?

3-2. Central idea

ARSOF conduct special operations during competition and conflict, as part of the JFC's campaign plan, to mitigate risk, deter, disrupt, or defeat hostile aggression, and gain time in order to set up strategic and operational options. By expanding partnerships with local irregular forces, Army special operations allow the joint force to sense and create a picture of the adversary's layered stand-off system. When directed, ARSOF penetrate denied areas to dis-integrate enemy anti-access and area denial systems thereby producing multiple physical, virtual, and cognitive dilemmas. This allows the JFC to consolidate operational gains and achieve the strategic objectives to return, under favorable terms, to a competitive environment.

3-3. Solution synopsis

a. ARSOF contributions to MDO. Army special operations mitigate risk, expand strategic options, and open windows of superiority for the joint force in MDO. Special operations reduce risk to the joint force by developing strategic options for either future action or for crisis off-ramps. These operations gain time for decision makers by removing strategic ambiguity via SOF-unique intelligence capabilities, deterring aggression through forward presence and building partner capacity, and enabling rapid decision cycles through situational awareness. In competition, ARSOF provide national response options below the threshold of armed conflict. This includes wielding influence through local partners to develop and leverage partner capacity and capability. ARSOF prepare and shape the environment through networks of relationships that provide deep knowledge of the civil-military situation and the resilience to counter adversary narratives and hostile attempts to alter the security framework. In armed conflict, including LSCO, extend the joint force's reach and ability to see, sense, stimulate and strike critical stand-off nodes throughout the battlefield. ARSOF C2 provides integrating headquarters at echelon that support a whole of government approach in competition and a bridge to joint and Army headquarters in conflict at the operational and tactical levels.

b. ARSOF in competition. Competition below armed conflict involves indirect, rather than direct, military power. This reflects a choice by the U.S. government to pursue policy objectives while constraining military actions, so they remain short of armed conflict.[17] Throughout competition, ARSOF gain an understanding of the relevant actors' perception of U.S. actions. ARSOF assess critical areas of interest, enhance partner capabilities, and advance cooperation with allies and partners while minimizing the commitment of U.S. forces and resources. This sets conditions that allow the JFC to maximize a range of military options if there is a change in the political situation. This position of strength supports a favorable environment for joint force, interagency, and partner efforts to counter adversaries' coercion efforts through unconventional and information warfare.[18] The main purpose of special operations in competition is to help the JFC achieve U.S. strategic objectives without escalation to armed conflict.

c. ARSOF in armed conflict. If deterrence fails in competition and armed conflict ensues, direct military power becomes the primary policy choice of the U.S. government. ARSOF, as part of a joint force, conduct special operations to penetrate and dis-integrate enemy anti-access and area denial systems and exploit the resultant freedom of maneuver to achieve strategic objectives. ARSOF's calibrated force posture, which includes forward presence and expeditionary forces, as well as its infiltration capability, creates windows of superiority for the JFC to engage the enemy

in the close, deep maneuver, operational deep fires, and strategic deep fires areas. ARSOF conduct its core activities to blunt or delay an enemy's attack and provide time for U.S. and its allies to surge forces into theater. ARSOF maneuver tactically and operationally, employ cross-domain, lethal and nonlethal fires, and maximize local partner combat potential as a multi-domain formation. Operating as a multi-domain formation requires the rapid convergence and continuous integration of capabilities across all domains, the EMS, and the information environment.

d. Army special operations in return to competition. In the return to competition, ARSOF support the joint force as it consolidates gains. During stabilization activities in theater, ARSOF enhance the efforts of conventional formations by providing additional capabilities to address civil-military requirements including support to governance and populations. ARSOF enhance partner capabilities and assure partners and allies in the newly framed security environment. They assist in shaping public opinion and reinforcing the legitimacy of post-conflict partner nations. Army special operations consolidate strategic gains for sustainable outcomes and reset force posture based on the new security framework.

3-4. Contributions in competition

a. Campaigning in competition.

(1) The U.S. military has traditionally associated campaigning with operations and activities in armed conflict focused on achieving strategic and operational objectives in order to attain victory. The aggressive actions of China and Russia indicate that they are willing to extend activities usually associated with armed conflict into the competition space. They desire to achieve their national objectives below the threshold of armed conflict during competition without provoking a conflict response. Therefore, the U.S. must place increased emphasis on each GCC's theater campaign plan and recognize that traditional theories of campaigning must expand in the competition space in order to achieve national strategic objectives.

(2) Nationally coordinated competition activities reduce strategic surprise, counter enemy narratives, and gain time for decision makers and joint force deployment. ARSOF support GCC campaign plans in competition to prevent the escalation to armed conflict or rescale an existing conflict. Gains in competition below armed conflict typically take the form of modifications in behavior rather than control of territory. In competition, the military will usually support other elements of national power—diplomatic, informational, or economic—as part of a whole of government approach to gain or retain a position of strategic advantage. Whether the military is the supported or supporting effort, ARSOF's persistent engagement through their forward and rotational presence is an important enabler of the GCC's theater campaign plan.

(3) Special operations conducted below the level of armed conflict enable the joint force to seize the initiative to gain time and develop flexible response options. ARSOF core activities shape the environment, counter threat narratives, and complicate adversary decision making. Disrupting the adversary's plans reduces the number of operational and mission variables that he can employ.[19]

(4) Joint force campaigning in competition begins with a deep understanding of the relevant actors' perceptions of the OE and of their decision making in the context of diplomatic, informational, military, and economic efforts. ARSOF access and placement provides the JFC deep knowledge of the OE and its actors through its persistent engagements and well-developed relationships enhanced by cultural and foreign language familiarity. ARSOF reduce strategic ambiguity through their capability to see, understand, assess, and wield influence across a diverse range of operating environments.

(5) ARSOF, through steady state activities and strategic crisis response mechanisms, help shape a favorable competition tempo and generate situational understanding. ARSOF global operations and activities condition the OE against threat activities below the level of armed conflict. The ARSOF operational approach recognizes that success in competition is a result of the aggregate effects of multiple operations and activities over time that enable the U.S. to retain or gain a position of advantage.

(6) ARSOF conduct irregular warfare and a broad array of activities such as establishing access to critical areas, positioning units forward, maintaining a persistent presence, conducting exercises, sharing intelligence, preparing the environment and conducting operations in the information environment to influence relevant populations. With their persistent presence in theater, ARSOF help mitigate the risk of an adversary achieving a *fait accompli* by providing strategic posturing across the OE. These forces assist in denying the enemy the conditions required and influence him to conclude that an armed attack would fail.

(7) Special operations disrupt adversary attempts to expand the competitive space by employing local partner forces using low-visibility, clandestine or covert methods, and by expanding options through the exercise of authorities and capabilities typically not associated with conventional ground forces. Long-standing relationships reduce the potential for "cold starts" and provide continuity for operations in competition and conflict. Continued engagement re-assures partners, demonstrates commitment to U.S. security guarantees, and attracts new partners.

(8) The SOJTF is one means by which the GCC can command and control special operations directly or through a JTF commander. The SOJTF can conduct multi-domain operations supporting GCC campaign plans during competition. Currently, the theater special operations commands (TSOCs) oversee activities of SOF assigned and attached to GCCs. However, as SOJTFs develop over the next decades, they can assume a greater role in trans-regional, multi-domain, and multifunctional operations. The SOJTF focuses on a specific region, or line of effort, leaving the TSOC free to maintain a broader theater perspective. A SOJTF is a deployable, JTF-capable, headquarters that supports joint all domain operations and Army MDO. ARSOF tailor the SOJTF 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 serve as an integrating headquarters for specific whole of government solutions designed to accomplish campaign plan objectives.

(9) The SOJTF is the equivalent of an Army echelon above brigade (EAB) formation for SOF operational level C2. It directs ARSOF's regional engagement to developing resilient, capable, and interoperable partners. Integrated joint force capabilities, including space and cyberspace

shape friendly, neutral, and hostile perceptions to levy strategic costs, disrupt threat influence activities, influence threat behavior, and disrupt threat information capabilities. The SOJTF can marshal ARSOF's partner networks to create stand-off against threats short of armed conflict, seize the initiative to prevent a surprise attack, and set conditions for a lower risk commitment of U.S. or coalition forces if diplomacy and deterrence fail. In the event of a major escalation leading to armed conflict, the SOJTF can facilitate joint force maneuver through activities such as enabling reception, staging, onward movement, and integration (RSOI), intelligence production and dissemination, joint targeting, and securing and expanding lodgments.

b. Global force posture.

(1) SOF's global force posture enables JFCs to see the operating environment at specific locations, characterize emerging events, and develop flexible response options. It includes forward stationed ARSOF, those deployed in support of contingency operations and activities across the globe, and those preparing to deploy. Special operations prepare the environment by establishing human networks that support intelligence operations and build the physical infrastructure to support future military operations. As part of the theater intelligence architecture, ARSOF employ counterintelligence (CI) capabilities necessary for those units and personnel that operate in deep areas. ARSOF identify and characterize threats; emplace sensors; provide an understanding of individuals, groups, populations, and information infrastructure; and provide civil information to identify critical nodes and links within the civil environment. Using both joint and Army capabilities, ARSOF share this knowledge with the joint force and interagency partners to inform and populate the joint common operational picture (COP) with multi-domain feeds.

(2) ARSOF's global force posture expands the competition space. It compels adversaries to orient in multiple directions and allocate resources to disparate perceived threats. ARSOF conduct a range of partner-based activities such as joint combined exchange training (JCET), counter-narcotics (CN), counter-weapons of mass destruction (CWMD) training, counterterrorism (CT) training, and multinational exercises. In the future operating environment, increasing the impact of these steady state activates will provide additional pressure against adversary attempts to expand the competitive space. Global force posture enables networked ARSOF elements to converge physical, virtual, and cognitive effects from around the world, and across multiple domains, in support of MDO. Global force posture places special operations in advantageous positions and in some cases within adversaries' interior lines of communication. Their physical, virtual, and cognitive presence in the right place and at the right time provides the joint force with strategic and operational flexibility and agility.

c. Harden the environment.

(1) Hardening the environment increases the available options for the U.S. and its partners while simultaneously reducing those of our adversaries. It leverages time with respect to ARSOF long-term regional engagement and nest with multi-year national strategies. Hardening requires proactively operating in all domains where competition occurs. Special operations core activities of FID, COIN, CT, UW, MISO, and CAO build partners' capacity and capability to resist hostile narratives and pressure to set conditions for long-term deterrence.

(2) Special operations harden the operational environment as well as the information environment by supporting partner nations in building capable and confident forces, resilient populations, and resistance capabilities. Strengthened partner forces provide a security environment where other instruments of national power can effectively operate. They strengthen the capability and will to resist adversary coercion and prevent aggression. Special operations in the information environment enable populations to identify, reject, and counter adversary misinformation, disinformation, and propaganda. A resilient population can discredit malign influences and assert itself in countering adversary disinformation. Army special operations build resistance capacity through security force assistance and FID. ARSOF support to a resistance complicates an oppressor's strategic calculations and timetables.

d. Expand SOF networks.

(1) The Global SOF Network is a system of personal and professional relationships with other SOF teams, command elements, joint forces, allied and partner forces, other governmental agencies and non-governmental organizations. It provides a network for interactive exchange of information to facilitate deep understanding and create decision-making advantages. It includes the hardware, software, procedures, and protocols used to plan and execute special operations. The network provides deep knowledge and timely understanding of malign activities in geopolitical spaces. The network is the fabric that connects ARSOF with its joint, interagency, and multinational partners to speed decision making and implement shared action. The global SOF network provides enhanced capabilities and flexible options for the joint force in MDO. ARSOF continuously seek to expand the SOF network with new partners around the globe and across various disciplines.

(2) Special operations develop and employ human networks. These networks are part of the Global SOF Network. They assist the joint force in characterizing and responding to adversary intentions and actions. In competition and conflict, they provide the necessary access and placement required to strike adversary critical capabilities in areas where either physical or domain access is denied. Networked with U.S. and partner cyberspace and space systems, special operations levy strategic costs that influence adversary behavior. Networked special operations provide decision makers with situational awareness when an adversary tries to conceal his intent and activities. The network provides mechanisms that enable effective crisis response options.

e. Reinforce partners and allies.

(1) ARSOF develop resilient and resistant partners able to prevail against adversary threats and maintains cohesive networks that condition the environment against sudden shocks. ARSOF support national objectives through overt activities such as training events that increase interoperability with partners. ARSOF leverage opportunities to expand the scope of traditional Theater Security Cooperation Plan (TSCP) events. ARSOF reinforce interpersonal relationships by sharing the difficulties and risks involved in fighting alongside partners. During operational deployments, ARSOF integrate partners and allies into their headquarters and share information and intelligence fully within caveats. For example, both SOJTF-A in Afghanistan and SOJTF-OIR in Iraq integrated allies and partners into their headquarters staffs and subordinate units of

action. ARSOF promote battlefield interoperability by exchanging tactics, techniques, and procedures (TTP) and providing mutual support.

(2) ARSOF promote the value of partnerships. In security cooperation, ARSOF reinforce partners and allies by participating in operations and activities that increase partner capabilities. ARSOF build professional and institutional relationships. ARSOF senior leaders conduct routine, persistent engagements that maintain long-term strategic partnerships. ARSOF formations maintain planned bilateral and multinational training events and opportunities for participation in exercises, symposiums, and conferences. ARSOF maintain regular personnel exchange programs with partners and allies for attendance at professional development schools. A persistent presence and long-term engagement characterize ARSOF partnerships.

f. Deep area preparation.

(1) In competition, ARSOF operate across the globe to generate deep cross-domain understanding and prepare the deep areas through sensing, influencing, developing human networks, and building partner capacity. This enables ARSOF to set conditions prior to armed conflict. The work that must occur during competition is critical to prevailing in conflict and deter or compel adversary behavior.[20] This includes developing mechanisms and networks that the joint force will not have time to create on the eve of conflict. Operations that cannot incorporate pre-established mechanisms and networks, especially when targeting sophisticated threats, rarely produce the comprehensive results required in conflict. ARSOF must initiate, build, and exercise these mechanisms and networks during peacetime to make them available to the joint force in wartime.

(2) ARSOF, in combination with partner forces, can conduct maneuver and deception operations to see and stimulate enemy mid- and long- range systems and fix or isolate enemy maneuver forces. Maneuver is cross-domain and includes converging virtual and cognitive effects in the scheme of maneuver. ARSOF leverage influence-focused targeting and employ organic capabilities to conduct operations in the information environment designed to achieve virtual, cognitive, and physical objectives. ARSOF converge space, cyberspace, and electronic warfare, fires intelligence, deception and influence capabilities to achieve deep area preparation in support of future joint force operations.

(3) ARSOF conduct deep area preparation through integrated teaming and applying their full suite of capabilities including sensitive activities. Special operations in competition provide the JFC:

- Intelligence on adversary plans and intentions.
- The ability to expose adversary plans and intentions.
- The capability to exploit friction in the competitive space: overtly, clandestinely, or covertly.
- The capability to create friction in the competitive space while managing escalation.
- Disruption of adversary plans overtly or through covert activities that syphons their national resources and prestige over time.

- Influence-focused targeting to exploit adversary vulnerabilities and dependencies, and erode third party support.

(4) Special operations and activities extend across the competition continuum; moderated in their intensity and duration according to priority and level of risk.[21] ARSOF conduct highly specialized raids and operations that can obtain a temporal position of advantage for the joint force and then quickly conclude, returning the competitive space to its previous state. To minimize risk while maximizing effect, special operations are synchronized across multiple-domains, in a campaign that begins in competition, emphasizing planning, preparation, locally procured knowledge, deep operational understanding, and extends, when necessary, through armed conflict.

3-5. Contributions in armed conflict

a. The MDO concept recognizes SOF as the only ground maneuver force in the deep fires areas. This places SOF in a unique position to converge effects from space, cyberspace, fires, intelligence, and information capabilities deep in otherwise denied areas. The Army uses special operations to broaden the range of combined-arms options for penetrating and dis-integrating enemy stand-off layers and exploiting the resultant freedom of maneuver. While ARSOF operate in the close and deep maneuver areas, the majority of ARSOF activities in armed conflict occur in the operational and strategic deep fires areas. ARSOF's objective in the deep fires area is to shape the close and deep fight and create windows of superiority for the joint force. For example, ARSOF operations against enemy long-range lethal and nonlethal fires capabilities in the deep fires areas produce effects in the close and deep maneuver areas in the form of reduced pressure on conventional forces. ARSOF will require advanced infiltration capabilities, such as military free fall, to penetrate and operate in the deep fires areas in 2028. Special operations expand options in armed conflict by providing the joint force a means to:

- Sense deep in denied areas.
- Enable deep area fires.
- Enable the dis-integration of key nodes within enemy A2/AD systems, specifically focusing on the integrated long-range fires complex and the integrated air defense system.
- Maneuver locally recruited, trained, and equipped forces in deep areas.
- Support conventional forces in the close fight.
- Converge cross-domain capabilities in the deep areas through SOF Command and Control.

b. Deep and denied area sensing.

(1) By sensing deep in time and space, special operations create a picture of the OE beyond conventional resources and capabilities. ARSOF retain the capability to see and sense deep unilaterally, or in coordination with its partners, when enemy interference creates domain denial gaps that degrade joint and national sensors. ARSOF access to, and presence in, denied spaces enhances persistent national sensing efforts. Deep and denied area sensing involves intelligence functions that ARSOF integrates into all special operations activities. Intelligence operations may include human intelligence, including military source operations; counterintelligence; airborne, high-altitude, and space, maritime, and ground-based signals and geospatial intelligence; tagging, tracking, and locating (TTL); intelligence, surveillance, and reconnaissance (ISR); and weather

sensing. As part of intelligence operations, ARSOF requires CI capabilities to preserve essential secrecy and that dependency is particularly acute for those units and personnel who will operate in the operational and strategic deep fires areas.

(2) Reporting intelligence information to the Army and joint force requires common procedures and intelligence fusion capabilities that work at disaggregated and disparate locations. These capabilities must process significant amounts of data and enable secure, continuous, and automated cross-domain and cross-coalition transfer in a communications degraded environment. Through SOF unique communications channels, ARSOF can communicate in a communications degraded environment. SOF, space forces, and cyberspace forces collect information, synthesize it, assess it for intelligence value, and share it within protocols that protect the security and integrity of the information and the assets that produce it. Writing-for-release, to include the use of tear-lines, maximizes the ability to share information. For example, space and cyberspace assets collect imagery, network infrastructure information, and point-to-point digital communications. ARSOF collect information regarding priority systems and targets and ascertain ground truth through personal observation and contact with local populations.

(3) In addition to human sensors, special operations integrate a network of dispersed sensors, to include weather sensors that are manually operated, semi-autonomous, or autonomous for ground, subterranean, and aerial systems. ARSOF disseminate data from these sensors through low visibility, low probability-of-detection, non-standard communication systems and related tactics, techniques and procedures to coordinate activities across echelons. ARSOF employ enhanced virtual and physical signature management to remain undetected.

(4) ARSOF converge cross-domain capabilities to enable the joint force to see, sense, stimulate, and strike deep into enemy systems to disrupt and degrade their stand-off capability. AI-enabled capabilities will process data to increase the speed and quality of decision making and enhance the production of information. Special operations deep sensing must overcome the technical challenges of processing data in denied and degraded environments. Exchanging information is a systemic challenge requiring the use of common hardware, software, and shared network infrastructure to capitalize on predictive, automated, and autonomous learning capabilities. ARSOF use Army communications and intelligence systems to receive and share data with joint forces and to populate the consolidated joint COP.

(5) ARSOF share data, using a common data standard, to support cross-domain targeting. Innovative efforts to acquire, process, distribute, employ, and share data helps to improve understanding and maintain the operational tempo.[22] Given the extremely rapid pace at which information systems are evolving, meeting joint forces information requirements will require working closely with partners, industry, and academia.

(6) ARSOF contributes to deep sensing by creating and employing local partner networks. Cross-cultural agility and competency in foreign languages help ARSOF tap the latent combat power within a population. ARSOF leverage this power to sense deep in denied areas. People living under the enemy's A2/AD "bubble" may retain the agility to circumvent the tactical challenges associated with foreign military sensors. ARSOF must develop and maintain the

capability to develop local civilian networks to see and sense the physical, virtual, and cognitive vulnerabilities that the joint force can exploit in deep and denied areas. ARSOF must be able to disseminate this information rapidly to national, joint, and Army databases.

c. Enable deep area fires.

(1) ARSOF coordinate deep operations with LRPF assets to disrupt and degrade the enemy's A2/AD system, particularly the integrated fires complex and the integrated air defense systems. Deep operations shape the close fight in support of conventional force maneuver. ARSOF conduct special reconnaissance to provide intelligence, weather information, and target acquisition data for engagement by Army and joint LRPF, and conduct post attack assessments. Special operations enable deep fires through sensing by technical and non-technical means. ARSOF integrate with future Army and joint fires networks to establish rapid sensor to shooter linkages that reduce latency. ARSOF employ future EMS target characterization and stimulation techniques to illuminate high value targets (HVT) for engagement by Army and joint fires assets.

(2) The convergence of forward positioned ARSOF with cyberspace and space capabilities creates the information synergy that enhances lethal and nonlethal effects in deep areas. ARSOF operators understand people and know how to employ the latent combat power within a population. Cyberspace operators know how to apply cybernetic effects within the enemy's automated battlefield. Space forces know how to execute space based activities to generate global effects. This nexus of capabilities enables the joint force to locate, target, and strike deep. The convergence of SOF, space, and cyberspace capabilities enhances military deception (MILDEC) efforts by providing access to enemy C2 nodes and information conduits.

(3) While enabling fires in the deep areas, ARSOF integrate with Space and Missile Defense Command and space-based assets to target enemy space assets as well as provide persistent pattern-of-life and targeting information for high value targets during periods of enemy domain degradation. ARSOF integrate with cyberspace forces to target enemy cyberspace capabilities by providing access and placement to cyberspace infrastructure in the deep areas. This allows unilateral or partnered targeting of critical enemy cyberspace components that may otherwise be inaccessible.

(4) ARSOF require AI enabled network systems that can utilize targeting and fire control quality data from multiple unified action partners over extended areas. Automated battle management tools minimize the human cognitive overload through a 'human on the loop' interface where sensors, shooters, and firing solutions are converged from multiple networks across domains. These solutions are monitored through common data terminals, managed by exception, creating an "any sensor, best shooter" architecture.

(5) Future sensor-to-shooter linkages must overcome the disconnected, intermittent, and low-bandwidth (DIL) conditions and cyber electromagnetic activities-affected environments of deep and denied areas. Providing information collected at the tactical edge to enable LRPF in deep areas requires both the technical means to minimize adversarial exploitation and procedural means to avoid being targeted. Special operations require varying levels of redundant communications

capabilities designed to provide reliable, long distance communication in a DIL environment, while reducing detection in support of deep fires.

d. Enable the dis-integration of the A2/AD system.

(1) ARSOF penetrate the enemy's A2/AD system, using advanced suppression and avoidance capabilities, to destroy critical nodes, including C2 facilities, ground-based air defense systems, and mid and long-range fires assets. ARSOF find, characterize, and attack components of the enemy's "kill web" globally. These components include capabilities that detect, identify, and track joint force aircraft, command and control centers that synchronize A2/AD efforts, and launch systems. Special operations conduct target identification and characterization then, through unilateral or partnered direct action or coordinated joint fires, destroy enemy delivery platforms and munitions.

(2) ARSOF human networks not only provide intelligence about high-priority systems and targets, but also offer an alternative platform to strike deep. Local populations attack enemy forces and infrastructure employing covert or clandestine means such as sabotage. ARSOF deep area preparation, done in competition, includes target analysis that identifies and illuminates critical and vulnerable components of the enemy A2/AD system. This includes components that are vulnerable to physical or virtual attack by locally recruited and trained personnel.

(3) ARSOF leverage unmanned aircraft systems (UAS) and counter-UAS capabilities in support of joint force efforts to dis-integrate an enemy's A2/AD system. With the forecasted advances in AI, computational techniques, and terahertz communications, these systems will possess capabilities far beyond those seen today. Unmanned systems are capable of operating in several domains and offer opportunities to generate lethal and nonlethal effects in denied areas. ARSOF will leverage drone technology advancements to support deep fires with future capabilities such as drone swarming. ARSOF can conduct drone ambushes and raids aimed at delivering "deep fires" in support of joint force objectives using small man-packable drones or those produced through local additive manufacturing processes. Deep targeting becomes increasingly effective when paired with technological advances such as drones that possess emergent behavior and are capable of making autonomous targeting decisions.

(4) Penetrating layers of stand-off requires lines of effort oriented on physical, virtual, and cognitive objectives in multiple domains. ARSOF combines with other deep-reach capabilities like cyberspace and space to penetrate the enemy's virtual defenses and disrupt their automated systems. Such a combination creates freedom of action because damaged information systems degrade enemy decision making. Combined arms effects from ARSOF, cyberspace, space, and electromagnetic spectrum capabilities penetrate the breadth and depth of networks, systems, processes and the computer-generated environments where people interact. Virtual penetration degrades, disrupts, or destroys critical nodes of the enemy's A2/AD system.

(5) Attacking along cognitive lines of operation influences, deceives, disrupts, corrupts, and distorts the decision making of opponents while protecting the decision making of friendly elements. ARSOF conducts influence-focused targeting to achieve influence objectives in the

minds of opposing leaders and relevant populations. Cognitive operations target the enemy's will, exploit vulnerabilities, and separate vulnerable populations from their oppressors. For example, operations targeting enemy information activities, organizations, and institutions can favorably shape popular perceptions, and influence popular actions in support of joint force objectives.

(6) Deep area preparation activities conducted during competition set the conditions for cognitive penetration and exploitation in armed conflict by aligning cognitive, physical, and virtual lines of effort (LOE). Operations in the information environment support these LOEs. Linking objectives that encompass the entire competition continuum enables cross-domain maneuver in deep and denied areas.

e. Deep area irregular partner force maneuver.

(1) ARSOF contribute to joint force operations in the deep areas by integrating local partner forces into schemes of maneuver through its core mission activities of FID and UW. ARSOF either enables the defeat of an insurgency or provides support to a resistance in support of deep area objectives. ARSOF partner forces add combat power forward of maneuvering corps and division main bodies. ARSOF leverage local resistance or insurgent assets to shape the OE, gain access and placement, and conduct attacks against enemy regional and global systems. Through its knowledge of population dynamics, ARSOF can harness and integrate disparate local assets to align sensors and drive targeting operations. Network relationships offer a particular advantage for incorporating multiple collection assets in the targeting processes. Through this approach, ARSOF can exploit vulnerabilities of enemy forces in deep fires areas.

(2) Unconventional warfare offers policymakers an option to coerce or disrupt an enemy's policies and objectives. UW is conducted against enemy governments and occupying powers in competition or conflict. ARSOF conduct UW through physical, virtual, or cognitive means in the denied area or supported from outside the denied area. UW enables resistance operations in areas where U.S. forces are not physically present, adding a virtual and cognitive dimension to deep operations. ARSOF can create a virtual axis of advance inside an enemy's interior lines that make it vulnerable to conventional attack.

(3) Remote train, advise and assist (TAA) operations may serve as a virtual vehicle that ARSOF employ to prepare local populations to conduct clandestine targeting of adversary A2/AD systems. Remote advising may include training and equipping resistance elements in a secure location outside the denied area or remotely advising and assisting these elements virtually from secure locations. Remote TAA leverages the synthetic training environment and emerging enhanced reality technologies. Remote advise and assist operations require synchronization and coordination across the U.S. government with sufficient policy, funding, authorities and permissions. TAA also requires sustainment with weapons, ammunition, supplies, and equipment from non-attributable sources; secure training facilities; and a secure sustainment infrastructure.

f. ARSOF support the close fight.

(1) ARSOF support the joint force in the close fight. They conduct special operations that support and reinforce joint force maneuver. ARSOF provide combat power, both organic and from

locally sourced forces, that supports the JTF Commander's efforts. Not all activities that comprise close operations necessarily take place near or at the point of direct enemy contact. As cited above, joint targeting operations against enemy fires capabilities in the deep areas can relieve pressure on divisions and BCTs operating in the close area. When ARSOF fight in the close or deep maneuver areas, ARSOF and CF exchange liaisons at echelon to achieve synergy and avoid fratricide. Employing ARSOF in the close area requires a deliberate decision that the importance of the objective outweighs the potential loss of ARSOF combat power.

(2) ARSOF conduct joint targeting and joint forcible entry operations to open windows of superiority in support of conventional force maneuver. Special operations are an integral part of forcible entry operations. ARSOF collect intelligence, seize key terrain, organize and train guerrilla forces, and conduct other activities that facilitate the introduction of conventional forces.[23] Joint targeting is an economy of force measure that allows other operations the time and space necessary to gain traction. Joint targeting operations create precise physical and psychological effects that foment doubt in the minds of enemy commanders, interrupt threat decision cycles, and re-orient enemy capabilities away from joint force vulnerabilities. Targets may include enemy subterranean C2 nodes, WMD sites, or strategic assets.

(3) ARSOF conducting UW operations in deep denied areas could potentially become part of the close area as conventional ground forces conduct operational maneuver and enter the same battlefield. In the event of a link-up between ARSOF and conventional forces, partner capability and capacity may support conventional operations in the close area. ARSOF partnered forces assist in securing the close area, protecting lines of communication, implementing populace and resources control, and providing local area intelligence. As noted in paragraph (1) above, ARSOF and CF conducting link ups exchange liaisons at echelon.

(4) ARSOF psychological operations (PSYOP) forces conduct operations and activities in the deep areas to draw enemy attention away from SOF elements, and create effects across the joint operations area (JOA). Coordinated timing, content of influence messaging, and psychological actions maximize the effects of lethal fires. These effects promote joint force operations in the close fight. ARSOF psychological operations forces build partner PSYOP force capability, conduct military deception (MILDEC) to include tactical deception and deception in support of operations security (DISO). They conduct influence and shaping operations, influence-focused targeting and internet-based military information support operations (MISO) to target the enemy’s will and influence the populace. Messaging includes themes that undermine the enemy’s governance and leadership, decrease external support for enemy actions, and promote a narrative that elicits behavior favorable to the accomplishment of U.S. objectives. Messaging also includes efforts to build legitimacy for U.S. operations, prepare civilians for the impacts of high intensity combat, degrade enemy morale and promote desertion, and mitigate the effects of unintended or negative actions. These activities in the deep areas support CF operations in the close and deep maneuver areas.

(5) ARSOF CA elements conduct civil network development and engagement (CNDE) to understand the interests, functions, capabilities, and vulnerabilities of populations, government institutions, and interorganizational partners that reside or operate in and around the joint special

operations area (JSOA). CNDE encompasses the tasks of conduct civil reconnaissance (CR), conduct civil engagement (CE), produce civil network analysis and evaluation (CNA&E), civil knowledge integration (CKI), build civil networks (BCN), and mobilize civilian networks. Executing these tasks enables ARSOF to map the OE and provide commanders the situational understanding required to energize their targeting and decision making cycles, maintain operational tempo by mitigating civilian interference and prevent the loss of combat power required to deal with humanitarian crisis. ARSOF CA forces support the consolidation of gains in the operational area, in coordination with conventional CA counterparts and civil sector partners, by conducting civil-military integration (CMI) and transitional governance operations (TGO). Civil-military integration involves establishing a civil-military information-sharing architecture, conducting civil knowledge management, and establishing a civil-military integration center (CMIC). Transitional governance operations involve providing governance expertise, providing support to civil administration (SCA), and establishing transitional military authority (TMA).

g. Enable convergence through SOF command and control.

(1) The SOJTF is the SOF C2 headquarters that converges cross-domain special operations across the competition continuum. The SOJTF is an operational-level, campaign capable EAB headquarters that integrates SOF capabilities with joint, interagency, and multinational (JIM) partners in competition across the combined joint force in armed conflict. It is a modular, tailorable, and scalable joint task force designed to provide integrated, fully capable, and enabled joint special operations forces to JFCs. The SOJTF is employed as a joint special operations component under the GCC or a subordinate JFC. It consists of CF, SOF, interagency and multinational partner forces. The SOJTF provides C2 for multiple 06-level joint special operations task forces (JSOTF) and a 06-level joint special operations air component (JSOAC).

(2) The SOJTF employs SOF and CF C2, communications, and intelligence systems to share and integrate information across the joint force. The full capability of a SOJTF provides JFCs situational understanding and a mechanism to preempt enemy plans. The SOJTF enables operations in the close and deep maneuver areas while simultaneously conducting special operations in the operational and strategic deep fires areas. The SOJTF is the operational level integrator of multi-domain special operations and the headquarters where SOF cross-domain convergence occurs. The SOJTF plans and executes lethal and nonlethal effects to create windows of superiority in support of the JFC's effort to shape the operational deep fires areas. It provides complementary effects that support BCT, division, and corps maneuver in the close and deep maneuver areas.

(2) The SOJTF Commander fosters an agile mission command environment across the enterprise. In LSCO, ARSOF commanders assume that the enemy will degrade or deny the C2 systems upon which the joint force relies to execute complex maneuvers. ARSOF mission command culture focuses on decisive results, achieved by subordinate commanders exercising initiative at key times and places. ARSOF commanders enable distributed operations through mission-type orders that allow subordinate commanders to exercise initiative and assume risk within the higher commander's intent.

(3) During the transition and early stages of armed conflict, the SOJTF serves as a C2 bridge prior to the establishment of a senior level headquarters. With its primary role to provide operational level command and control of SOF, the SOJTF conducts forward-looking planning nested with that of the JFC. It provides strategic options, while seeking opportunities to maximize synergy with other components and partners. The SOJTF keeps ahead of critical resource paths, like the Air Tasking Order, ensuring processes reinforce solution convergence while retaining flexibility. It receives information and inputs from across multiple joint and interagency capabilities that are sensing deep and translates collected data and information, through either automation or a combination of human and automated analysis, into actionable intelligence and targeting options. The SOJTF provides a SOF C2 mechanism to enable the convergence of deep capabilities, either to execute fires or transfer solution options to a better-positioned headquarters. The SOJTF links military and non-military activities to ensure sustainable lethal and nonlethal fires.

(4) To enable synchronization across the JOA, the SOJTF commander may elect to employ Special Operations Command and Control Elements (SOCCE) or other liaison elements. The SOCCE is the focal point for CF-SOF coordination and the synchronization of special operations activities with other joint operations.[24] ARSOF send and receive a variety of liaison and coordination elements, such as a Special Operations Liaison Element (SOLE) to coordinate, de-conflict, and synchronize special operations air, surface, and subsurface operations with conventional operations. Liaison elements aid in executing the mission and, eliminating duplication of effort, while avoiding any disruption of ongoing operations, or loss of intelligence sources. These efforts are crucial to maintaining unity of effort, convergence, and synchronization of close and deep operations.

(5) When a GCC establishes and employs subordinate JTFs, the GCC or commander, theater special operations command (CDRTSOC), may establish and employ a SOJTF, a joint force special operations component command (JFSOCC), a special operations command-forward (SOC-FWD), or JSOAC to control SOF assets and integrate special operations requirements. The GCC establishes command and support relationships between SOF commanders and other JTF commanders.

3-6. Contributions to the return to competition

a. Consolidate gains. ARSOF contribute to the return to competition by supporting the consolidation of gains, denying enemies the ability to prolong conflict after fielded forces are defeated, and transitioning control over territory and populations to legitimate authorities. During consolidation of gains, special operations perform multiple tasks. ARSOF support the physical seizure of critical capabilities such as computer server farms, television, and radio broadcast stations. They also support the seizure of storage areas containing weapons, munitions, and WMD or its components. They can target high value individuals, enemy stay-behind networks and enemy resistance elements. Special operations activities, executed with partner political and military forces, enable the physical control of population centers and support the rapid and comprehensive use of information to shape public opinion, discredit enemy narratives, and promote friendly objectives. Special operations CA capabilities, enabled by civil networks, provide direct support

to establishing civil control, civil security, and help reestablish local governance. These actions, coupled with security force assistance and other special operations activities, reinforce the new security framework.

b. Retaining the position of advantage. To retain the nation's position of advantage, the joint force manages the transition between security and stability tasks as security requirements lessen and stability tasks increase ahead of the return to competition. In that transitional period, the roles of the supported and supporting commands will change to reflect the shift to stability and back to a competition environment. As combat and combat support forces retrograde, the headquarters managing the emerging competition environment will require forces with capabilities to achieve both stability and competition objectives. A SOJTF or JSOTF has the capability to assume the lead in stability operations that enable a return to competition and retain the nation's position of advantage.

c. Re-posture in a reframed security environment. In the reframed security environment, Army special operations reinforce partners and allies to assure their success through partner building activities, MISO and CAO. ARSOF identify and exploit new opportunities and manage risk in the reframed security environment. They continue to protect the homeland and our national interests in the fight against VEOs. Based on new opportunities, ARSOF establish a global force posture based on the new security framework.

d. ARSOF Role in securing terrain and populations. ARSOF support joint force objectives to secure terrain and populations across the MDO framework. ARSOF CA and PSYOP provide a comprehensive understanding of the civil and informational environments and work together with Special Forces Operational Detachments-Alpha (SFOD-A) to secure terrain and populations by working through and with local forces and populations to consolidate gains throughout the close and deep areas. ARSOF legitimize U.S. efforts and military activities and while isolating enemy forces and criminal elements capable of destabilizing an area. CA elements provide commanders with the capability to see, understand, engage, and shape the civil component and the civil security environment. PSYOP conducts MISO to direct the population to comply with security and safety measures as well as provide civil information on locations of food, water, shelter, and medical care. During stability operations, military information is directed at target audiences and populations who can contribute to the acceptance of friendly forces and reject enemy presence and activities in stabilized areas. Local forces trained by SFOD-As help secure terrain and counter renewed aggression of by-passed or stay-behind enemy elements. ARSOF help partners in the JOA reestablish essential services and governance in accordance with national stabilization objectives.

3-7. Supporting ideas

a. CF-SOF synergy.

(1) The joint force gains and maintains freedom of action when it optimizes the synergy between conventional and special operations. During competition, the joint force not only prepares the OE to gain and maintain physical and cognitive positions of advantage, it also uses CF-SOF synergy to maneuver forces and ideas in support of physical and cognitive objectives.

These objectives are oriented on gaining multi-domain understanding, while disrupting the enemy's decision making, timelines, and freedom of action.

(2) ARSOF work with the local population to generate alternate forms of mass and extend operational reach into dimensions of the battlefield not typically accessible by conventional capabilities. Using direct action and unconventional warfare, special operations prevent unnecessary delay of conventional forces along ground lines of operation, defeat enemy resistance where possible, secure key physical and virtual terrain, and contain enemy forces and capabilities. ARSOF MISO reduces impediments to ground maneuver created by a displaced civilian populace. ARSOF train partner forces to recognize and undermine enemy propaganda.

(3) Special operations disrupt enemy forces by attacking operational and strategic targets in advance of conventional ground maneuver elements. The joint force combines CF and SOF capabilities to mass forces with joint targeting operations in the deep areas that shape the close fight. Special operations deliver robust targeting abilities that, in conjunction with conventional fires, generate operational and strategic effects. CF-SOF synergy produces compounding dilemmas that overwhelm enemy decision-making processes, disrupt the enemy's operational tempo, and create windows of superiority for friendly maneuver.

(4) CF-SOF synergy enhances the JFC's ability to see, sense, stimulate, and strike across multiple domains, the EMS, and the information environment. This requires operating within a shared information system, where all aspects of data from one element are available for action by another element, at echelon. This is especially critical for parallel efforts among CF and ARSOF CA and PSYOP units in order to ensure unity of effort.

b. Counter WMD.

(1) ARSOF play a key role in disrupting WMD pathways and directing efforts against the acquisition, development and proliferation of chemical, biological, radiological, and nuclear (CBRN) materials in the possession of actors of concern or in sensitive locations. Countering WMD activities may include targeting WMD delivery systems, as well as an adversary's ability to assemble, stockpile, transfer, or employ WMD.

(2) CWMD operations are deliberately planned operations, actions, and investments aimed at delaying, disrupting, denying, defeating, interdicting, and exploiting (D4IE) WMD threats and associated networks along the pathway activity continuum. ARSOF conduct CWMD to control, defeat, disable, and dispose of WMD threats, and prevent the employment and proliferation of WMD. Commanders take advantage of the following capabilities as they integrate special operations into the design of deep and close operations:

- Gaining access to people, places, and things that enable the Nuclear Weapons Network (NWN).
- Interdict NWN devices, components, designated material of concern, and high value individuals to prevent the use, loss, or proliferation.
- Breach hardened facilities to include underground facilities (UGF) to D4IE nuclear WMD and other WMD threats.

- Seize and secure nuclear weapons and other WMD designated material of concern and facilitate transfer to a competent authority.
- Employ CBRN sensors to detect presence or confirm the employment of CBRN weapons.

c. Conduct personnel recovery (PR). ARSOF support joint force personnel recovery and conduct unilateral or personnel recovery with other governmental agencies or local partner elements to recover isolated, missing, detained, or captured personnel in both competition and conflict. ARSOF units' man, train, and equip to conduct nonconventional and unconventional assisted recovery. Nonconventional assisted recovery forces generally deploy into their assigned areas before offensive operations begin and provide the JFC with an on-call coordinated personnel recovery capability. ARSOF UW forces are trained to develop an unconventional assisted recovery infrastructure in denied areas through resistance-controlled escape and evasion mechanisms where other PR capabilities are either infeasible, inaccessible, or do not exist. Additionally, ARSOF support joint combat search and rescue operations in hostile territory to find and extract isolated personnel.

d. Create alternative security dilemmas.

(1) ARSOF can create multiple fronts that present compounding dilemmas for the opponent in both competition and conflict. For example, in competition ARSOF could conduct UW to coerce a competitor to abandon a favorable economic venture by raising its political, economic, and military costs. In conflict, the JFC could conduct irregular warfare as a demonstration or feint to disrupt the enemy's plans. These operations draw resources away from the enemy's main effort and relieve pressure on friendly forces. In the deep fight, ARSOF, enhanced by local partner forces, can force the enemy to deploy resources to counter friendly special operations. Forcing the enemy to counter ARSOF operations in the deep areas reduces the resources available for attacking friendly forces in the close and deep maneuver areas.

(2) ARSOF create alternative security dilemmas outside of the theater of operations in order to divert enemy resources and consume the time available for operations in the main battle area. This is especially viable when confronting aggressive behavior during competition. Using their Global SOF Network, ARSOF identify and blunt adversary adventurism in one theater while targeting adversary interests in another. In coordination with the joint force and other elements of national power, these activities may be enough to force an adversary to re-orient and abandon a plan of action. ARSOF create alternative security dilemmas to hold an adversary's military and economic interests at risk using overt, clandestine, or covert methods. This enables the joint force to regain the operational initiative and maintain a position of advantage.

(3) Special operations create cognitive and virtual dilemmas for opponents. Influence-focused targeting and cyberspace operations cause uncertainty, doubt, and lack of resolve in the minds of our adversary's leaders, forces, and populations. These operations sow uncertainty and counter adversary narratives and degrade, disrupt, or destroy adversary cyberspace capabilities, infrastructure, and equipment. An operation may create effects for various durations, levels of severity, and attribution.

e. ARSOF sustainment.

(1) When feasible, ARSOF logistical elements connect to the theater sustainment architecture, as well as with interagency and multinational partners. In 2028, ARSOF will conduct distributed operations of significant size and duration in austere or denied areas where conventional combat sustainment capabilities may not be present. The lower cost and increasing availability of threat A2/AD capabilities and sensor networks will compound the challenge of executing and sustaining distributed operations. Distributed operations may stress ARSOF logistical assets to the point of failure and preclude the sustainment of some elements.

(2) Sustaining distributed special operations in deep areas requires self-sufficiency, the ability to provide sustainment across extended distances, and a high degree of autonomy. Predictive analytic decision support tools will enable sustainment commanders to anticipate, prepare, and deliver the right commodities and services to the right place, at the right time, and in the right quantity. Innovation and improved technologies, including AI and systems that produce at, or near, the point of need further reduce ARSOF's dependency on the supply chain, enabling greater independence and enhancing autonomous activities.

(3) Technologies such as autonomous robotics, data science analytics, artificial intelligence, additive manufacturing, new energy sources, and predictive analytics will reduce demand and the logistics footprint while increasing throughput.

(a) Multi-modal distribution. Distribution plans must include multiple movement corridors as well as multiple methods or modes to provide support during times when ARSOF cannot assure domain superiority.

(b) Interoperability with partners. The capability to integrate communications and other systems with allied and partner forces facilitate unified, interoperable sustainment systems.

(c) Sustainment caches. A primary logistical consideration for maneuver with local partner forces is the requirement to supply and reinforce elements operating without standard supply mechanisms. Sustainment caches could provide an alternative means for providing materiel. Sustainment caches developed during competition would provide viable options for common user logistics to MDO formations executing either semi-independent maneuver or maneuver with partner forces. ARSOF can augment sustainment caches through use of Operational Contract Support mechanisms, existing Foreign Military Sales agreements or through Acquisition and Cross-Servicing Agreements (ACSA) if conditions are permissive.

(4) ARSOF medical sustainment.

(a) The organization of the ARSOF health support system is determined by the joint force's mission, the threat, intelligence, anticipated number of patients, duration of the operation, the theater patient movement policy, available lift, medical logistics (MEDLOG) capabilities, force health protection (FHP) and hospitalization requirements. The TSOC 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 (MEDEVAC), Role 2 or Role 3 medical capabilities.

(b) The JFC may augment ARSOF units with Role 2 medical teams and damage control surgery (DCS) capabilities. Doctrinally, GCC service capabilities provide Role 3 support (definitive surgery). ARSOF HSS includes limited resources of medical, critical care management, casualty evacuation, patient holding, and primary care capabilities. Theater or JTF Role 2 medical teams and DCS capabilities may augment ARSOF operational headquarters. ARSOF may rely on CF assets for evacuation of casualties and medical treatment facilities. The ARSOF headquarters surgeon must work with the JTF and GCC surgeons to ensure that a Role 3 medical facility is in the evacuation system for the movement of casualties requiring definitive surgery.

(c) ARSOF operational elements, at echelon, employ unmanned ground, air, and water-borne delivery and medical and casualty evacuation systems, leverage local civilian 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 and 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.

(d) For ARSOF, the ability to produce the materials necessary for medical support remotely fundamentally changes the way organizations think about force projection and protection. Advances in additive manufacturing, predictive analytics, internet of things (IoT), automation, and AI will provide expanded opportunities for ARSOF units to deliver medical sustainment. ARSOF will explore tech-integrated approaches to field medicine to enable long-term distributed operations in denied areas. These advanced capabilities could support self-aid, or treatment via local medical providers for isolated individuals and provide ARSOF operators with the ability to produce pharmaceuticals, medical devices, and replacement tissue and organs. ARSOF will take advantage of innovative medical solutions that enhance Soldier protection as well as innovative delivery and evacuation solutions.

f. Complex terrain.

(1) Operating in dense urban terrain requires empowered operators who can move among the population, conduct commercial activities, and transmit high concentrations of digitized information. The urban security environment is severely restricted because hostile security forces control access to supplies, movement, and communications.

(2) The critical challenge for special operations in dense urban terrain below armed conflict is maintaining sufficient concealment of personnel, capabilities, and actions. In armed conflict, the critical challenge is to protect forces and capabilities from the impacts of both friendly and enemy operations. This is particularly critical as formations disperse into numerous small teams, minimizing their exposure to detection while complicating their synchronization and control.

(3) Subterranean operations exacerbate the challenge of operating in complex terrain as operations go into tunnels, subways, underground floors of buildings, parking areas, and city service areas. Small teams must be prepared to operate independently because the reach of their communications may be localized and limited. Reinforcing lethal capabilities such as fires and air support will be constrained, requiring teams to maneuver with enough self-contained lethal capacity to inflict sufficient damage and sustain operational tempo.

g. Army Special Operations Aviation (ARSOA).

(1) The ARSOA supports ARSOF operational requirements and missions in both competition and armed conflict. ARSOA deploys globally without notice and operates in austere conditions over long distances; through complex integrated air defense systems (IADS); overwater from an afloat forward staging base; in jungle, arctic, mountain, desert, or urban environments; and in degraded and poor weather conditions.

(2) ARSOA maintains a regional focus while remaining flexible to meet global demands. The regional focus of ARSOA enables aviation assets to build and sustain valuable relationships with other ARSOF units operating in the region as well as with partner nation forces. Regional focus enhances the cultural awareness and aviation expertise necessary to operate successfully in those environments.

(3) In competition below armed conflict, ARSOA supports ground SOF by moving personnel and equipment including transporting and sustaining surrogate forces. In armed conflict, ARSOA extends the joint force's reach into the deep fires areas through its detection avoidance, aerial refueling, and technical capabilities. Its offensive capabilities enable ARSOA to attack deep targets to help dis-integrate an enemy's A2/AD system. ARSOA contributes to the intelligence and weather pictures through their capabilities to integrate data and share information across significantly large geographic areas.

h. 75th Ranger Regiment. The 75th Ranger Regiment plans and conducts special operations in competition and armed conflict against strategic and operational targets in pursuit of national or theater objectives. Rangers conduct military operations independently as well as jointly with conventional forces, other SOF, and interagency personnel. Rangers perform complex infantry missions with TTPs and capabilities beyond the expertise or resources of conventional infantry, airborne, or air-assault units. Ranger direct action operations are usually deep-penetration raids or interdiction operations against targets of strategic or operational significance. Rangers may conduct direct action operations within conventional or multinational force areas of operation throughout the range of military operations through close coordination. Direct action missions for Rangers typically include joint forcible entry operations, airfield seizures, and the capture or destruction of targets.

i. ARSOF use of publicly available information (PAI). ARSOF monitor PAI for situational awareness during competition and armed conflict. As the proliferation of mobile digital devices increases and the use of digital information capabilities continue to become increasingly prevalent,

the ability of ARSOF to provide situational awareness, warning indicators, and weather information from PAI takes on greater significance in establishing and retaining a position of information dominance. ARSOF intelligence personnel conduct open-source intelligence (OSINT) collection to support preparation of the environment, tip and cue an adversary's plans or intentions, and provide essential elements of mission planning and lethal and nonlethal target development. During conflict, OSINT collection supports deep, denied area sensing, and can provide battle damage assessments and sentiment analysis of the populace.

j. Counter threat finance. ARSOF deny, disrupt, destroy, and defeat threat finance systems in coordination and cooperation with a broad range of Army, DOD, U.S. government and international partners. ARSOF CA, PSYOP, finance, and comptroller Soldiers contribute significantly to the ability to understand threat and international financial systems, identify patterns of activity, track the movement of money globally, coordinate with other government departments, and interdict the adversary's finances at critical opportunities. Conducting counter threat finance as an element of both counter threat networks and irregular warfare provides the joint force the ability to present additional dilemmas to actors ranging from violent extremist organizations through rogue regimes up to great powers.

Chapter 4
Conclusion

a. The *Army Futures Commend Concept for Special Operations* challenges Army leaders to visualize the conduct of multi-domain operations with the integration of special operations. In competition, ARSOF support MDO by preparing the environment, influencing behavior, advancing partnerships, countering adversaries' plans and activities, and responding quickly and precisely to crisis. ARSOF activities in the ***contact layer*** mitigate risk by setting deterrence conditions early and providing warnings and indicators of hostile intentions. ARSOF function as an initial crisis response force in the ***blunt layer*** to delay or disrupt hostile actions if deterrence fails. In the ***surge layer***, ARSOF mobilize populations to generate locally developed mass, counters hostile influences, and expands the range of combined-arms options for the joint force.

b. In LSCO, ARSOF human intelligence activities such as military source operations; counterintelligence activities; airborne, maritime, and ground-based signals intelligence; tagging, tracking, and locating; and intelligence, surveillance, and reconnaissance enable the joint force to see and sense deep in denied areas. Deep sensing enables long-range fires to disrupt the enemy's A2/AD systems. ARSOF maneuver and strikes deep—unilaterally or by, with, and through local irregular partner forces—to penetrate and dis-integrate critical stand-off nodes such as C2 facilities, weapons launch and recovery sites, munition storage areas, transport capabilities, and lines of communication. The convergence of joint and Army conventional and special operations presents enemy commanders with multiple and compounding dilemmas that will delay, disrupt, or destroy their ability to counter joint force initiatives. Army special operations contribute to the return to competition by supporting the consolidation of gains, denying the enemy's ability to prolong conflict after fielded forces are defeated, and transitioning control over territory and populations to legitimate civilian authorities.

Appendix A
References

Army regulations, DA pamphlets, FMs, and DA forms are available at https://armypubs.army.mil/. TRADOC publications and forms are available at https://adminpubs.tradoc.army.mil/index.html. Joint publications are available at https://www.jcs.mil/Doctrine/.

Section I
Required References

ADP 1
The Army

ADP 3-0
Operations

ADP 3-05
Army Special Operations

FM 3-0
Operations

JP 3-05
Special Operations

TRADOC Pamphlet 525-3-1
The U.S. Army in Multi-Domain Operations, 2028

Section II
Related References

Army Cyber Command. (04 October 2019). ARCYBER Information Paper. *SUBJ: Army Cyber Command transformation to Information Warfare Command*. Ft. Belvoir, Virginia, USA: U.S. Army Cyber Command.

Army Cyber Command. (10 July 2019). *Information Warfare Foundational Study: Introducing Information Warfare* (U//FOUO) Working Draft. Ft. Eustis, VA: U.S. Army Cyber Command.

Army Futures Command, Futures and Concepts Center, Future Warfare Division. (27 August 2019). *Future Study Plan 2019, Operationalizing Artificial Intelligence for Multi-Domain Operations* . Fort Eustis, VA: U.S. Army Futures Command.

Barton, F., & von Hippel, K. (2008). *Early Warning? A Review of Conflict Prediction Models and Systems.* Washington, DC: Center for Strategic and International Studies.

Chairman of the Joint Chiefs of Staff. (7 April 2017). *CJCSI 3110.05F Military Information Support Operations Supplement to the Joint Strategic Capabilities Plan.* Washington, DC: Joint Chief of Staff, J7.

Chessen, M. (2017). *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy.and What Can Be Done About It.* Washington DC: Atlantic Council.

Department of Defense. (January 2020). *Dictionary of Military and Associated Terms.* Washington, DC: Department of Defense.

Freier, N. P., Bado, C. M., Bolan, C. J., Hume, R. S., & Lissner, J. M. (2017). *At Our Own Peril: DoD Risk Assessment in a Post-Primacy World.* United States Army War College, Strategic Studies Institute. Carlisle Barracks: United States Army War College Press.

Headquarters, Department of the Army. (31 July 2019). *Army Doctrine Publication No. 3-0 Operations*. Washington, DC: Headquarters, Department of the Army.

Headquarters, Department of the Army. (31 July 2019). *Army Doctrine Publication No. 6-0 Mission Command: Command and Control of Army Forces*. Washington, DC: Headquarters, Department of the Army.

Headquarters, Department of the Army. (6 March 2015). *Army Training Publication 6-01.1 Techniques for Effective Knowledge Management*. Washington, DC: Headquarters, Department of the Army.

Headquarters, Department of the Army. (9 January 2014). *Field Manual No. 3-05 Army Special Operations*. Washington, DC: Headquarters, Department of the Army.

Headquarters, Department of the Army. (4 April 2017). *Field Manual No. 3-12 Cyberspace and Electronic Warfare Operations*. Washington, DC: Headquarters, Department of the Army.

Headquarters, U.S. Army Training and Doctrine Command. (21 December 2018). *TRADOC Pamphlet 525-3-8 The U.S. Army Concept for Multi-Domain Combined Arms Operations At Echelons Above Brigade 2025-2045*. Fort Eustis, VA: Headquarters, U.S. Army Training and Doctrine Command.

Joint Chiefs of Staff. (19 October 2016). *Joint Concept for Human Aspects of Military Operations (JC-HAMO).* Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (16 March 2018). *Joint Concept for Integrated Campaigning*. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (25 July 2018). *Joint Concept of Operating in the Information Environment (JCOIE)*. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (3 June 2019). *Joint Doctrine Note 1-19 Competition Continuum*. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (20 October 2016). *Joint Doctrine Note 3-16 Joint Electromagnetic Spectrum Operations.* Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (14 July 2016). *Joint Operating Environment 2035, The Joint Force in a Contested and Disordered World.* Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (27 November 2012, Incorporating Change 1, 20 November 2014). *Joint Publication 3-13, Information Operations.* Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (31 January 2018). *Joint Publication 3-33 Joint Task Force Headquarters.* Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (28 September 2018). *Joint Publication 3-60, Joint Targeting.* Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (20 March 2012). *Joint Publication 6-01 Joint Electromagnetic Spectrum Management Operations*. Washington, DC: Joint Chiefs of Staff.

Masterman, J. C. (2012). *The Double Cross System: the incredible story of how Nazi spies were turned into double agents.* USA: Lyons Press (Kindle Edition).

Operationalizing Deep Knowledge White Paper. (15 April 2016). Retrieved June 26, 2019, from United States Army Special Operations Command: https://www.soc.mil/USASOCTalks/OperationalizingDeepKnowledge.html.

Rempler, K. (16 October 2019). *Army Times*. Retrieved from Army Cyber lobbies for name change this year, as information warfare grows in importance: https://www.armytimes.com/news/your-army/2019/10/16/ausa-army-cyber-lobbies-for-name-change-this-year-as-information-warfare-grows-in-importance/.

Scoble, R., & Israel, S. (2017). *The Fourth Transformation: How Augmented Reality & Artificial Intelligence Will Change Everything.* United States: Patrick Brewer Press (Kindle Edition).

Secretary of Defense. (19 January 2018). *Summary of the National Defense Strategy of the United States of America*. Washington, DC: Department of Defense.

Thomas, J., Stillion, J., & Rehman, I. (2014). *Hard ROC 2.0: Taiwan and Deterrence Through Protraction.* Washington, DC: Center for Strategic and Budgetary Assessments.

White House. (December 2018). *National Security Strategy of the United States of America.* Washington, DC: The White House.

Appendix B
Key Required Capabilities

B-1. Introduction
This appendix reflects required capabilities (RCs) necessary to conduct operations as described in this concept. The RCs for this concept were binned into warfighting functions.

B-2. Warfighting function RCs

a. Command and control.

(1) RC 1-1. Future ARSOF require the ability to share information and intelligence to the fullest extent possible in competition and conflict against a near-peer adversary or enemy with joint services and partner forces to create a crowdsource-like, multi-angle, multi-dimension picture of the operational environment that is unhindered by differing information exchange procedures and protocols. (TRADOC Pamphlet 525-3-1, MDO: pg C-9 paras C-5 b & d and pg D-3 para b. (2); 3-4c, Harden the Operating Environment; 3-5e, Deep Area Irregular Partner Force Maneuver)

(2) RC 1-2. Future ARSOF require an enduring ability to synchronize influence operations in multiple domains during competition and conflict with the interagency, joint SOF, conventional, and partner forces to increase the speed of messaging, awareness, coordination, and approval of messaging while preventing information fratricide in both competition and armed conflict. (3-4f, Deep Area Preparation; 3-5g, Enable Convergence through Command and Control)

(3) RC 1-3. Future ARSOF require the ability to coordinate, synchronize, integrate, or deconflict ARSOF and CF activities in time, space, and purpose. (3-7A. Supporting Ideas (SOF-CF Synergy)

b. Movement and maneuver.

(1) RC 2-1. Future ARSOF require the ability to mitigate detection in competition by near-peer adversary human and technical means in environments to allow ARSOF to penetrate and operate in denied, hostile, and politically sensitive areas. (3-4f, Deep Area Preparation)

(2) RC 2-2. Future ARSOF require the ability to increase the precision of influence operations in deep fires areas conducted against near-peer adversary or enemy opposition during competition and conflict to shape the human terrain for ground maneuver. (3-4f, Deep Area Preparation; 3-5c, Enable Deep Fire Areas)

(3) RC 2-3. Future ARSOF aviation require capability to penetrate and operate within near-peer adversary or enemy denied airspace in competition and conflict. (3-4f, Deep Area Preparation; 3-5e, Deep Area Irregular Partner Force Maneuver; 3-7g, Army Special Operations Aviation)

(4) RC 2-4. Future ARSOF require an enhanced capability in competition and conflict to provide precision, cross-domain, lethal and nonlethal fires in support of ground and air special

operations forces in all operating environments. (3-4f, Deep Area Preparation; 3-5e, Deep Area Irregular Partner Force Maneuver; 3-7g, Army Special Operations Aviation)

(5) RC 2-5. Future ARSOF require the capability in competition and conflict to rapidly modify threat-warning devices in response to new, modified, and regional counter-air systems in order to understand and mitigate threats while supporting ARSOF ground forces in a denied access environment. (3-4f, Deep Area Preparation; 3-5d, Enable the dis-integration of the Anti-Access and Area Denial (A2/AD) System; 3-5e, Deep Area Irregular Partner Force Maneuver; 3-7g, Army Special Operations Aviation)

(6) RC 2-6. Future ARSOF Soldiers require the ability to understand and map adversary finances to gain a position of advantage to shape the security environment, deter aggression, provide freedom of maneuver within an operational environment and its approaches with the ultimate intent to defeat adversary financing across the competition continuum. (3-7k, Counter Threat Finance)

(7) RC 2-7. Future ARSOF require the ability to penetrate layered stand-off undetected by land, sea, and air to access denied areas in competition and conflict using current and emergent infiltration tactics, techniques, and procedures (TTP) in order to create lethal and nonlethal effects in the operational and strategic deep fires areas. (3-5a, Contributions in Armed Conflict)

c. Intelligence.

(1) RC 3-1. Future ARSOF require the ability to conduct continuous command, control, communication, computers, cyber, intelligence, surveillance and reconnaissance (C5ISR) in deep fires areas across multiple domains in conflict and in deep areas during competition against a near-peer enemy or adversary, so that sensitive activities can increase the precision of joint force targeting during MDO. (3-4f, Deep Area Preparation; 3-5d, Enable the dis-integration of the (A2/AD))

(2) RC 3-2. Future ARSOF require automated, autonomous C5ISR across multiple domains for operations in deep fires areas in conflict and in deep areas during competition to speed decision-making processes that rely heavily on synthesizing massive amounts of disparate and dynamically changing sources of data. (3-4f, Deep Area Preparation; 3-5b, Deep and Denied Area Sensing)

(3) RC 3-3. Future ARSOF Soldiers require the ability to conduct multi-domain tagging, tracking, and locating (TTL) throughout competition and conflict against a near-peer adversary or enemy HVTs to increase the precision of multi-domain fires against stationary or mobile systems. (3-4a, Campaigning in Competition; 3-5b, Deep and Denied Area Sensing)

(4) RC 3-4. Future ARSOF require the ability to provide updated information and integrated intelligence products to, and receive timely situational assessments from, Army and Joint Intelligence Enterprises affected by DIL conditions in competition and conflict during MDO

against a near-peer adversary or enemy. (3-4a, Campaigning in Competition; 3-4f, Deep Area Preparation; 3-5b, Deep and Denied Area Sensing)

(5) RC 3-5. Future ARSOF require the ability to access all joint and national data feeds in Disconnected, Intermittent, and Limited-bandwidth (DIL) environments to provide operational commanders and tactical elements a near or real time holistic depiction of the operating environment in competition and conflict against a near-peer adversary or enemy during MDO. (3-4a, Campaigning in Competition; 3-4f, Deep Area Preparation; 3-5b, Deep and Denied Area Sensing)

(6) RC 3-6. Future ARSOF require the ability to collect PAI and OSINT and integrate open-source data with classified data bases in DIL environments against near-peer adversaries in competition and enemies in conflict to improve the timeliness and quality of situational awareness, warning intelligence, weather information, sentiment analysis, preparation of the environment (PE), lethal and nonlethal target development, and battle damage assessment during MDO. (3-4a, Campaigning in Competition; 3-4f, Deep Area Preparation; 3-5b, Deep and Denied Area Sensing; 3-7i, ARSOF use of PAI)

(7) RC 3-7. Future ARSOF require the ability to identify messaging opportunities in support of the U.S. narrative, while also monitoring adversary and enemy narratives and their efforts to counter the U.S. narrative, in order to exploit opportunities in the information environment based on current events during both competition and armed conflict. (3-4c, Hardening the Operating Environment; 3-5b, Deep and Denied Area Sensing)

d. Fires.

(1) RC 4-1. Future ARSOF require the ability to converge the effects of both multi-domain fires and intelligence capabilities during competition and conflict against any adversary to increase lethality, expand maneuver, enable joint force targeting, refine intelligence and weather information, and conduct MDO in the operational and strategic deep fires areas during MDO. (3-4f, Deep Area Preparation; 3-5b, Deep and Denied Area Sensing)

(2) RC 4-2. Future ARSOF require the ability to automatically identify and characterize physical and virtual targets across multiple environments. (3-5g, Enable Convergence through SOF Command and Control)

e. Sustainment.

(1) RC 5-1. Future ARSOF sustainment elements require the ability to resupply ARSOF, proxies, and surrogates in deep areas in low visibility conditions clandestinely without adversary or enemy detection. (SILENT QUEST 19 Wargame Finding; 3-4e, Reinforce Partners and Allies; 3-5e, Deep Fires Area Irregular Partner Force Maneuver)

(2) RC 5-2. Future ARSOF require the ability to decrease the sustainment footprint or supply chain of the ARSOF operating force in the deep fires areas or denied environments thereby

reducing risk to ARSOF personnel. (3-4e, Reinforce Partners and Allies; 3-5e, Deep Fires Area Irregular Partner Force Maneuver, 3-7e, SOF Sustainment)

(3) RC 5-3. Future ARSOF require the ability to integrate with or leverage CF sustainment. (3-4e, Reinforce Partners and Allies; 3-5e, Deep Fires Area Irregular Partner Force Maneuver; 3-6b, Retaining the Position of Advantage; 3-7e, SOF Sustainment)

(4) RC 5-4. Future ARSOF require the ability to evacuate casualties from deep fires areas. (3-7e, SOF Sustainment)

(5) RC 5-5. Future ARSOF require the ability to perform enroute critical care in order to evacuate and treat casualties in all environments. (3-7e, SOF Sustainment)

f. Protection.

(1) RC 6-1. Future ARSOF operational and tactical headquarters require the ability in competition and conflict to protect facilities, personnel, and equipment from attacks originating from all domains and across the MDO battlefield framework to remain resilient and to maintain continuous control of operations tempo. (3-4b, Global Force Posture; 3-5g, Enable Convergence through SOF Command and Control)

(2) RC 6-2. Future ARSOF Soldiers require a means to defeat near-peer targeting systems in competition and conflict to deny targeting data for integrated air defense systems (IADS) and integrated fires complex (IFC). (3-4c, Harden the Operating Environment; 3-5d, Enable the dis-integration of the Anti-Access and Area Denial ((A2/AD) System)

(3) RC 6-3. Future ARSOF require home-station protection of families, installations, facilities, systems, logistics, and strategic transportation against cyberattacks and information warfare in the strategic support area to enable reliable, rapid force projection and uninterrupted operations across the competition continuum. (2-1, The Future Operational Environment for ARSOF; TRADOC Pamphlet 525-3-1, MDO, pg C-4, para C-2. (4) (a))

(4) RC 6-4. Future ARSOF require the ability to overcome near-peer adversary or enemy communication detection, denial, and degradation capabilities in contested electromagnetic environments to increase the resiliency of C2 capabilities and retain control of operations tempo during competition and conflict. (3-4b, Global Force Posture; 3-5c, Enable Deep Area Fires)

(5) RC 6-5. Future ARSOF require ability in competition and conflict to detect chemical and biological threats during deep area operations and in low-oxygen environments to sustain operational tempo and mitigate risks of early culmination against near-peer adversaries or enemies who are capable of employing such threats. (3-4f, Deep Area Preparation; 3-5e, Deep Area Irregular Partner Force Maneuver; 3-7b, Counter WMD)

(6) RC 6-6. Future ARSOF require the ability to provide early warning of the threat's intention to employ CBRN weapons. This could be from movement of weapons from caches to

employment. Time permitting the ARSOF Soldiers can move to interdict and render the threat neutral. (3-4f, Deep Area Preparation; 3-5e, Deep Area Irregular Partner Force Maneuver; 3-7b, Counter WMD)

Appendix C
Science and Technology

> New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future.
> — *National Defense Strategy 2018*

C-1. The ARSOF approach

a. The Army has recognized that great power competition necessitates a new means of fighting. In response, it has developed the MDO concept. ARSOF's *approach to acquiring technology to support MDO focuses on equipping the operator, not providing an operator for equipment*. The key problem in developing an approach for science and technology (S&T) is getting the arc of technological change about right. The technologies below singly or in combination will provide tools for future ARSOF. Every technology listed except one is currently at Technology Readiness Level (TRL) 2 or higher. They hold forth promise of availability within the 2028–2035 timeframe envisioned by MDO. For a listing of TRLs, see Appendix C - Annex 1.

b. ARSOF operations.

(1) ARSOF units of action will operate in a very different environment than that of today. ***However, humans will still be more important than hardware***. ARSOF will need to develop innovative forms of creating locally developed mass, enabled by exponentially changing technology. ARSOF will need to break out of the Industrial Age organizational and personnel management paradigms if it is to adapt to the socio-technological changes that are coming. Changes in technology will drive the need for an enhanced suite of survivability countermeasures to prevent increasingly capable adversary reconnaissance and surveillance systems from acquiring ARSOF Soldiers and units. This will impel ARSOF to operate in a manner similar to an autonomous swarm—in pulses of activity.

(2) ARSOF units will often need—depending on the mission profile—to operate in the open or to "hide in plain sight". They will also have to cope with the operational, legal, moral, and ethical impacts of human augmentation—both friendly and adversary. Because of the decreasing cost and increasing availability of such technologies as AI, nanotechnology, additive manufacturing, robotics, and gene-editing techniques such as clustered regularly-interspaced short palindromic repeats (CRISPR), super-empowered individuals will become a problem requiring attention.[25] These factors will also affect the ARSOF approach to sustainment, making it depend more on non-standard logistical approaches.

c. Technology converges to produce exponential effects.

Figure C-1. Exponential Convergence. *Five converging technologies will drive the exponential development of increasingly capable Artificial Intelligence.*

(1) The National Intelligence Council's *Global Trends 2035* and the Joint Chiefs of Staff *Joint Operating Environment 2035* points out an ever-increasing rate of technological change, the growth of mega-cities, and the diffusion of cutting-edge technology into the hands of both state and non-state actors.[26] Over the next ten to twenty years, the world will experience dramatic changes in technology, many of which will affect how ARSOF operate. Businesses are investing billions of dollars into tech startups associated with information technologies. Commercial enterprises recognize the tremendous advantages associated with combining AI and quantum computing to make sense of increasingly large volumes of data. Rapid understanding of complex data has monetary value, ensuring these trends will continue into the foreseeable future. A noted technologist and futurist, observed that the five emerging technologies noted in figure C-1 are driving an exponential growth in AI.[27] He postulates that this growth rate will approximate that of Moore's Law, doubling in power while dropping in price every two years. Increasingly capable AI will in turn accelerate the development of each of the five converging technologies. U.S. adversaries will undoubtedly seek to harness those trends to accomplish their ends.

(2) Another futurist of note, predicts that soon AI will be both cheap and ubiquitous. He uses electricity as a comparison to illustrate the future of AI in society. In addition to being cheap and ubiquitous, it will also be diffuse, running many of the processes of society without even being noticed—until it does not work. He forecasts, "You'll simply plug into the grid and get AI as if it were electricity. It will enliven inert objects, much as electricity did more than a century past."[28] AI will enable the robotics and autonomous systems (RAS) that will be a significant part of future military operations and warfare. In fact, AI will enable every future technology discussed in this paper.

Figure C-2. ARSOF will converge technologies to attack the adversary.

(3) ***When countering future adversaries, ARSOF will converge a wide variety of technology and technical means to enable operations in competition and conflict***. While they possess insufficient capacity to *defeat* an adversary, they can employ ARSOF units of action supported by advanced technologies to create opportunities for conventional forces to exploit. ARSOF can advise and assist irregular partner forces in denied areas as they conduct sabotage against key infrastructure that supports strategic or operational objectives. They can train irregular partner forces to attack key adversary C2 nodes or other targets or target sets. They can also conduct

unilateral operations in the physical, cognitive, and virtual realms to destroy key infrastructure, dislocate enemy operations, converge the effects of space, cyberspace, intelligence and fires, or secure isolated personnel.

d. Data is an operational enabler.

(1) Data gleaned from the IoT and social media and processed by AI will be a vital operational enabler for ARSOF in competition and conflict. It will allow ARSOF to support the joint force in altering the risk calculus of our adversaries to prevent conflict. ***Avoiding adversary strengths during competition, it will allow the joint force to position forces and ideas that present the adversary with multiple dilemmas.*** In the virtual and cognitive realms, social media data can fine-tune our messaging. ***This wealth of available data should also enable AI to perform predictive templating with high degrees of accuracy***. This would allow the joint force to plan and execute operations during competition in the physical, virtual, and cognitive dimensions of the contact or blunt layers from a position of advantage.

(2) Data can illuminate misinformation. Analyzed by AI, adversary IoT and social media data will develop patterns that can indicate adversary misinformation efforts. Similarly, AI analyzed IoT and social media data from friendly, neutral, or hostile sources can gauge the effect of friendly messaging. An example might be if friendly messaging wanted to persuade the population to remain in place, the IoT data gleaned from smart phones or other personal devices could establish if the population was heeding the message.

e. Technology Fueled by data helps converge time horizons. Physical effects have time horizons that range from seconds to hours, but ***it's their convergence with the virtual to achieve both physical and cognitive effects that makes the temporal aspects of physical activities and operations a more critical consideration***.[29] While the NDS envisions the contact layer as a competitive space, it does not rule out lethal or nonlethal engagements. Virtual effects occur at or near the speed of light.[30] This could make a difference when operating at machine speed across continental distances.

f. Meeting the speed of change. ***As more technologies become like information technology, their speed of change becomes exponential rather than linear***. The DOD must develop a means of coping with this exponential rate of technological development across the entire range of DOTMLPF-P. Otherwise, any adversary able to buy off-the-shelf technology and adapt tactics, techniques, and procedures to use it may be able to over match our forces. Therefore, other components of the solution include:

- New organizational model
- Capability and operational transformation
- Data Science driven talent management
- Education and institutional training
- Incorporating lessons learned
- Research and Development
- Concept for the next level of digitalization and integration

g. Mission areas. In the two tables below, the mission areas will equate to the ARSOF core activities. They are:

- Unconventional warfare (UW)
- Foreign internal defense (FID)
- Counterinsurgency (COIN)
- Counterterrorism (CT)
- Countering weapons of mass destruction (CWMD)
- Security force assistance (SFA)
- Direct action
- Special reconnaissance (SR)
- Military information support operations (MISO)
- Civil Affairs operations (CAO)
- Preparation of the environment (PE)
- Hostage rescue and recovery (HRR)
- Foreign humanitarian assistance (FHA)

C-2. Part I Foundational Research Explored and Addressed

This part identifies S&T areas that are between TRL 1- 4, which can help specific missions or mission areas and are linked to required capabilities discussed in the concept. The TRL listed for each technology is an approximation.

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
Artificial General Intelligence (AGI)	ALL[31]	1-1, 2-1, 2-2, 2-5, 2-6, 3-2, 3-4, 3-6, 4-1, 4-2, 6-1, 6-2, 6-3	AGI refers to a type of artificial intelligence that is broad in the way that human cognitive systems are broad, that can do different kinds of tasks well, and that really simulates the breadth of the human intellect, rather than focusing on more specific or narrower types of tasks. The term is used to distinguish various types of artificial intelligence from each other—the terms "strong artificial intelligence" or "full artificial intelligence" are also used to discuss broader artificial intelligence goals.[32]	AGI would greatly enhance semi-autonomous unmanned systems, together with automated intelligence, targeting and decision support tools, including the ability to execute accurate human and social modeling and effects. Ultimately, AGI would produce truly autonomous systems capable of making decisions on limited amounts or data (generalization) at machine speeds. AGI would never forget, get bored, or have its attention wander from its task, but without precautions, may potentially be vulnerable to corrupted data or learning.	1
Human Machine Interface	ALL	3-1, 3-2, 3-5, 4-1	This will be either a wearable device or an implant that allows the user to communicate directly with an RAS or an AI. This could include communication through thought alone.[33]	This will allow for human-machine teaming, the combination of humans, computers, and robotics into a functioning entity ultimately guided by the human where the sum of the whole is greater than the sum of the parts (teamed autonomy).	4
Metamaterials	UW / FID / COIN / CT / CWMD / DA / SR / PE	2-1, 3-3, 6-1, 6-2, 6-5	"A metamaterial (from the Greek word μετά meta, meaning "beyond") is a material engineered to have a property that is not found in nature. They are made from assemblies of multiple elements fashioned from composite materials such as metals or plastics. Metamaterials	"Their precise shape, geometry, size, orientation and arrangement gives them their smart properties capable of manipulating electromagnetic waves: by blocking, absorbing, enhancing, or bending waves, to achieve benefits that go beyond what is possible with conventional materials."[34]	4

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
			derive their properties not from the properties of the base materials, but from their newly designed structures."		
Nanotechnology	UW / COIN / CT / CWMD / DA / SR / PE	2-1, 2-3, 3-3, 6-1, 6-2, 6-5	"Nanotechnology is the process of manipulating matter at the nanometer or atomic scale.[35]	Nanotechnology will allow the creation of materials that can yield properties that can offer exceptional attributes of strength, power, and programmable intelligence."[36] Nanotechnology would provide novel and virtually undetectable means of attacking enemy systems and personnel. Nanomaterials such as graphene could increase the stealth and durability of UAS and other equipment while lowering their weight.[37] Graphene is harder than diamond yet more elastic than rubber. It is tougher than steel yet lighter than aluminum. Graphene is the strongest known material.[38] For example, the use of nanomaterials such as graphene would allow engineers to design tougher drones with higher payloads using the same amount of power in a conventional drone.	4
Quantum Computing	ALL	1-1, 2-3, 6-1, 6-2, 6-3	Quantum computers are based on the principles of quantum physics. This provides them with tremendous computational power.	Quantum computing offers the possibility of truly secure communications[39] through quantum encryption. It will provide AI with computational power that is orders of magnitude greater than any conventional computer. It would also provide unparalleled computational power to both encrypt and break non-quantum encryption.	4
Terahertz wireless	ALL	1-1, 1-2, 2-3, 2-5, 3-1, 3-7, 4-1, 4-2, 6-4	Terahertz (THz) wireless transmitter is capable of transmitting digital data over a single channel at a speed of 105 gigabits per second (Gbps).[40]	Terahertz wireless could attain data transmission speeds comparable to fiber-optics speed in-flight and mobile metropolitan internet, allowing the use of enhanced reality technology anywhere that could receive a satellite signal. Terahertz	4

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
				wireless communication could lead to fiber-optics speed of transmission of data for ground RAS or drones in flight. Hiroshima University demonstrated this capability between ground stations and satellites in 2017. As an article in Kurzweil.ai noted, "For perspective, that's more than 100 times faster than the fastest (1 Gbps) internet connection in the U.S. or more than 3,000 times faster than the 31 Mbps available to the average U.S. household in 2014, according to an Federal Communications Commission (FCC) report. It's also ten times or more fast than the fastest rate expected to be offered by fifth-generation mobile networks (5G) for metropolitan areas around 2020."[41] The ability to send or receive such volumes of data would be a game changer.	
Virtual Assistant (VA)	ALL	1-1, 1-2, 2-1, 2-2, 2-4, 3-4, 3-7, 4-2, 6-3	A conversational, computer-generated character that simulates a conversation to deliver voice- or text-based information to a user via a Web, kiosk or mobile interface. [42] This character can take the form of an Avatar in VR/MR. VAs learn user preferences and take action to meet user needs. A current example of the technology is Siri.	VAs help decision makers to sort through data at machine speeds to come up with viable courses of action. In short, they have the potential to speed up both the observe, orient, decide, and act (OODA) loop and military decision making process (MDMP). They also can link the user to the IoT. Hacked VAs will provide a means to access and influence their users.	7/1[43]
Wearable computers	ALL	1-2, 2-1, 3-3, 3-7, 4-2, 6-5	Wearable computers and their interfaces are designed to be worn on the body, such as a wrist-mounted screen, a head-mounted display, or contact lenses to enable mobility and hands-free/eyes-free activities.[44]	Wearable computers could allow Soldiers to employ Edge AI in combat to power personal virtual assistants. This would constitute a huge step forward in the USSOCOM Hyper-enabled Operator concept. Wearable computers are already in use for mobile industrial inspection, maintenance, and the military. For example,	4[45]

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
				Massachusetts Institute of Technology (MIT) has demonstrated SixthSense, a gesture-controlled necklace device that projects digital information onto real-world objects and locations. Potential uses include display peripherals, computer-ready clothing and smart fabrics.	

Table C-1 Foundational Technologies for future ARSOF

C-3. Part II: Advanced Research and Technology

This part identifies S&T areas that are between TRL 5- 9 that can help specific missions or mission areas and are linked to required capabilities discussed in the concept. The TRL listed for each technology is an approximation.

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
Additive Manufacturing	UW / FID / COIN / CWMD / SFA / / CAO / FHA	5-1, 5-2, 5-3	Additive Manufacturing refers to a process by which digital 3D design data is used to build up a component in layers by depositing material. The term "3D printing" is increasingly used as a synonym for Additive Manufacturing. However, the latter is more accurate in that it describes a professional production technique which is clearly distinguished from conventional methods of material removal. Instead of milling a work piece from solid block, for example, Additive Manufacturing builds up components layer by layer using materials which are available in fine powder form. A range of different metals, plastics and composite materials may be used.[46]	Additive Manufacturing will allow future ARSOF Soldiers to manufacture what they need as they need it. These machines are already capable of manufacturing weapons, replacement parts, electronic components, drones, and pharmaceuticals. In the future, they have the potential to bio-print replacement organs and skin. As the technology proliferates, it has many possible applications in reducing the logistical tail of individuals and units in any environment, to include denied or hostile areas.	6
Artificial Intelligence (AI)	ALL	1-1, 1-2, 2-2, 2-5, 2-6, 3-2, 3-4, 3-6, 3-7, 4-1, 4-2, 6-1, 6-2, 6-3	Digital technologies that perform tasks that traditionally required human intelligence, such as visual perception, speech recognition, decision making and language translation. [47]	AI will enable the RAS that will be a significant part of future military operations and warfare. In fact, AI will enable every technology discussed in this paper. An example is that AI is the engine that makes VR/MR credible and believable. It allows for objects and avatars that behave in a manner, which does not stretch the credulity of the observer. It empowers the spatial computing vital to an interactive environment. It also enables VA, shortening both the OODA Loop and MDMP.	8

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
Augmented Reality (AR)	ALL	1-1, 2-5, 3-3, 3-4, 3-5, 4-2, 6-1, 6-3, 6-5	Augmented Reality (AR) is a live direct or indirect view of the physical, real-world environment whose elements are supplemented by computer-generated sensory input such as sound, video, graphics or location data.[48] Google Glass is an early example of the technology. (See Annex 2)	This technology will allow the future ARSOF Operator to draw situational awareness or operational data from the cloud unobtrusively. Empowered by AI, it would provide a means for users to visualize the battle space and to virtually work together via avatars (see below). This technology also supports the Army's Synthetic Training Environment (STE) as well as being a critical enabler for Remote TAA activities.	7
Avatars	UW / FID / COIN / CT / CWMD / SFA / MISO / PE / HRR /	1-1, 1-2, 2-5, 3-3, 3-4, 3-5, 4-2, 6-1, 6-3, 6-5	Virtual Reality (VR) [49] and Mixed Reality (MR)[50] Avatars are representations of a person in VR or MR. They mimic the actions and appearance of the person they represent. Moreover, they can currently do so anywhere with an Internet connection and the appropriate headset/hardware.	Teamed with autonomous systems, this would allow the SOF Operator to safely experience the environment within a subterranean feature or complex urban environment through the "eyes" of the autonomous system. This technology also supports the Army's Synthetic Training Environment (STE) as well as being a critical enabler for Remote TAA activities.	7
Blockchain	ALL	1-1, 4-2, 5-1, 5-2	Blockchain is an information technology based upon a series of universally accessible, encrypted digital ledgers distributed at numerous points across the Internet. It is a subset of distributed ledger technology.[51] In blockchain the digital ledgers are called a chain because changes can only be made by adding new transaction information at the end. It provides a way to "securely and transparently store information in near real time	For the joint force, the area offering the most opportunities to employ blockchain is logistics. The Federal Government is already testing blockchain in contract management, to include vendor tracking, financial commitments and transactions, schedule tracking, and performance tracking. [53] In the near future they will be used to monitor assets and ownership registries, supply chain transfers, in a manner that is cheap, auditable, and open.[54] Additionally, logisticians can use blockchain to track data from stationary or mobile assets or major end items.[55]	7

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
			thereby providing transaction confidence in a trustless environment." Blockchain and digital ledger technologies have become "tools to record, enable, and secure huge varieties of transactions, incorporating rules, smart contracts, and digital signatures among many new and emerging technologies." [52]		
Cloud computing	ALL	1-1, 1-2, 2-1, 2-2, 2-5, 3-2, 3-4, 3-6, 3-7, 4-1, 4-2, 6-1, 6-2, 6-3	"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."[56] It is common to categorize cloud computing services as infrastructure as a service (IaaS), platform as a service (PaaS) or software as a service (SaaS).	Cloud computing will allow SOF to collect, analyze, and operationalize data to a degree never before possible. The advent of remote data centers such as Amazon Web Services, Google Cloud, IBM Cloud, and Microsoft Azure allows for storage and computation to occur with only an Internet connection. The vast arrays of servers at disparate locations makes for a robust and resilient capability far superior to a local network.	8
CRISPR	ALL	6-1, 6-3, 6-5	CRISPR, which stands for *clustered regularly-interspaced short palindromic repeats*, is RNA[57] used by the immune systems of prokaryotes.[58] In effect, it is a set of genetic scissors employed by the prokaryotes to attack and render	This tool could lead to gene editing techniques that could strengthen disease resistance, improve strength, and improve mental abilities. "As the accuracy, efficiency, and cost-effectiveness of the system became more and more apparent, researchers and pharmaceutical companies	5

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
			harmless invading viruses. When employed by researchers, it relies on the Cas9 enzyme and guide RNAs to find specific, problematic segments of a gene and cut them out. In 2015, researchers discovered that this same technique could be applied to humans.	jumped on the technique, modifying it, improving it, and testing it on different genetic issues."[59]	
Directed Energy	UW / COIN / CT / CWMD / DA / SR	2-3, 2-4, 6-1, 6-3	The two most common forms of directed energy weapons are high powered microwaves and lasers.	Directed energy weapons offer the ability to engage targets without requiring a lead. Also directed energy can affect multiple targets in a single pulse. For example, microwaves have the advantage of being an area effect weapon. When they hit a target such as a drone or group of drones, they disrupt their electronics. This could lead to a crash or a set down. However, their range is comparatively short. Lasers have longer range but have to stay on their target to take effect. Working together, they have great defensive potential.	5
Directional Jammers	UW / COIN / CT / CWMD / DA / SR	2-3, 2-4, 6-1, 6-2, 6-3	Directional jammers act to interfere with signals, either between RAS and drone or their base station. Unlike omnidirectional jammers, they can jam a very narrow slice of the sky. They can also jam GPS signals. There are a number of directional jammers already on the market which can jam common frequencies used by drones.[60] [61]	Ideally, a military grade jammer used to counter drone or RAS swarms would be able to detect their communications frequency, jam it, and cause the swarm to lose at least some of its cohesion. However, as RAS/drones become increasingly capable of employing Edge AI, non-GPS Precision Navigation and Timing (PNT) and quantum communication links, jammers or any type will become increasingly ineffective.	7
Edge Artificial Intelligence	ALL	1-1, 2-2, 2-3, 2-4, 2-5, 3-1, 3-2, 3-	Edge AI allows for the application of AI within a system, without	Edge AI has the potential to truly operationalize AI throughout the battlefield. It could power individual virtual assistants, providing their users	5

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
		3, 3-5, 3-6, 4-1, 4-2, 6-1, 6-3, 6-5	requiring a link to a cloud or other systems.	with a decision edge. Edge AI also has the potential to produce RAS swarms that exhibit emergent behaviors not possible when operating alone.[62] Emergent behavior is a phenomenon observed when creatures or machines working together behave very differently than when apart. These behaviors could not be deduced from observation of a single subject. A good example of emergent behavior is displayed by ants. By themselves, ants are pretty dumb. However, when brought together in a large group, they begin to do such complex things as building tunnel complexes, farming, and defending their territory. Edge AI can also produce UAS which can out-maneuver any human pilot.[63] It can also make the individual RAS more resistant to jamming by making them autonomous.[64]	
Holographic display	ALL	1-1, 2-2	A holographic display is an image created by a photographic projection of a recording of a light field rather than an image formed by some sort of lens. It appears as a three-dimensional representation which can be seen without intermediate optics such as goggles or glasses.[65]	This will allow commanders and their staffs to visualize the battle space in real time. An Australian company has constructed the world's first multi-user holographic table, capable of tracking the eye positions and viewing angles of multiple people simultaneously and updating its models to correspond to what they're seeing from their specific angles.[66]	6
Hyperspectral Sensors	UW / COIN / CT / CWMD / DA / SR	3-1, 3-2, 3-3, 4-2, 6-1, 6-3, 6-5	Hyperspectral sensors detect light from hundreds of bands in the EMS. "While cameras (and eyeballs) identify targets by their shape or by contrasts of light and dark, hyperspectral scanners can collect reflections at various IR wavelengths and automatically determine the material that a target is made of."[67]	Hyperspectral sensors will improve the ability of Edge AI and a human operator to detect and assess incoming threats or improve targeting. Teamed with LIDAR, motion detection technology, and sound detection, hyperspectral sensors will make it very difficult for a threat to approach undetected or for a target to hide.	5

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
Improved Batteries / Power Sources	ALL	2-3, 3-1, 3-2, 4-1, 4-2, 5-1	Battery power is a limiting factor for all RAS. It is particularly problematic for drones, which have to make a tradeoff between the amount of battery they carry, their payload, and how long they can remain aloft. [68] One solution to the power challenge would be to produce longer lasting, higher capacity batteries through approaches such as lithium/sodium glass which charges ten times faster, has three times the capacity of lithium ion batteries, and is far less likely to explode or catch fire. [69] [70] Another approach would be to power the drones wirelessly while aloft from a microwave ground station.[71] The drones could orbit the ground station until a target presented itself. Then they would go into action, fully charged. A novel approach still in its infancy would be to 'refuel' the drones while aloft by replacing their batteries in flight.	Improved batteries / power sources would lighten the load of the ARSOF Soldier, improving their mobility and allowing them to operate for longer periods without resupply. Converging better batteries, microwave charging, and in flight battery replacement could also produce the improved power sources needed to produce a persistent, extended range RAS/UAS swarm.	5
IoT	ALL	1-2, 2-2, 2-5, 3-1, 3-2, 3-3, 3-7, 4-1, 6-2, 6-4, 6-5	The IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.[72] Like the Internet, the IoT is a physical layer or network whose primary function is to transport	IoT data will facilitate friendly pulse type operations. The heightened battlefield awareness it provides will allow friendly forces to maneuver physically, virtually, and cognitively though areas not under adversary control. IoT data will support joint force physical, virtual, and cognitive targeting as well increasing the precision of kinetic and non-kinetic means. Data from the IoT	6

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
			information from one point to another quickly, reliably, and securely. While speed and reliability present few problems, security is another matter. The foremost reason is that the IoT was not created with security as a primary consideration. Instead, security was an addition to the software components of the IoT.	and social media, analyzed by AI will provide SOF with advanced warning of attacks whether physical, virtual or cognitive. This will allow SOF to prevent or mitigate effects of attacks on personnel and physical assets. Protection may consist of repositioning or reconfiguring. Repositioning is simply moving the person or physical asset within physical or virtual space. Reconfiguring will consist of altering the physical or virtual signature of the person or physical asset to confuse and deceive the adversary. The IoT provides numerous reference points to wearable technology, further enhancing the fidelity of its displays/output. Data from the IoT will allow AI to proactively configure and reconfigure networks, services, and underlying physical services. Cybersecurity will be aided by data from the IoT as well as it protects, defends, and restores information systems. However, the IoT will also pose significant cybersecurity challenges for the joint force.	
Integrated multi-spectral sensors	UW / FID / COIN / CT / CWMD / SFA / MISO / PE / HRR /	3-1, 3-2, 3-3, 4-2, 6-1, 6-3, 6-5	These integrate sensors which can perceive via visible light spectrum, infrared, acoustic, and radar. Advanced optoelectronics employing graphene will be significantly lighter and 100,000 times more sensitive than conventional silicon based versions.[7374] Light Detection and Ranging (LIDAR) is a detection system which works on the principle of radar, but uses light from a laser. Currently, there is a single channel LIDAR app for	Employed in combination, they are extremely effective in mapping the environment, navigating, or detecting and engaging threats. For example, some subterranean features have natural or man-made light sources. However, operations in that environment cannot depend upon the availability of light. Instead, SOF Operators or their supporting systems would benefit from access to integrated multispectral sensors. When considering the feasibility of integrated multi-spectral sensors, it is worth noting that the typical smart phone has a dozen sensors.[77] As sensors become smaller and less costly, they will continue to proliferate.	5

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
			mobile phones. A COTS 32 channel LIDAR sensor is available for $8,000.[75] In the future, the cost of such highly capable sensors will decrease dramatically, particularly as autonomous vehicles take hold.[76]		
Meshed networks of either microsatellites, micro aerostats, micro UAS	ALL	1-1, 2-2, 2-5, 3-1, 3-2, 3-3, 4-1, 6-2, 6-4, 6-5	A mesh network (or simply meshnet) is a local network topology in which the infrastructure nodes (i.e., bridges, switches, and other infrastructure devices) connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients.	Such a network would provide a constant and very difficult to interrupt communications link between units and headquarters.	5
Mixed Reality (MR)	ALL	1-1, 2-5, 3-3, 3-4, 3-5, 4-2, 6-1, 6-3, 6-5	MR "integrates computer-generated images so tightly that users cannot tell the difference between what is real and what is virtual."[78] A current example of the technology is Microsoft HoloLens. (See Annex 2)	This technology supports the Army's Synthetic Training Environment (STE) as well as being a critical enabler for Remote TAA activities. This technology will allow the future ARSOF Operator to meet with others in a manner that allows for the meeting to be hidden in plain sight using digital avatars. The current world-wide traffic involving avatars in Massively Multiplayer Online Role Playing Games (MMORPG) has millions of players. *World of Warcraft*, a popular MMORPG, has *over 10 million subscribers* as of November 2014.[79] Such opportunities will be even more common in the future.	5/8[80]
Nanotechnology	ALL	2-1, 2-3, 3-3, 6.1, 6-2, 6.5	"Nanotechnology is the process of manipulating matter at the nanometer or atomic scale.	Nanotechnology will allow the creation of materials that can yield properties that can offer exceptional attributes of strength, power, and programmable intelligence."[81] Nanotechnology	5

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
				would provide novel and virtually undetectable means of attacking enemy systems and personnel.	
Nano-transistors	ALL	1-2, 2-1, 2-3, 3-7, 4-2, 6.5	A Nano-transistor is a transistor—the component that acts as an electronic signal switch or amplifier—that is near the scale of a billionth of a meter (or nanometer) in size.[82] Currently, 5 nanometer transistors have been developed by a number of labs.	Nano-transistors are foundational to wearable computers. It also permits the development of extremely small sensors, enables Edge AI, and is indispensable to the IoT. Nano-transistors enable the STE as well as Remote TAA	7
Precision Navigation and Timing (PNT)	ALL	2-3, 3-1, 3-2, 3-3, 3-4, 3-5, 3-6, 4-1, 5-1	PNT is a non-GPS dependent means of determining precise location for the purposes of navigation, geolocation, and targeting.	PNT maintains the situational awareness and orientation of the person or system employing it. It also enables precise mapping of terrain, subterranean features, or complex urban environments by autonomous systems or SOF operators, regardless of adversary attempts to jam or interfere.	5
Quantum communications	UW / CT / CWMD / DA / SR / MISO / PE / HRR	1-1, 1-2, 2-1, 3-4, 3-5, 3-6, 3-7, 4-2, 5.1, 6.2, 6.4	Quantum communications rely on the principles of quantum physics and are not subject to tampering by any known means.	Quantum communication can provide units and UAS with an assured link to a ground station or to each other. Based on the quantum physics concept of entanglement, these links are unaffected by any known form of electromagnetic interference. An article in IEEE Spectrum claims, "Chinese researchers are developing an airborne quantum communications network with drones as nodes. Scientists at Nanjing University in China, notes the recent explosive advances in drone technology, have designed a "quantum drone" to serve as an airborne node in a quantum network."[83]	5
Ramming Interceptors	UW / FID / CT / CWMD	6-1, 6-2,6-3	Ramming interceptors are already a reality. Small, fast, and maneuverable, these drones are designed to simply ram an	Employed by ARSOF singly or in large numbers, they could destroy a single adversary drone or severely attrite an attacking drone swarm. AerialX's "DroneBullet" interceptor is a rocket-shaped quadcopter, whose four small rotors	6

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
	/ DA / SR / PE		approaching hostile drone to bring it down.[84]	extend out from the main body. Roughly the size of a 16 oz. bottle of soda, it has onboard deep learning and visual processing that allows it to track a target from launch to impact. The Russians have demonstrated a similar interceptor.[85]	
Robotic and Autonomous Systems (RAS)	ALL	1-2, 2-1, 2-2, 2-3, 2-4, 2-5, 3-1, 3-2, 3-7, 4-1, 5-1, 5-2, 6.1, 6-2, 6-3, 6-5	Robotic and Autonomous Systems (RAS) - is an accepted term within academia and the science and technology (S&T) community and highlights the physical (robotic) and cognitive (autonomous) aspects of these systems. RAS is a framework to describe systems that have a robotic element, an autonomous element, or more commonly, both.[86] To be autonomous, a system must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation.[87] Autonomous systems combine robotics and AI to achieve their goals.	These systems will allow the future ARSOF Operator to extend their physical presence as part of a human-machine network. They will increase situational awareness; lighten the Soldier's physical and cognitive workloads; sustain the force with increased distribution, throughput, and efficiency; facilitate movement and maneuver; and protect the force. Depending on operational, legal, and ethical constraints, the operator may be in or on the loop. For example, instead of sending a person to investigate a subterranean feature, an autonomous ground or air system might be preferable. Equipped with integrated multi-spectral sensors, such systems could navigate and map subterranean or complex urban terrain features even in conditions of total darkness and of contaminated atmosphere. They could identify potential adversaries as well. Armed autonomous systems[88] could also engage and destroy any hostile persons or systems in the area. The means of engagement could range from standard projectiles to thermobaric weapons.	6/9[89i]
Virtual Assistant (VA)	ALL	1-1, 1-2, 2-5, 3-3, 3-4,	A conversational, computer-generated character that simulates a	VAs help decision makers to sort through data at machine speeds to come up with viable courses of	7/1[91]

Technology	Mission Area	Required Capability	Description	Impact	Technology Readiness Level (TRL)
		3-5, 3-7, 4-2, 6-1, 6-3, 6-5	conversation to deliver voice- or text-based information to a user via a Web, kiosk or mobile interface. [90] This character can take the form of an Avatar in VR/MR. VAs learn user preferences and take action to meet user needs. A current example of the technology is Siri.	action. In short, they have the potential to speed up both the OODA loop and MDMP. They also can link the user to the IoT. Hacked VAs will provide a means to access and influence their users.	
Virtual Reality (VR)	ALL	1-1, 2-5, 3-3, 3-4, 3-5, 4-2, 6-1, 6-3, 6-5	VR "is a computer technology that replicates an environment, real or imagined, and simulates a user's physical presence in a way that allows the user to interact with it. Virtual realities artificially create sensory experiences, which can include sight, touch, hearing and smell."[92] A current example of the technology is Oculus Rift. (See Annex 2)	This technology supports the Army's Synthetic Training Environment (STE) as well as being a critical enabler for Remote TAA activities. It is also a powerful enabler for conducting rehearsals.	5/8[93]

Table C-2 Advanced Technologies for the future ARSOF

Annex 1
Technology Readiness Levels

Table C-2-1
Technology Readiness Levels

Level	Definition	DoD DAG Description
1	Basic principles observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2	Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4	Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5	Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment.
6	System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness.
7	System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space.
8	Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9	Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

Annex 2
Enhanced Reality

a. Purpose. This annex provides an overview of the three components of enhanced reality (XR); augmented reality (AR), virtual reality (VR), and mixed reality (MR). It provides definitions for each component and provides examples of each of the six factors that differentiate the various components: display device, image source, environment, perspective, presence, and awareness.

b. Definitions.

(1) Virtual reality. A computer technology that replicates an environment, real or imagined, and simulates a user's physical presence in a way that allows the user to interact with it.

(2) Augmented reality. A live direct or indirect view of the physical, real-world environment whose elements are supplemented by computer-generated sensory input such as sound, video, graphics or location data.

(3) Mixed reality. The merging of real and virtual worlds to produce new environments and visualizations where physical and digital objects co-exist and interact in real time.

c. Display devices.

(1) VR employs special headsets or smart glasses. These devices block out normal vision and substitute virtual images.

Figure C-2-1. VR display device

(2) AR and MR employ devices, which superimpose virtual information or images without obscuring the normal field of vision. Headsets are optional. They can include holographic displays and other tech.

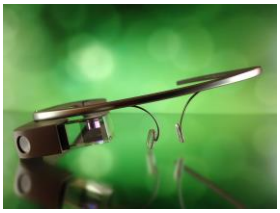


Figure C-2-2. An AR display device

Figure C-2-3. An MR display device

d. Image source.

(1) VR image sources are computer graphics or real images produced by a computer.

Figure C-2-4. VR image source

(2) AR and MR image sources combine computer generated images and real life objects. AR is mostly a superimposition of information, while MR employs virtual objects within the field of view.

Figure C-2-5. AR image source (left), MR image source (right)

e. Environment.

(1) The VR environment is fully digital.

Figure C-2-6. VR employs a fully digital environment

(2) In both, AR and MR blend both virtual and real life objects in the environment. AR accomplishes this through superposition, while MR blends the objects into the environment.

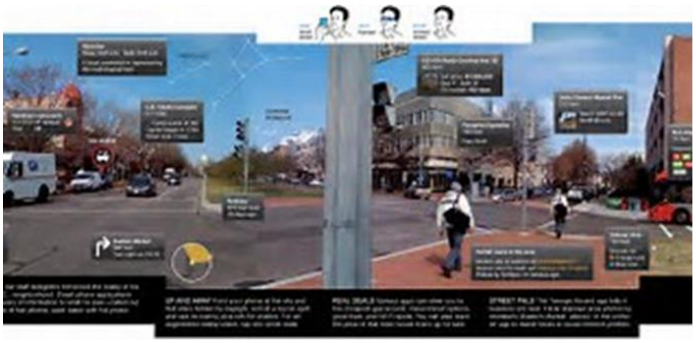


Figure C-2-7. AR environment (left), MR environment (right)

f. Perspective.

(1) In VR, virtual objects will change their perspective and size according to user's perspective in the virtual world.

Figure C-2-8. Perspective in VR matches that of the user in the virtual world.

(2) In both AR and MR, virtual objects behave based on user's perspective in the real world.

Figure C-2-9. In VR (left) and MR (right), perspective matches that of the user in the real world.

g. Presence.

(1) In VR, the user has a feeling of being transported somewhere else with no sense of the real world.

Figure C-2-10. Example of VR presence.

(2) In AR and MR, the user has the feeling of still being in the real world, but with new elements and objects superimposed

Figure C-2-11. Presence examples for AR (left) and MR (right).

h. Awareness.

(1) In AR, the user can identify virtual objects based on their nature and behavior, such as floating text that follows a user.

Figure C-2-12. Floating text in AR allows users to identify virtual elements

(2) In VR and MR, the user cannot distinguish perfectly rendered virtual objects from the real deal. However, most current systems have lag which makes perfect rendering outside the current technical capability.

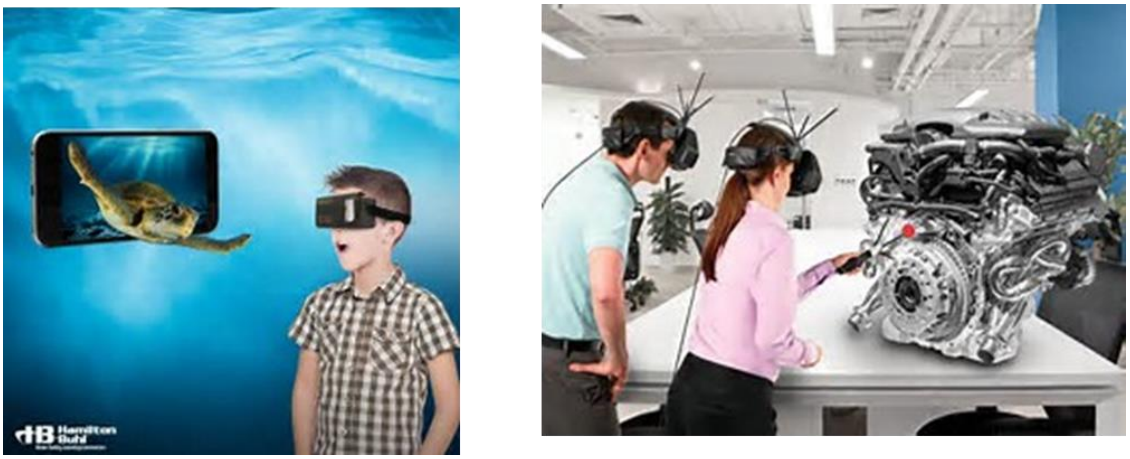


Figure C-2-13. Perfectly rendered images, whether in VR (left) or MR (right) immerse the awareness of the user.

Glossary
Section I Abbreviations

3D	three dimensional
5G	fifth-generation mobile network
A2/AD	anti-access and area denial
ACSA	acquisition and cross-servicing agreement
ADP	Army doctrine publication
AGI	artificial general intelligence
AR	augmented reality
ARSOA	Army special operations aviation
ARSOF	Army special operations forces
BCA	build civil networks
BCT	brigade combat team
C2	command and control
C5ISR	command, control, communication, computers, cyber, intelligence, surveillance and reconnaissance
CA	civil affairs
CBRN	chemical, biological, radiological and nuclear
CF	conventional forces
CI	counterintelligence
CKI	civil knowledge integration
CMI	civil military integration
CMIC	civil-military integration center
CN	counternarcotics
CNA&E	civil network analysis and evaluation
CNDE	civil network development and engagement
COIN	counterinsurgency

COP	common operating picture
COTS	commercial off the shelf
CRISPR	clustered regularly-interspaced short palindromic repeats
CT	counterterrorism
CWMD	countering weapons of mass destruction
D4IE	delaying, disrupting, denying, defeating, interdicting, and exploiting
DA	Department of Army
DCS	damage control surgery
DIL	disconnected, intermittent, and low-bandwidth
DISO	deception in support of operations security
DOD	Department of Defense
DOTMLPF-P	doctrine, organization, training, material, leadership, personnel, facilities, and policy
EAB	echelon above brigade
EMS	electromagnetic spectrum
FCC	Federal Communications Commission
FHA	foreign humanitarian assistance
FHP	force health protection
FID	foreign internal defense
Gbps	gigabits per second
GCC	geographic combatant command
GPS	global positioning system
HA	humanitarian assistance
HRR	hostage rescue and recovery
HSS	health service support
HVT	high value target
IaaS	infrastructure as a service
IADS	integrated air defense system
IFC	integrated fires complex
IoT	Internet of Things
IR	infrared radiation
IRC	information related capabilities
ISR	intelligence, surveillance and reconnaissance
JCET	joint combined exchange training
JFC	joint force commander
JFSOCC	joint force special operations component command
JOA	joint operations area
JP	joint publication
JSOA	joint special operations area
JSOAC	joint special operations air component
JSOTF	joint special operations task force
JTF	joint task force

LIDAR	light detection and ranging
LRPF	long range precision fires
LSCO	large-scale combat operations
Mbps	megabits per second
MDO	multi-domain operations
MDMP	military decision making process
MEDLOG	medical logistics
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MILDEC	military deception
MISO	military information support operations
MIT	Massachusetts Institute of Technology
MR	mixed reality
NDS	National Defense Strategy
NSS	National Security Strategy
NWN	nuclear weapons network
OE	operational environment
OIR	Operation Iraqi Freedom
OODA	observe, orient, decide, and act
OSINT	open-source intelligence
PaaS	platform as a service
PAI	publicly available information
PE	preparation of the environment
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
PNT	precision navigation and timing
PR	personnel recovery
PSYOP	psychological operations
RAS	robotics and autonomous systems
RC	required capability
SaaS	software as a service
SAR	search and rescue
SCA	civil administration
SFA	security force assistance
SOCCE	special operations command and control element
SOF	special operations forces
SOJTF	special operations joint task force
SR	special reconnaissance
STE	Army synthetic training environment
S&T	science and technology
TAA	train, advise, and assist
TGO	transitional governance operations
THz	terahertz

TMA	transitional military authority
TRADOC	U.S. Army Training and Doctrine Command
TRL	technology readiness level
TSCP	Theater Security Cooperation Plan
TSOC	theater special operations command
TTL	tagging, tracking, and locating
TTP	tactics, techniques and procedures
UAS	unmanned aircraft system
UGF	underground facility
U.S.	United States
USASOC	United States Army Special Operations Command
USSOCOM	United States Special Operations Command
UW	unconventional warfare
VA	virtual assistant
VEO	violent extremist organization
VR	virtual reality
WMD	weapons of mass destruction
XR	enhanced reality

Section II
Terms

advanced force operations
Operations conducted to refine the location of specific, identified targets and further develop the operational environment for near-term missions. (JP 3-05)

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

civil affairs operations
Actions planned, coordinated, executed, and assessed to enhance awareness of, and manage the interaction with, the civil component of the operational environment; identify and mitigate underlying causes of instability within civil society; and/or involve the application of functional specialty skills normally the responsibility of civil government. (JP 3-57)

competition
Exists when two or more actors in the international system have incompatible interests but neither seeks to escalate to open conflict. (Joint Concept for Integrated Campaigning)

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

countering weapons of mass destruction
Efforts against actors of concern to curtail the conceptualization, development, possession, proliferation, use, and effects of weapons of mass destruction, related expertise, materials, technologies, and means of delivery. (JP 3-40)

counterinsurgency
Comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes. (JP 3-24)

counterterrorism
Activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. (JP 3-26)

direct action
Short-duration strikes and other small-scale offensive actions conducted as a special operation in hostile, denied, or diplomatically sensitive environments and which employ specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets. (JP 3-05)

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

foreign humanitarian assistance
Department of Defense activities conducted outside the United States and its territories to directly relieve or reduce human suffering, disease, hunger, or privation. (JP 3-29)

foreign internal defense
Participation by civilian agencies and military forces of a government or international organizations in any of the programs and activities undertaken by a host nation government to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security. (JP 3-22)

hostage rescue and recovery
Sensitive crisis response missions in response to terrorist threats and incidents; offensive operations to support hostage rescue and recovery can include the recapture of U.S. facilities, installations, and sensitive material overseas. (JP 3-05)

intelligence operations
Intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. (JP 2-01) Referenced in ADP 3-05, ATP 2-01, ATP 3-05.1. (Army) Tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements. (ADP 2-0)

irregular warfare
A violent struggle between state and non-state actors for legitimacy and influence over the relevant population(s). (JP 1)

joint combined arms
The conduct of operational art through the integration of joint capabilities in all domains is how the joint force will achieve military advantage over threats in the security environment. (NMS 2018)

military information support operations
Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. (JP 3-13.2)

nonconventional assisted recovery
Personnel recovery conducted by indigenous/surrogate personnel that are trained, supported, and led by special operations forces, unconventional warfare ground and maritime forces, or other government agencies' personnel that have been specifically trained and directed to establish and operate irregular partner or surrogate force infrastructures. (JP 3-50)

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

operational preparation of the environment
The conduct of activities in likely or potential areas of operations to prepare and shape the operational environment. (JP 3-05)

operational reach
The distance and duration across which a joint force can successfully employ military capabilities.

preparation of the environment
An umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations. (JP 3-05)

security force assistance
Activities that support the development of the capacity and capability of foreign security forces and their supporting institutions. (JP 3-20)

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 reconnaissance
Reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or diplomatically and/or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. (JP 3-05)

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 assisted recovery
Operations executed in conjunction with or facilitated by special operations forces to return isolated personnel to friendly control in denied areas where other personnel recovery capabilities are infeasible, inaccessible, or do not exist. (ADP 3-05)

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. (JP 3-05)

End Notes

[1] As used in this concept, the term "virtual" describes something that does not physically exist, but by means of software, appears to do so; it also describes actions or information that an entity may carryout, access, or store by means of a computer, especially over a network. The implication is that ARSOF may apply capabilities in relation to virtual objectives in cyberspace that support joint force campaign plans.
[2] "The Global Operating Model describes how the Joint Force will be postured and employed to achieve its competition and wartime missions." Secretary of Defense, Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, January 19, 2018 (Washington, DC, 7). Hereafter NDS 2018.
[3] Ibid., 7.
[4] A physical, virtual, and cognitive dilemma may include but is not limited to such things as: Physical roadblocks, destroyed bridges, cratered roads; virtual misinformation and disinformation through EW or cyberspace; cognitive effects on enemy decision making process.
[5] Army Doctrine Publication 3-05 *Army Special Operations*, 31 July 2019, Headquarters, Department of the Army, Washington. DC ix.
[6] NDS 2018, 2.
[7] U.S. Army Training and Doctrine Command, *Pamphlet 525-3-1 The U.S. Army in Multi-Domain Operations 2028*, December 6, 2018, (Fort Eustis, 6).
[8] Ibid., 7.
[9] Ibid.
[10] Ibid., 8.
[11] Ibid.
[12] Ibid., 9.
[13] Ibid., 11.
[14] Ibid.
[15] A *fait accompli* attack is intended to achieve military and political objectives rapidly and then to consolidate those gains quickly so that any attempt to reverse the action by the U.S. would entail unacceptable cost and risk. (derived from *The U.S. Army in Multi-Domain Operations 2028* concept, 11).
[16] U.S. Army Training and Doctrine Command, Pamphlet 525-3-1 *The U.S. Army in Multi-Domain Operations 2028*, 7.
[17] Joint Chiefs of Staff, *Joint Doctrine Note 1-19 Competition Continuum* (Washington, DC: Joint Chiefs of Staff, 2019) 9. Hereafter JDN 1-19.
[18] TRADOC Pam 525-3-1 *The U.S. Army in Multi-Domain Operations 2028*, 25.
[19] Operational variables consist of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). Mission variables consist of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). See ADP 3-0, July 3, 2019, (Washington, DC, 1-2, 1-3).
[20] JDN 1-19, 8-11.
[21] JDN 1-19, V. The competition continuum comprises a mixture of security relationships described as cooperation, competition below armed conflict, and armed conflict.
[22] Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, March 16, 2018 (Washington, DC, 28).
[23] Joint Chiefs of Staff, *Joint Forcible Entry Operations*, May 11, 2017, Validated June 27, 2018 (Washington, DC, IV-14)
[24] Joint Chiefs of Staff, *Joint Publication 3-05 Special Operations*, July 16, 2014 (Washington, DC, III-18).
[25] Clustered regularly interspaced short palindromic repeats (CRISPR)
[26] The FOE depicted in this paper is a synthesis of the National Intelligence Council, *Global Trends: Paradox of Progress*, January 2017 (Washington, DC), and Joint Chiefs of Staff, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*, July 14, 2016 (Washington, DC).

[27] Figure C-1 from James Canton, "AL Futures" (presentation at the United States Army Special Operations Command Futures Forum, Fort Bragg, NC, August 8, 2017).
[28] Kevin Kelly, *The Inevitable, Understanding the 12 Technological Forces That Will Shape Our Future* (New York: Penguin Books, 2017), 33, Kindle Edition.
[29] David Ewalt, Defying Reality, *The Inside Story of the Virtual Reality Revolution*. (New York: Penguin Random House LLC, 2018), 96-97, Kindle Edition. Enhanced Reality (XR), in particular Virtual Reality (MR) and Mixed Reality (MR) can be effective tools to bring this about. This is because what a user experiences in VR or MR is stored in that region of the brain which deals with experience, as opposed to learning. This represents a quantum leap in the capability to influence others.
[30] Sebastian Anthony, "Researchers Create Fiber Network that Operates at 99.7% Speed of Light, Smashes Speed and Latency Records," March 25, 2013, https://www.extremetech.com/computing/151498-researchers-create-fiber-network-that-operates-at-99-7-speed-of-light-smashes-speed-and-latency-records (accessed March 5, 2020). Light slows down when it travels through a medium other than the vacuum of space. For example, it travels at ½ c in most fiber optic cable. However, new research has cut that latency significantly and light travels at 99.7% c through the new fiber optic cables.
[31] All indicates that the technology would affect every one of the ARSOF Core Activities.
[32] "Artificial General Intelligence," Technopedia, last modified March 19, 2019, https://www.techopedia.com/definition/31618/artificial-general-intelligence-agi (accessed February 24, 2020).
[33] IEEE Spectrum, "Startup Neurable Unveils the World's First Brain-Controlled VR Game," August 7, 2017, http://spectrum.ieee.org/the-human-os/biomedical/bionics/brainy-startup-neurable-unveils-the-worlds-first-raincontrolled-vr-game (accessed March 5, 2020).
[34] "Metamaterial," Wikipedia, last modified February 7, 2020, https://en.wikipedia.org/wiki/Metamaterial (accessed March 5, 2020).
[35] A nanometer is one billionth of a meter.
[36] James Canton, *Future Smart: Managing the Game-Changing Trends That Will Transform Your World* (Boston: Da Capo Press, 2015), 159, Kindle Edition.
[37] Berger, Michael. "'Stitching' together ultrastrong graphene films." *Nanowerk.* May 17, 2019. https://www.nanowerk.com/spotlight/spotid=52819.php (accessed November 25, 2019).
[38] Michael Berger, "'Stitching' Together Ultrastrong Graphene Films," Nanowerk. May 17, 2019, https://www.nanowerk.com/what_is_graphene.php (accessed November 25, 2019).
[39] Christianna Reedy, "China's New Quantum Communication Network Will Be 'Unhackable,'" Futurism, July 25, 2017, https://futurism.com/chinas-new-quantum-communication-network-will-be-unhackable/ (accessed March 5, 2020).
[40] "Terahertz Wireless Could Lead to Fiber-Optics Speed In-Flight and Mobile Metropolitan Internet," Kurzweili Accelerating Intelligence, February 14, 2017, http://www.kurzweilai.net/terahertz-wireless-could-lead-to-fiber-optics-speed-for-in-flight-and-mobile-metropolitan-internet (accessed November 25, 2019).
[41] "Terahertz Wireless Could Lead to Fiber-Optics Speed In-Flight and Mobile Metropolitan Internet," Kurzweili Accelerating Intelligence, February 14, 2017, http://www.kurzweilai.net/terahertz-wireless-could-lead-to-fiber-optics-speed-for-in-flight-and-mobile-metropolitan-internet (accessed November 25, 2019).
[42] "Virtual Assistant," Gartner, accessed March 5, 2020, http://www.gartner.com/it-glossary/virtual-assistant-va/.
[43] VAs with limited functionality such as Siri are already in use. The sort of VA generated by an AGI is only in the conceptual stages, hence the 7/1 rating.
[44] "Wearable Computer," Gartner, accessed March 5, 2020, http://www.gartner.com/it-glossary/wearable-computer/.
[45] Although wearable computers are in use, they have not reached a size or form (i.e., smart fabrics) to merit a TRL higher than 4.
[46] "Additive Manufacturing," EOS, accessed March 5, 2020, https://www.eos.info/additive_manufacturing/for_technology_interested.
[47] Robert Scoble and Shel Israel, *The Fourth Transformation: How Augmented Reality & Artificial Intelligence Will Change Everything* (United States: Patrick Brewer Press, 2017), 352, Kindle Edition.
[48] Scoble and Israel, 2822.
[49] Scoble and Israel, 2916. VR "is a computer technology that replicates an environment, real or imagined, and simulates a user's physical presence in a way that allows the user to interact with it. Virtual realities artificially create sensory experiences, which can include sight, touch, hearing and smell."
[50] Scoble and Israel, 2890. MR "integrates computer-generated images so tightly that users cannot tell the difference between what is real and what is virtual."

[51] For more on distributed ledger technologies, see Christina Majaski, "Distributed Ledgers," Investopedia, last modified April 26, 2019, http://www.investopedia.com/terms/d/distributed-ledgers.asp (accessed March 5, 2020); and David Mills et al., "Distributed Leger Technology in Payments, Clearing, and Settlement," Financial and Economics Discussion Series 2016-095 (Washington, DC: Board of Governors of the Federal Reserve System), https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf (accessed January 18, 2020).
[52] American Council for Technology-Industry Advisory (ACT-IAC), *Enabling Blockchain Innovation In The U.S. Federal Government, A Blockchain Primer* (Fairfax, VA: American Council for Technology-Industry Advisory, 2017), 1.
[53] Ibid., 11-12.
[54] Ibid., 13-14.
[55] Ibid., 14.
[56] "Cloud Computing," Techopedia, last modified August 7, 2018, https://www.techopedia.com/definition/2/cloud-computing (accessed February 24, 2020).
[57] Ribonucleic acid.
[58] "Prokaryotes: Single-Celled Organisms," North Carolina State University, accessed March 03, 2020, http://projects.ncsu.edu/project/bio183de/Black/prokaryote/prokaryote1.html. Prokaryotes are the smallest forms of life that can live independently. Most prokaryotes are tiny single cells, but some can form larger, multi-celled structures. The most familiar prokaryotes are bacteria.
[59] "CRISPR Is Rapidly Ushering in a New Era in Science, Futurism, March 13, 2017, https://futurism.com/crispr-is-rapidly-ushering-in-a-new-era-in-science/ (accessed March 5, 2020).

[60] Max Montero, "AFP to Acquire Shoulder-Fired Anti-Drone Directional Jammers from Singapore," Techapeek, June 05, 2019. https://www.techapeek.com/2019/06/05/afp-to-acquire-shoulder-fired-anti-drone-directional-jammers-from-singapore-maxdefense-philippines/ (accessed November 25, 2019).
[61] "RF Jammers," SECINTEL Security and Defense Technologies, accessed November 25, 2019, https://www.secintel.com/ecom-catshow/rf_jammers.html.
[62] Valerie Insinna, "Air Force's Future ISR Architecture Could Feature Drone Swarms and Hypersonics—with AI Underpinning It All," C4ISRNET, August 01, 2018, https://www.c4isrnet.com/air/2018/08/01/air-forces-future-isr-architecture-could-feature-drone-swarms-and-hypersonics-all-with-ai-underpinning-it-all/ (accessed November 25, 2019).
[63] Evan Ackerman, "JPL's AI-Powered Racing Drone Challenges Pro Human Pilot," IEEE Spectrum, December 06, 2017, https://spectrum.ieee.org/automaton/robotics/drones/jpl-ai-powered-racing-drone (accessed November 25, 2019).
[64] Patrick Tucker, "US Army Seeks Internet-of-Battlefield-Things, Distributed Bot Swarms." *American Military News*, July 24, 2017, https://americanmilitarynews.com/2017/07/us-army-seeks-internet-of-battlefield-things-distributed-bot-swarms/?utm_medium=facebook&utm_campaign=alt&utm_source=lod (accessed November 25, 2019).
[65] "Hologram," Technopedia, last modified November 10, 2015, https://www.techopedia.com/definition/15888/hologram (accessed February 24, 2020).
[66] Joel Hruska, "The First True Multi-User Holographic Table Has Been Built," Extreme Tech, August 16, 2017, https://www.extremetech.com/extreme/254215-first-true-multi-user-holographic-table-built (accessed February 24, 2020).
[67] Joe Pappalardo, "Hyperspectral Sensors: The Flying Eyes that See the Invisible," *Popular Mechanics*, June 28, 2011, https://www.popularmechanics.com/military/a6730/hyperspectral-sensors-the-flying-eyes-that-see-the-invisible/ (accessed November 25, 2019).
[68] Even Ackerman, "Swappable Flying Batteries Keep Drones Aloft Almost Forever," IEEE Spectrum, September 26, 2019, https://spectrum.ieee.org/automaton/robotics/drones/swappable-flying-batteries-keep-drones-aloft-almost-forever (accessed November 25, 2019).
[69] Tim De Chant, "Super-Safe Glass Battery Charges in Minutes, Not Hours," Nova, March 17, 2017, https://www.pbs.org/wgbh/nova/article/super-safe-glass-battery-charges-in-minutes-not-hours/ (accessed November 25, 2019).
[70] Jessica Hall, "New Solid-State Battery Chemistry with Glass Electrolyte Delivers 3 Times the Capacity," Extreme Tech, March 8, 2017, https://www.extremetech.com/extreme/245490-new-solid-state-battery-chemistry-glass-electrolyte-same-guy-pioneered-lithium-ion-cells (accessed November 25, 2019).

[71] "BU-412: Charging without Wires," Battery University, last modified September 28, 2017, https://batteryuniversity.com/learn/article/charging_without_wires (accessed November 25, 2019).
[72] "Internet of Things," Garter, accessed March 5, 2020, http://www.gartner.com/it-glossary/internet-of-things.
[73] Michael Berger, "Advanced Optoelectronics with Graphene-Based Mixed-Dimensional van der Waals Heterostructures," Nanowerk. July 29, 2019, https://www.nanowerk.com/spotlight/spotid=53275.php (accessed November 25, 2019).
[74] Dexter Johnson, "Here's How Graphene Makes Photodetectors 100,000 Times as Responsive as Silicon," IEEE Spectrum, January 26, 2018 https://spectrum.ieee.org/nanoclast/semiconductors/materials/graphene-photodetectors-100000-times-more-responsive-than-silicon-photodiodes (accessed November 25, 2019).
[75] "Ouster Introduces Low-Cost, High-Resolution 32-Channel Lidar Sensor." Lidar News. November 14, 2019. https://lidarnews.com/press-releases/ouster-introduces-low-cost-high-resolution-32-channel-lidar-sensor/ (accessed March 5, 2020).
[76] Charles Murray, "LiDAR Has Applications Beyond Automotive." DesignNews, October 24, 2018. https://www.designnews.com/electronics-test/lidar-has-applications-beyond-automotive/110149840159693 (accessed November 25, 2019).
[77] Piyush Kumar Maloo, "How Many Different Sensors Are Available Inside a Smartphone?" Quora, December 12, 2016. https://www.quora.com/How-many-different-sensors-are-available-inside-a-smartphone (accessed November 25, 2019).
[78] Scoble and Israel, 2890.
[79].Bobby Bernstein, "'World of Warcraft' Back to 10 Million Subscriptions," last modified November 20, 2014, https://heavy.com/games/2014/11/world-of-warcraft-back-10-million-subscribers-buy-warlords-of-draenor-blizzard/ (accessed March 5, 2020).
[80] MR is at a stage where it could be tested for operational use. It is in the final stages of testing to support the STE.
[81] Canton, *Future Smart: Managing the Game-Changing Trends That Will Transform Your World*, 159.
[82] Margaret Rouse, "Nanotransistor," WhatIs.com, accessed March 5, 2020, http://whatis.techtarget.com/definition/nanotransistor.
[83] Charles Choi, "World's First 'Quantum Drone' for Impenetrable Air-to-Ground Data Links Takes Off," IEEE Spectrum, June 18, 2019, https://spectrum.ieee.org/tech-talk/computing/networks/quantum-drone (accessed November 25, 2019).
[84] Kelsey Atherton, "When You Can't Jam a UAV Signal, Drone-on-Drone Violence Will Do Just Fine," C4ISRNET, May 17, 2019, https://www.c4isrnet.com/unmanned/2019/05/17/when-you-cant-jam-a-uav-signal-drone-on-drone-violence-will-do-just-fine/ (accessed November 25, 2019).
[85] Kelsey Atherton, "If This Rocket Is So 'Dumb,' How Does It Ram Enemy Drones Out of the Sky?" C4ISRNET, April 23, 2019, https://www.c4isrnet.com/unmanned/2019/04/23/russian-robot-will-ram-drones-out-of-the-sky/ (accessed November 25, 2019).
[86] Maneuver, Aviation, and Soldier Division, Army Capabilities Integration Center, U.S. Army Training and Doctrine Command, *The U.S. Army Robotic and Autonomous Systems Strategy*, March 2017 (Fort Eustis, 7, 24).
[87] Definitions for intelligent system, autonomy, automation, robots, and agents see Lawrence Shattuck, Transitioning to Autonomy: A Human Systems Integration Perspective," *(p*resentation at Naval Postgraduate School, Monterey, CA, March 11, 2015), https://human-factors.arc.nasa.gov/workshop/autonomy/download/presentations/Shaddock%20.pdf (accessed November 25, 2019).
[88] Department of Defense, *Department of Defense Directive Number 3000.09, Autonomy in Weapons Systems*, November 21, 2012, (Washington, DC: 13) defines an autonomous weapons system as. "A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation."
[89] Some RAS, particularly UAS are already in use. Others, such as ground systems are still under development.
[90] "Virtual Assistant," Gartner, accessed March 5, 2020, http://www.gartner.com/it-glossary/virtual-assistant-va/.
[91] VAs with limited functionality such as Siri are already in use. The sort of VA generated by an AGI is only in the conceptual stages, hence the 7/1 rating.
[92] Scoble and Israel, 2916.
[93] VR is in full use in the STE. It is being tested for use in remote TAA.