AFC Pamphlet 71-20-3

Army Futures Command Concept for Intelligence 2028

18 September 2020

This page intentionally left blank

Foreword

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

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.

Army intelligence is inherently multi-domain as it collects from and against multiple domains and has access to partners that cover gaps in Army information collection capabilities. In competition the Army relies on its intelligence capabilities as a key element in preparing the operational environment and understanding threat capabilities and vulnerabilities. Throughout the competition continuum, Army intelligence provides commanders and staffs at each echelon needed situational awareness to visualize and command a battle in all domains, the electromagnetic spectrum, and the information environment and to converge organic and external capabilities at decisive spaces.

This concept describes the key challenges, solutions, and supporting capabilities required to enable Army intelligence 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 Army intelligence forces, 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 Commander
United States Army Intelligence Center of Excellence

After nearly two decades fighting the Global War on Terror, the Army is pivoting to prepare for competition or large scale combat operations against a near-peer or peer threat. Our organizations, tools, and training have all focused on a decentralized fight against an asymmetric threat. The Joint Force dominated most domains and held significant technological advantages across the battlefield. To successfully transition from the battlefields of Iraq and Afghanistan to potential large scale combat operations, the Army must change. In December 2018, the Army published a new operating concept, Multi-Domain Operations, in response to new threat capabilities.

Intelligence has long been a multi-domain warfighting function, integrating and synchronizing collection from all domains, to support situational understanding and decision-making across echelons. Army intelligence has always been out front in the competition fight. The shift to large scale combat operations requires commanders to see farther, understand sooner, and share wider than ever before. The Army selected an aim point of 2028 for initial capability and 2035 for full capability. Army intelligence eagerly accepts this challenge.

The transition of Army intelligence to support the MDO AimPoint Force 2035 is already in progress. Institutional learning identified capability gaps, and organizational, materiel, and training solutions are underway to mitigate those gaps. Affecting change takes time, and our clock is ticking.

This concept outlines the plan Army intelligence will execute to deliver capability to the MDO AimPoint Force 2035 and beyond. It describes the organizational, material, and training changes already begun and identifies future efforts that will improve that capability. These changes will allow commanders to see farther, understand faster, and share wider across the competition continuum. They will improve interoperability across the intelligence points of presence and with unified action partners.

Finally, none of these changes will work without the right people. The Army's most valuable resource is people. Army intelligence is no exception to this rule. Finding, recruiting, training, and managing the right Soldiers, leaders, and Army Civilians will ensure success whether it is winning the competition fight, or if needed, on future battlefields.

LAURA A. POTTER
Major General, USA
Commanding

This page intentionally left blank

Executive Summary

The Army Futures Command Concept for Intelligence provides a plan for Army intelligence force modernization activities to support the Army's MDO AimPoint Force 2035 to conduct multi-domain operations across the competition continuum against peer competitors. It provides insights to support the MDO AimPoint Force beyond 2035. This concept is a modification to the ideas outlined in the 2017 U.S. *Army Functional Concept for Intelligence*: intelligence operates as an enterprise across all domains with extensive partner input. This concept extends those ideas to address the number one identified Army gap in conducting large scale combat operations: deep sensing to support long range precision fires. Leading Army intelligence modernization initiatives are organizational changes to provide capability at echelons above brigade combat team and four materiel solutions to support the deep sensing problem.

Organizational changes to support the MDO AimPoint Force 2035 enable theater army, corps, and division commanders to shape the deep maneuver and fires areas with long range precision fires and other effects. At theater level, military intelligence brigades have increased capacity and the new multi-domain task force has military intelligence capability. Expeditionary military intelligence brigades are re-purposed and re-organized to support the corps and division commanders rather than maximize downward support to the brigade combat team.

Materiel changes to support the MDO AimPoint Force 2035 converge all sensors, all shooters, and all command and control nodes with the appropriate authorities, in near real-time targeting of a threat. The Multi-Domain Sensing System provides a future family of aerial intelligence, surveillance, and reconnaissance systems from very low altitudes to low earth orbit, which support targeting at the tactical and operational level facilitating long range surface to surface fires. The Terrestrial Layer System integrates select signals intelligence, electronic warfare, and cyberspace capabilities to enable commanders to compete and win in cyberspace and the electromagnetic spectrum. The Tactical Intelligence Targeting Access Node leverages space, high altitude, aerial, and terrestrial layer sensors to provide target nominations directly to fires systems as well as multi-discipline intelligence support to targeting and situational understanding in support of command and control. Finally, with the distributed common ground system, the Army increases speed, precision, and accuracy of the intelligence cycle.

Accompanying these initiatives are Soldier training and talent management approaches designed to maximize intelligence support to targeting and decision making. From the 2028 MDO AimPoint Force, Army intelligence will continue to improve the military intelligence corps to support the MDO AimPoint Force 2035 and beyond.

This concept identifies how Army intelligence will transform to support the Army and Joint Force against peer competitors across the competition continuum.

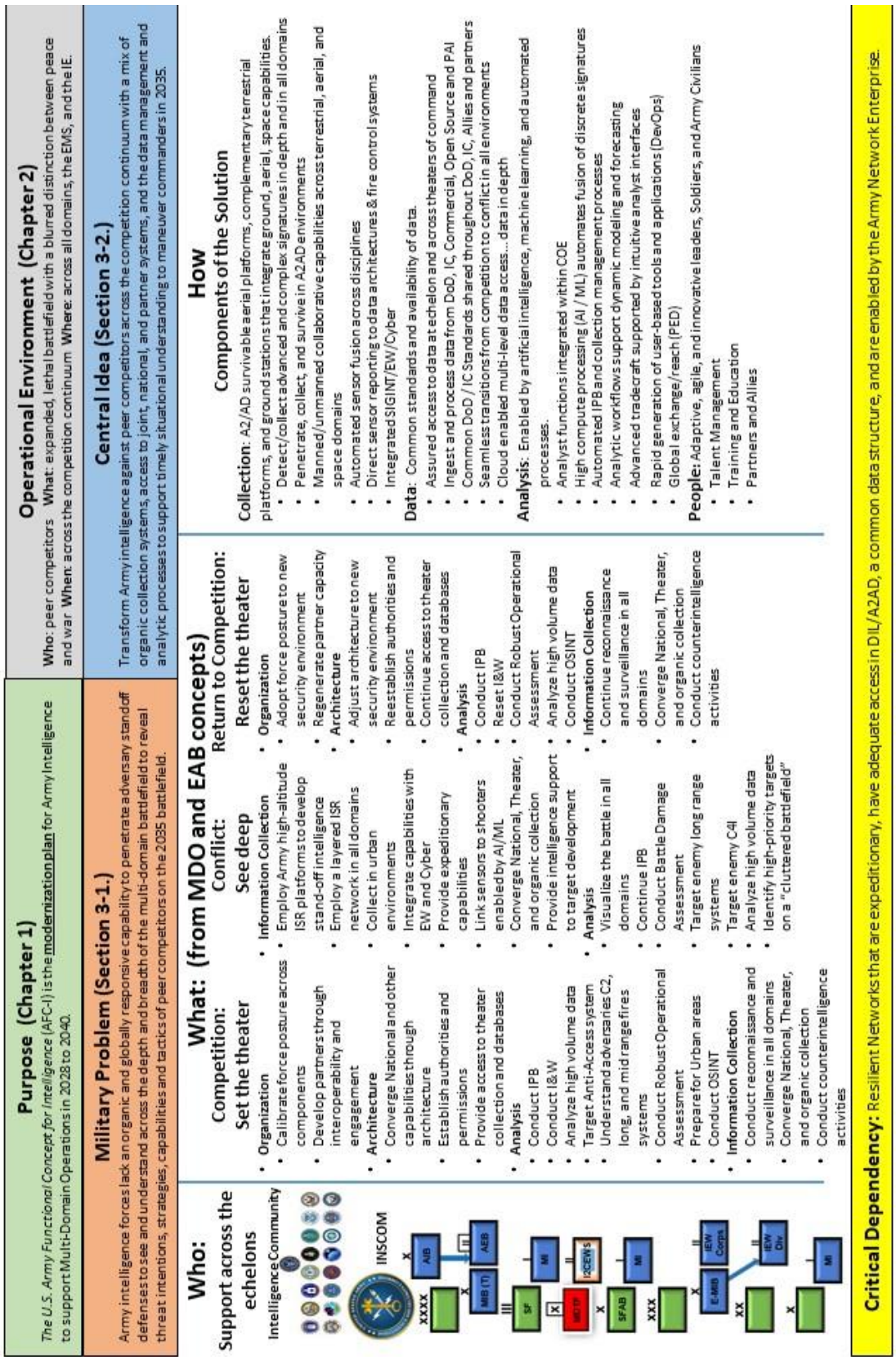

Figure 1. Logic Map

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

***AFC Pamphlet 71-20-3**

18 September 2020

Force Management

ARMY FUTURES COMMAND CONCEPT FOR INTELLIGENCE 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 pamphlet supersedes the United States (U.S.) Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-2-1 dated 25 January 2017. Because this publication is altered extensively, not all changed portions are highlighted in the summary of change.

Summary. The U.S. Army Futures Command (AFC) Pamphlet 71-20-3 describes capabilities the Army will require in the 2028 to enable multi-domain Army intelligence. This concept describes force development and modernization efforts by establishing a common framework within which to develop specific capabilities required to enable Army intelligence in the future.

Applicability. This functional 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 intelligence 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 supplementation 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, FCC (FCFC-XX), 950 Jefferson Avenue, Fort Eustis, VA 23604.

*This publication supersedes TRADOC Pamphlet 525-2-1, dated 25 January 2017.

Suggested improvements. Users are invited to submit comments and suggested improvements via The Army Suggestion Program online at https://armysuggestions.army.mil (Army Knowledge Online account required), or via DA Form 2028 to Director, FCC (FCFC-XX), 950 Jefferson Avenue, Fort Eustis, VA 23604. Suggested improvements may also be submitted using DA Form 1045.

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

Summary of Changes

Army Futures Command Pamphlet 71-20-3, Army Futures Command Concept for Intelligence

This revision dated 18 SEP 2020:

o Changes the applicability period.

o Updates the background, operational context, and assumptions that provide the basis for the concept's solutions (para 1-4, 1-5, and chap 2). Adds doctrinal implications and recent learning to chapter 2.

o Updates the military problem, central idea, and solutions (chap 3). Primary change to chapter 3 is focus on deep sensing and support to long range precision fires.

o Revises the summary and the required capabilities statements (chap 4 and appendix B).

o Adds appendices on materiel solutions, and system descriptions.

Contents

Table of figures

ARMY FUTURES COMMAND CONCEPT FOR INTELLIGENCE

Chapter 1
Introduction

1-1. Purpose

a. The *Army Futures Command Concept for Intelligence* drives modernization activities for the Army intelligence force of 2028. It identifies the key challenges, solutions, and supporting capabilities required to enable Army intelligence to support multi-domain operations (MDO) across the competition continuum against near-peer and peer competitors to accomplish campaign objectives and protect U.S. national interests. This publication provides a plan for Army intelligence force modernization as described in Army Regulation 5-22 and describes a pathway to modernize Army intelligence. While this publication supersedes the previous concept, it does not rescind previous and ongoing capability development work.

b. This concept poses and answers the following questions:

(1) How have changes in the threat changed the way Army intelligence enables the force?

(2) What are the doctrinal and policy implications that limit Army intelligence from supporting commanders in MDO?

(3) What are the shortcomings in Army intelligence as demonstrated in recent experimentation and other events?

(4) What specific capabilities must Army intelligence adjust or develop to support future combined arms operations?

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

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

1-4. Assumptions

a. Most critical assumption. The most critical assumption is adequate network access. It is described in four parts:

(1) Department of Defense (DOD) information networks will be robust, reliable, secure, and resilient enough to support the demands of Army intelligence.

(2) The network will connect a sufficient number of sensors to the appropriate processing, exploitation, and dissemination (PED), analytic element, and decision maker to support situational understanding and targeting.

(3) Intelligence modernization efforts will engineer technologies and procedures that ease the burden on the network.

(4) Although the network will certainly be disrupted, it will still support the essential demands of operations and intelligence integration.

b. Derivative assumptions. The assumptions of TRADOC Pamphlets 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* and 525-3-8, *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045* are valid.

c. Other assumptions.

(1) Future recruits will be available to develop into intelligence professionals with the cognitive, physical, social, and technical skills needed in the future operating environment.

(2) Future Soldiers will have the skills, knowledge, and attributes to leverage intelligence community (IC) resources to help solve complex problems under conditions of uncertainty at a rapid pace.

(3) Army processes will dictate the pace of modernization.

(4) Funding will remain available for modernization.

(5) The rate of technology innovation, advancements and proliferation will continue to outpace government development and acquisition processes and render government developed capabilities viable for shorter periods.

(6) The Army will sustain legacy systems to mitigate gaps or bridge capabilities until replaced by legacy compatible modernized systems.

(7) Army intelligence will continue to see a significant increase in daily operational requirements due to increased complexities in the operational environment

(8) The proliferation of advanced threat air defense and surface to surface systems, and adversary acquisition of 5th generation fighters will continue to threaten U.S. aerial systems, ground forces, and critical assets.

(9) The Army will take a unified approach integrating signals intelligence (SIGINT), electronic warfare (EW), and cyberspace operations (CO) capabilities.

(10) National intelligence agencies, particularly the specific discipline functional managers, will continue capability modernization and de-classification efforts to enable sharing with Army intelligence at echelon.

(11) Army intelligence will continue to execute the current doctrinal core competencies of intelligence operations, intelligence analysis, intelligence synchronization, and intelligence PED.[1]

(12) The Army will increase interoperability and relationships and capability with allies and partners.

(13) The Army will unify counterintelligence (CI) capabilities into a single military department CI organization to provide counterintelligence as a service.

1-5. Linkage to other concepts

a. The U.S. Army Operating Concept (AOC). The AOC describes how Army forces operate in multiple domains. Army intelligence is inherently multi-domain as it collects from and against multiple domains and has access to partners who cover gaps in Army information collection capabilities. The central idea of the AOC addresses defeating layered stand-off, including anti-access (A2) and area denial (AD) systems. This concept describes an expansion of current Army intelligence capabilities designed to defeat A2AD challenges across the competition continuum.

b. Multi-Domain Combined Arms Operations at Echelons Above Brigade (EAB) Concept. The EAB concept addresses roles of echelons division through theater army across the competition continuum. It also includes support to the national level and to coalition forces. This concept describes actions at EAB in the critical competition period, during armed conflict, and during return to competition. This concept supports the ideas of understanding, shaping, maintaining contact, and converging capabilities to persistently compete across the competition continuum to identify windows of superiority to gain an operational advantage.

1-6. The critical dependency

The critical dependency to this concept is resilient networks that are expeditionary, have adequate access and throughput in disconnected, intermittent, limited (DIL) and A2AD environments, have a common data structure, and are enabled by the Army Enterprise Network.

Chapter 2
Operational environment

2-1. The Operational environment (OE)

a. This chapter provides an overview of prevailing thoughts on the future OE and threats to assist in focusing the aim point for Army intelligence force modernization. The 2018 National Defense Strategy and The Joint Operating Environment 2035 both envision an increasingly complex global security environment characterized by overt challenges to international order with the reemergence of long-term, strategic competition between nations resulting in persistent disorder. This renewed competition between nations, especially with Russia and China, is the central challenge to U.S. security. Two other nations, North Korea and Iran, will also figure prominently in the future OE by sponsoring terrorism and seeking nuclear weapons. Although

terrorism will remain a persistent threat, inter-state competition is the primary concern of U.S. national security.[2] There are five interrelated trends shaping future competition and conflict.

b. Contested in all domains, the electromagnetic spectrum (EMS), and the information environment. Since the end of the Cold War the United States enjoyed uncontested use or dominance in every domain. Integrating capabilities across the domains was not necessary to achieve desired effects. Today the Joint Force faces challenges in every domain - air, land, maritime, space, and cyberspace - and can no longer assume dominance in any domain, the EMS, or the information environment.

c. Opposed access. Operations Desert Shield and Desert Storm demonstrated the ability to quickly deploy and sustain over 200,000 troops into a distant theater.[3] The U.S.'s unparalleled ability to project power forced the Russians and Chinese to reassess their operational approach to war. Based on these ongoing reassessments both Russia and China have developed capable anti-access systems to counter the Joint Force's predictable operational approaches in armed conflict. Russia and China continue to improve these anti-access systems and are also proliferating these associated technologies and techniques to other states.

d. Increased lethality and hyperactivity: In armed conflict, Russia and China seek to achieve physical stand-off to separate elements of the Joint Force, rapidly inflict unacceptable losses on U.S. and coalition military forces, and achieve campaign objectives before the U.S. can effectively respond. The anticipated scale of lethality could encourage opponents to strike first to preclude potentially catastrophic losses. A Rand study published in 2016, *War with China: Thinking Through the Unthinkable*, states, "U.S. military advantages have steered Chinese thinking about warfighting toward taking the initiative, making sudden gains, degrading U.S. strike forces, and then limiting the ensuing conflict's geographic scope, weapons, targets, and duration."[4] Additionally, the pace and consequences of potential miscalculations could lead to hostilities. A crisis could unfold so rapidly the need to act immediately eliminates the option of a more measured and graduated approach. This thought is emphasized in *China's Revolution in Doctrinal Affairs*, a recent publication, which clearly states, "It has become possible to achieve operational objectives before an enemy can make a response - If the People's Liberation Army (PLA) fights with a high-tech and powerful enemy, we must achieve operational suddenness."[5]

e. Competition below armed conflict. Russia and China are in a state of continuous competition actively exploiting conditions to achieve their objectives without resorting to armed conflict. Fostering regional and national instability, their objectives are to create dependency of target populations and governments on Russian or Chinese political, economic, or social systems, and to fracture U.S. alliances, partnerships, and resolve. They attempt to create stand-off through the integration of diplomatic and economic actions, unconventional and information warfare (social media, false narratives, cyber-attacks), and the actual or threatened employment of conventional forces. Creating political and economic separation results in strategic ambiguity reducing the speed of friendly recognition, decision, and reaction. Through these competitive actions, Russia and China believe they can achieve objectives below the threshold of armed conflict.[6]

f. Rapid technological advancements: Rapid advances in technologies with military implications coupled with increasing availability and reduced cost are changing the security

environment. The technological edge the U.S. enjoyed is eroding or, in some cases, gone. These are the same technologies the Joint Force relies on to win the wars such as computing, "big data" analytics, artificial intelligence (AI), autonomy, robotics, directed energy, hypersonic weapons, and biotechnology. These enablers are improving at a rapid pace, becoming more affordable and ubiquitous.[7]

2-2. The threat

a. Russia. Russia desires to reassert its authority over nations on its periphery in terms of their governmental, economic, and diplomatic decisions, and change European and Middle East security and economic structures to its favor. Moscow will continue to pursue aggressively its foreign policy and security objectives by employing the full spectrum of the state's capabilities. Russia's whole of government approach and its powerful military, coupled with the threat of intervention, allows Russia to remain a major force in world affairs.

(1) Military activities in competition. Russia's leaders believe it is at war with the West. Although not necessarily in a close combat conflict, they believe such a war is increasingly possible. The Russian military plays a crucial, but not a primary role in this whole of government political warfare strategy. The mission of Russia's military is "first to intimidate and then to deter the West, acquire a usable military superiority over neighbors on Russia's frontiers and sustain the regime." To accomplish these missions Moscow is rebuilding its nuclear and conventional forces while simultaneously conducting "unrelenting asymmetric information and cyber warfare" to target "key socio-political, infrastructural institutions and grids using organized crime, media and intelligence subversion of foreign politicians, movements and parties." The goal is the ability to control all the phases and potentials for escalation throughout any crisis from start to finish.[8]

(2) Anti-access. Russian military planners have a comprehensive approach to anti-access operations including the following key components: information operations/cyberwarfare, integrated air defense systems (IADS) and space/counter-space operations.

(a) Information operations and cyberwarfare. Information operations and cyberwarfare: Russia sees information operations as a critical capability to achieve decisive results in the initial period of conflict by controlling the EMS in all dimensions of the modern battle space. Russian theorists consider cyberwarfare as an integral component of the larger domain of information warfare which should be "employed as part of a whole of government effort, along with other, more traditional, weapons".[9] Not only is information warfare a separate domain, they consider it the most important or primary domain in the current operating environment, which, "under certain circumstances, it (information warfare) can, by itself, lead to victory and the enemy's strategic capitulation."[10] Russian use of non-governmental criminal entities for cyberwarfare activities complicates U.S. response options.

(b) EW. Russia's world-class EW forces support denial and deception operations and allow identification, interception, disruption, and, in combination with traditional fires, destruction of adversary command, control, communications, and intelligence capabilities. Additionally, effective use of EW can confuse Joint Force commanders and decision-making, demoralize opposing troops, and allows Russian forces to seize the operational initiative. Russia has fielded

a wide range of ground-based EW systems to counter global positioning system, tactical communications, satellite communications, and radars. Further, military academics have suggested that EW fuse with cyber operations, allowing EW forces to corrupt and disable computers and networked systems as well as disrupt use of the EMS.[11]

(c) IADS. Russia will continue to develop and field capable air defense systems to integrate future and existing systems around a command and control (C2) structure that includes offensive and defensive systems. These efforts are intended to limit access to its territory and extend its strategic depth.

(d) Space. Russia views wars as often undeclared, fought for relatively limited political objectives, and occurring across all domains, including outer space and the information space. Russia's space program is formidable and growing in both capability and capacity. One of Russia's priorities is the modernization of its existing communications, navigation, and earth observation systems, while continuing to rebuild its electronic intelligence (ELINT) and early warning system constellations to provide high-resolution imagery, terrestrial and space weather, communications, navigation, and missile warning. Russia believes that gaining and maintaining supremacy in space will have a decisive impact on the outcome of future conflicts.[12]

(e) Counter-space. The Russian General Staff argues that disrupting foreign military C2 or information, is critical to the fast-paced, high-technology conflicts characteristic of modern warfare. Russia believes that having the military capabilities to counter space operations will deter aggression by space-enabled adversaries and enable Russia to control escalation of conflict if deterrence fails. Military capabilities they possess that provide space deterrence include the ability to strike against satellites or ground-based infrastructure supporting space operations. Russians are believed to have spoofed and jammed GPS receivers in recent conflicts. Ground-based lasers are capable of dazzling U.S. satellites.[13]

b. China. China employs an all-of-nation long-term strategy to reorder the Indo-Pacific region to its advantage by using military modernization and information operations, as well as predatory and coercive economics. China's near-term objective is Indo-Pacific regional hegemony with the ultimate goal of replacing the United States as the preeminent global power.

(1) Military activities in competition. China desires a world-class military to secure its status as a great power on the world stage and to be the preeminent power in the Indo-Pacific region. To support this goal Chinese leaders are committed to developing military power "able to fight and win wars, deter potential adversaries, and secure Chinese national interests overseas, including a growing emphasis on the importance of the maritime and information domains, offensive air operations, long-distance mobility operations, and space and cyber operations."[14] To continue its military modernization while also attempting to degrade core U.S. technological advantages, China will employ a variety of methods to acquire foreign military technologies, including targeted foreign direct investment, cyber theft, and private Chinese nationals' access to these technologies, as well as computer intrusions, intellectual property theft, and other illicit approaches.

(2) Anti-access capabilities. The results of the 1991 Persian Gulf War "sent shockwaves throughout China's military community and accelerated the PLA's modernization and shifts in

strategy"[15] to refocus military priorities away from a large standing army and nuclear weapons to focus on introducing high-technology to the force to deter, delay, and degrade intervention, especially from the U.S. To this end, China continues to develop IADS and long-range strike capabilities to counter third-party forces and allow for a range of tailored military options against Taiwan and potential third-party military intervention.

(3) Cyberwarfare capabilities. Chinese leadership consolidated the PLA's space, cyberspace, and EW capabilities into the Strategic Support Force (SSF) in 2015 to enable cross-domain synergy in "strategic frontiers." A part of this restructuring also combined cyber reconnaissance, cyberattack, and cyber defense capabilities into one organization to streamline C2. The PLA will use cyberspace capabilities to support military operations in three key areas. First, cyber reconnaissance allows the PLA to collect, often to steal, technical and operational data for intelligence and operational planning for cyberattacks. Second, the PLA will employ its cyberattack capabilities to establish information dominance in the early stages of a conflict to constrain an adversary's actions or slow mobilization and deployment by targeting network-based command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR), logistics, and commercial activities. Third, cyberwarfare capabilities can serve as a force multiplier when coupled with conventional capabilities during a conflict. The PLA also plays a role in cyber theft. In May 2014, the U.S. Department of Justice indicted five PLA officers on charges of hacking into the networks of U.S. companies for commercial gain. The PLA's SIGINT and cyberspace assets target foreign satellite, line of sight, and over-the-horizon communications, as well as computer networks.[16]

(4) Space capabilities. China sees U.S. reliance on C4ISR as an American Achilles' heel, and has expanded its arsenal to include cyberwarfare and anti-satellite weapons to degrade or destroy these capabilities.[17] The unification of China's space, SIGINT and cyberwarfare capabilities under the SSF in 2015 indicates the importance China places on the ability to target foreign satellite, line of sight, and over-the-horizon communications, as well as computer networks. This consolidating of space, cyberwarfare, and EW capabilities into the SSF enabled cross-domain synergy in "strategic frontiers."[18]

c. Other. North Korea and Iran will continue attempts at regional destabilization through their pursuit of nuclear weapons and/or terrorism. Additionally, they may serve as proxies for near-peer and peer threats in their regions, further complicating U.S. response.

(1) North Korea. Survival is paramount to the North Korean regime. It will use all means available including nuclear, biological, chemical, conventional, and unconventional weapons, forces, and tactics to gain coercive influence and leverage over South Korea, Japan, and the U.S. to remain in power.

(2) Iran. Iran is pursuing regional hegemony by fostering instability through state-sponsored terrorism as well as an increasingly capable missile program to achieve its objectives.[19] These objectives include defending allies (Hezbollah, the Syrian government, and other Shiite political entities throughout southwest Asia and the Middle East) while continuing to challenge Israel, the U.S., and Saudi Arabia.

(3) Transnational. Although inter-state competition is currently the primary concern of U.S. national security, enduring threats from transnational criminal organizations, terrorist groups, and other irregular threats will persist. A wide range of insurgents, transnational extremists, and other states is likely to exploit weak or failing central governments. An international environment with power vacuums caused by weak or failed nation-states will result in shifting alliances, partnerships, and relationships allowing transnational terrorist organizations and global cyber activist networks to exploit internal political, ethnic, or economic fractures to further their own strategic interests. Some sub- or transnational groups see the U.S. as underwriting world order and believe that delivering catastrophic damage to the U.S. homeland will serve to divert U.S. military power from interdicting them overseas. These non-state actors may launch attacks (both kinetic and non-kinetic) within the homeland to prevent the U.S. from interfering with their goals and objectives.[20]

2-3. Doctrinal implications

a. The ADP 2-0 and FM 2-0 cover the concepts and themes described in TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, adequately with only minor adjustments needed as noted below.

b. U.S. Army intelligence doctrine is grounded in published higher level combined arms doctrine. In order to affect intelligence doctrine, operations doctrine must first articulate the fundamental principles with supporting tactics, techniques, procedures, and terms and symbols to guide actions of Army forces in support of national objectives. In order to align with the MDO concept, combined arms doctrine should specifically address the below topics.

(1) Army operational level command. Army doctrine does not currently have a published doctrinal manual that addresses the Army operational level command. The initial draft of FM 3-94, Armies, Corps, and Division Operations, staffed in Jan - Feb 2020, describes a provisional, operational level Army headquarters, with no approved organizational design. If the Army chooses to create an Army operational level command other than the one currently in the Indo-PACOM Theater, combined arms doctrine should address how its functions are executed by other parts of the force.

(2) Artificial intelligence. Army doctrine does not currently address AI and how it supports decision making.

(3) Terminology. There are minor inconsistencies between the MDO concept and published doctrine.

(4) Multi-domain task force. Army doctrine does not currently have a published doctrinal manual that addresses the function, roles, and tasks of this formation in MDO. The initial draft of ATP 3-19.94, Multi-Domain Task Force, will staff in 2020.

b. The MDO and EAB concepts introduce several ideas without describing how the Army will execute them. Combined arms doctrine must provide greater details to provide a useful bridge for future U.S. Army intelligence doctrine.

(1) What is the U.S. Army's role in competition prior to armed conflict?

(2) How will the U.S. Army organize by echelon to conduct MDO?

(3) What new or expanded authorities must the Army gain and delegate to conduct MDO?

(4) How does the Army converge capabilities to create windows of superiority?

(5) What is the Army's role as part of the Joint Force in penetrating A2AD environments?

2-4. Recent learning

a. The Army conducted significant experimentation after publishing the previous AOC in October 2014 and the supporting *Army Functional Concept for Intelligence*. The Unified Quest and Unified Challenge (UC) series, Army intelligence focused Bottom Up Review (BUR) and Intelligence, Surveillance, and Reconnaissance (ISR) Table Top Exercise (TTX), a Combined Arms Center study, and derivative writings identified multiple shortfalls in the ability of Army intelligence to support large scale combat. The following are highlights of that learning.

b. The Army lacks multi-domain deep sensing, analysis, and PED for warning intelligence and A2AD targeting at all echelons division and above. The military intelligence (MI) brigade - theater (MIB (T)) lacks adequate organic capability to locate and target IADS or fires systems, provide timely warning, or continuously execute theater intelligence preparation of the battlefield (IPB) in competition or conflict. The corps expeditionary MI brigade (E-MIB) is optimized for counterinsurgency. The Army lacks responsive and integrated intelligence deep sensing capabilities, EW systems and training that support cyberspace and electromagnetic activities cell operations and support to EMS dominance.[21]

c. Army intelligence capabilities and capacities must be optimized across the echelons. Commanders at every echelon require persistent, multi-domain intelligence operations, reconnaissance, surveillance, and security. Commanders need the ability to develop situational understanding to support operations and decision-making. Manpower and grade plate reductions at corps and division exacerbate analytic gaps at tactical echelons. The Army needs modular, flexible organizations to support commanders at each echelon and weight their effort through reinforcing subordinates. Commanders need improved manned and unmanned, air and ground sensors to identify targets and determine effects.[22]

d. Army intelligence must have an architecture to support intelligence at the speed of C2. Existing IC architectures and processes are not responsive to tactical commanders' sensing requirements. Architecture must connect all points of presence -- sensors, PED, analysis, storage, decision makers, and shooters -- across all domains, command echelons, and multiple security levels. The architecture must connect joint all-domain C2 systems and joint, interagency, intergovernmental, and multinational (JIIM) partners with intelligence specific information technology systems. The architecture must be resilient, interoperable, reliable, and allow operations for short time periods in degraded and denied environments.[23]

e. Army intelligence lacks adequate deep and urban sensing. Dense urban areas have become the centers of political and economic power in the global commons. Collection cannot support commanders to shape and target across domains and the EMS. Organic collection cannot see deeply enough to support EAB commanders. Commanders cannot see into urban canyons, valleys, and subterranean areas due to urban geometry and the phenomenology of the urban environment. Electronic surveillance must accommodate the sheer volume of cellphone communications, social media postings, and financial transactions. Sensors require networking to provide cross-cueing and persistent shooter linkages. Additionally, terrestrial sensors have range limitations and aerial sensors have survivability concerns creating reliance on joint, national, other partner, and open collection means. Identity verification and identity intelligence must be able to identify threat actors.[24]

f. The Army must conduct expeditionary operations. Army intelligence must support an expeditionary Army. During competition, Army intelligence must set the theater, work with partners through regional engagement and security cooperation, and provide warning should conditions change. MIBs (T) require analysis, PED, human intelligence (HUMINT), and CI capacity for competition and additional capacity for transition and combat operations. MI units must be able to deploy rapidly, operate from austere conditions, sustain low density equipment and skill sets, and maintain situational understanding during transit. Intelligence units must balance forward and reach capabilities to meet the commander's needs.[25]

g. MDO against a near-peer or peer threat in a future operating environment requires new approaches in doctrine and training. Integrating intelligence operations, PED, and analysis in a distributed manner requires a comprehensive approach to cross domain collection and the management of responsive, distributed PED and analysis. Training at home station and at training centers requires a data rich environment, replicated theater targeting databases, and responsive simulations that bring together distributed capabilities which allow units to train as they would fight. Additionally, sustainment and replacement of low density equipment and personnel with unique technical and language skills need review.[26]

h. Army intelligence must operate in a contested, congested, and commercial cyberspace and electromagnetic environment to support and protect operations across all domains. Army intelligence, with assistance from cyberspace and EW organizations, must understand the cyberspace and electromagnetic environments, including electronic order of battle (EOB), to support and protect operations across all domains. SIGINT must integrate with cyberspace and EW capabilities during training, planning, and operations.[27]

i. Army intelligence must overcome the challenges of data volume, data velocity, data variety, and data veracity. The increase in collection volume and access to stored data have complicated meeting the timeliness and fidelity needs of commanders at all levels. All levels lack capacity to process and exploit information collection into a usable form and the follow-on dissemination for timely action. The variety and veracity of available data are overwhelming for human analysts alone and will require some degree of AI to meet the velocity of MDO decision making.[28]

j. Analysts need advanced tools to solve advanced problems at the speed decision makers require. The future operating environment is large, complex, and multi-dimensional. Analysts

will use data from every intelligence discipline collected by diverse intelligence partners, combat reporting, and an increasing array of non-traditional sources and sensors. Analysts must understand sophisticated military systems and formations, urban and other complex terrain environments, contaminated or hazardous environments, and diverse human actors with competing and often unclear motivations. Analytic efforts, including urban modeling, must begin early during competition and continue through the continuum. Analysts will need advanced tools to solve advanced problems if they are to provide critical and creative analysis to support commanders' situational understanding and decision making.[29]

k. Commanders require understanding of certain specific problem sets when conducting MDO in a future operating environment. Examples include surface and air long-range fires; littoral and other mines; chemical, biological, radiological, nuclear and weapons of mass destruction capabilities; identity intelligence; cyberspace and electromagnetic activities; and early warning intelligence.[30] Commanders must also understand the regional health threat with its associated disease and battle injury implications it presents to the force. Finally, commanders must understand the interests, functions, capabilities, and vulnerabilities of populations, government institutions, and interorganizational partners that reside or operate in or around an area of operations.

l. MI Soldiers must dominate cognitively. The multi-domain operating environment requires competent, agile, and resilient Soldiers and leaders. Operations in the future, multi-domain operating environment require Soldiers and leaders who are competent, agile, and resilient with the physical and social skills to thrive under conditions of uncertainty, rapid change, and complexity.[31]

2-5. Summary of Army intelligence challenges

The primary challenge to Army intelligence against a future near-peer or peer threat is the ability to sense and understand the depth and breadth of the battlefield and identify windows of superiority to enable maneuver to defeat A2AD systems. New sensing capabilities will stress data and analytic capabilities supporting PED, intelligence, and weather analysis. These activities will occur contested across all domains, the EMS, and the information environment.

Chapter 3
Military Problem and Components of the Solution

3-1. Military problem

Army intelligence forces lack an organic and globally responsive capability to penetrate adversary stand-off defenses to see and understand across the depth and breadth of the multi-domain battlefield to reveal threat intentions, strategies, capabilities, and tactics of peer competitors on the 2035 battlefield.

3-2. Central idea

Transform Army intelligence against peer competitors across the competition continuum with a mix of organic collection systems, access to joint, national, and partner systems, and the data

management and analytic processes to support timely situational understanding to maneuver commanders in 2035.

3-3. Solution synopsis

a. Army intelligence leverages the resources of formal JIIM partners and less permanent coalition and interorganizational partners. These capabilities and capacities hind together by architecture designed to maximize support to commanders. However, Army commanders may fall short in a theater priority that may not meet their needs in a timely fashion. Organic capability eases this problem. Therefore, the principal shift from *The U.S. Army Functional Concept for Intelligence* (2017) is the addition of organic Army deep sensing and the doctrine, organization, training, materiel, leadership and education, personnel, and facilities and policies (DOTMLPF-P) implications that will allow the Army to process, analyze, and distribute the increased collection results. The solution consists of the collection, data, analysis, and human knowledge, skills, behaviors, and preferences needed to meet the commanders' requirements across the depth of the OE.

b. Collection. Army intelligence capabilities must detect, identify, locate, and track advanced and discrete signatures across a diverse array of adversaries' organizations, systems, and capabilities throughout the depth of the battlefield exposing vulnerabilities and identifying opportunities the U.S. can exploit. Army intelligence must have the sensors to detect these signatures, the survivable platforms to position these sensors, the processes to direct these platforms to the right place at the right time, the organizations at echelon to employ the capability, and the Soldiers to ensure success. Army intelligence must have assured access to IC and non-traditional ISR and weather sensor data, be it from Army, partner, or open sources. Enemy capabilities threaten U.S. forces globally, from the continental U.S. (CONUS) homeland to the enemy homeland, and Army intelligence must collect against that threat. This capability must deliver timely information collection results to the right decision maker.

(1) The Army must detect, locate, recognize, identify, classify, and track advanced, agile, non-traditional, and complex signatures, as well as traditional and commercially available signatures generated by rapidly evolving threats in depth and in all domains, the EMS, and the information environment. Merriam Webster defines a signature as something "closely and distinctively associated and identified with someone or something." A complex signature is one that requires advanced capabilities to detect and identify. Rapid changes in technology change both the capability to observe a signature and the ability of others to disguise a signature. This capability must support targeting while facing a contested EMS and adversary attempts at denial and deception.

(2) The Army must penetrate, collect, and survive in A2AD environments. Survivable aerial platforms include ones with small signatures, ones that can overwhelm enemy defenses through sheer numbers, those capable of penetrating enemy defenses, and those able to achieve stand-off through altitude.[32] Reliable, maintainable, survivable expeditionary, terrestrial platforms with the same mobility characteristics and visual signature as supported formations, provide persistent support and complement aerial collection.[33] Ground stations will integrate ground, aerial, and

space capabilities in an open, modular, and scalable design to enable tailored mission configurations by echelon.[34]

(3) The Army must operate manned/unmanned collaborative capabilities across terrestrial, aerial, and space domains. In order to effectively deliver sensing capabilities, Army intelligence requires platforms that can survive, can suffer attrition at an acceptable rate, or that are designed for one time use (expendable).[35] A mix of manned and unmanned capabilities improves efficiency, effectiveness, and sustainability.[36]

(4) The Army must provide automated sensor fusion across disciplines. Processing at the point of collection improves correlation of detected activity, speeds entity identification, reduces burden on the network, and reduces man-in-the-loop PED requirements. It also improves the fusion of disparate reporting from multiple intelligence disciplines and other non-MI sensors. These advances improve sensor to shooter timelines and target accuracy.

(5) The Army must deliver direct sensor reporting to data architectures and fire control systems. Direct sensor reporting to common data architectures, C2 suites, and fire control systems is imperative in order to accelerate analytical and targeting processes. Processing at the sensor (also known as edge computing), an open system architecture, and common communications from the collection platform, coupled with automatic target identification and classification aided by AI and cognitive engineering, reduce targeting decision and execution cycles.

(6) The Army must integrate SIGINT, EW, and CO at all echelons. SIGINT and EW have long been complementary capabilities and part of the cyberspace approach. The integration of electronic attack (EA) and offensive cyberspace operations (OCO) with SIGINT creates temporal, spatial, and technological advantages over an enemy in the physical and cognitive domains. These capabilities will enable commanders to sequence kinetic and non-kinetic fires from a position of relative advantage.[37] Additionally, intelligence supports defensive CO.

(7) The Army must conduct identity intelligence across the competition continuum. Intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest aids targeting. People operate components of systems whether they are the commander or the technician that maintains a search radar integral to an anti-access system. Identity intelligence aids preventing peer adversaries from conducting counter intelligence operations, espionage, sabotage, surveillance, and reconnaissance against U.S. forces and partner nations to prevent collection of essential elements of friendly information. It aids warning intelligence during competition. It develops actionable identity intelligence against high value individuals, aids in the processing of enemy prisoners of war and detainees, identifies threat-actors in or near population centers and sanctuary areas, and identifies threat-actors attempting to access facilities, critical infrastructure and events.

(8) The Army must collect and report human derived information. HUMINT operations, site exploitation, and document and media exploitation provide valuable insights across the competition continuum.

c. Converged data architecture. Army intelligence professionals require assured access to relevant data at echelon from across the DOD, IC, commercial vendors, and open sources including publicly available information (PAI). Materiel developers must adhere to common data configuration and reporting standards to establish the foundation for seamless collaboration and sharing within Army C2 networks, between services, the IC, and allies within the mission partner environment to seamlessly facilitate the warfighter's ability to transition from competition to conflict, across all echelons of command, and theaters of operation. Quantum technology, AI, and other autonomous solutions will be able to rapidly ingest, sort, process and archive data at speeds and measures of performance far beyond human capacity.

(1) Assured access to data at all echelons and across theaters of command. Assured access is an architecture problem. It requires communications connectivity, permissions and credentials based on mission needs and security levels, data standards, access to tools and services, and user knowledge to find the right data at the right time. Assured access includes procedures to sanitize information to make available to coalition partners and BCTs, battalions, and companies.

(2) Ingest and process data from DOD, IC, commercial, open source, and PAI. Army intelligence needs a data fabric which enables processing, storage and use of data from the wide array of both streaming and stored data. Army intelligence must have a configurable automated normalization capability that converts data into the form and format needed for user understanding, that enables system processing, and allows consumption by an external system.[38] This applies to various data storage configurations and both structured and unstructured data.

(3) Common DOD and IC standards shared throughout DOD, IC, allies, and unified action partners. DOD efforts to standardize data requirements and build toward a universally accepted open architecture construct under the sensor computing environment (CE) will directly inform and assist in the development of this requirement. The common operating environment (COE) will support common standards.

(4) Seamless transitions between competition and conflict in all environments. Transitions stress architectures. Data volume increases greatly, temporal relevance of data may be reduced, and users increase as the force builds. Additional sensors increase not only volume, but types of data inputs as they are delivered from new enterprise points of presence. As decision cycles shorten and activities are more dynamic, data must be current. In most transitions, force buildup expands the architecture to enable access to relevant stores and new collection for new users.

(5) Data in depth through cloud enabled multi-security level data access. Cloud technology supports the constant update of flexible, intuitive, powerful tools that help analysts anticipate an adversary's actions. The cloud-based approach solves tactical storage and processing power limitations to leverage advanced analytic software applications, deliver ease of use, and provide intuitive visualization. Cloud computing provides redundancy and depth. Army intelligence needs an automated capability that identifies and extracts content from products (structured, semi-structured, unstructured), marks the source product when extraction is completed, creates links between the source product and the extracted content, and maintains and creates pedigree. This capability must meet multi-level information assurance requirements of availability, integrity, authentication, confidentiality, and non-repudiation.[39]

d. Analysis. Army intelligence professionals require high compute processing technologies paired with intuitive analyst-system interfaces to conduct doctrinal functions of the intelligence cycle. Advanced analytic tools and applications will support warning intelligence and rapid fusion of information across intelligence disciplines, terrain and weather, dynamic modeling, and forecasting of the OE and threat capabilities. Introducing AI and cognitive engineering into analytic workflows will reduce resources required to perform data intensive steps within the IPB process and intelligence production cycles while providing analysts time to apply judgment in developing predictive assessments.

(1) Analyst functions integrated within COE. COE is an approved set of computing technologies and standards that enables secure and interoperable applications to be rapidly developed and executed across six CEs: mobile/handheld CE, mounted CE, command post CE, enterprise CE, sensor CE, real time/safety critical CE. Analyst functions must be available and integrated across these CEs to increase interoperability and speed support to commanders at all levels. The Army must provide analysts with familiarization training on computation and data science, and develop tools with computational and data analysis capabilities.

(2) High compute processing, AI, and ML enable automation and fusion of advanced signatures at machine speed. Army intelligence requires access to a variety of data and computational science related tools and capabilities for processing, exploiting, and analyzing the increasing volume, variety, velocity, and veracity of disparate structured, semi-structured, and unstructured data in all functional areas to provide timely, accurate, relevant intelligence, and weather effects information to support decision making.[40] AI algorithms will support analytic tools to speed identification of target sets and aid BDA calculation. ML will enable computers to learn from data patterns as they evolve and change. AI will also aid identification of false positives resulting from adversary deception operations. Ground stations must use these tools to perform single source analysis and hasty fusion supported by automated data correlation to identify and locate dynamic targets.

(3) Automated IPB and collection management processes. Army intelligence supports the commander through the military decision making process (MDMP) and other integrating processes. IPB, targeting, battle damage assessment (BDA) aggregation, and collection management all support the commander and the operations process. Automating routine actions in these processes to improve speed and consider all relevant data will allow computers to overcome speed and data volume challenges and allow humans to apply context and render judgment.

(4) Analytic workflows support automated and dynamic activity modeling, forecasting, and automated collection management strategies. Predictive analytic workflows must support warning intelligence and be as dynamic as large scale combat. Modeling activity aids the analyst to identify and forecast threat branches, and provides the baseline for providing key indicators to tip automated and dynamic collection management models. Results and interfaces must be intuitive, easy to understand, and difficult to misunderstand. This reduces the cognitive burden in complex operations and terrain, such as dense urban areas.

(5) Advanced tradecraft supported by intuitive analyst interfaces. The Army develops, trains, and practices advanced analytic techniques to understand the spectrum of problems driven by commanders' information gaps. MDO requires IPB that analyzes all domains, the EMS, and the information environment to find the opportunities in time and space to generate overmatch, present multiple dilemmas to the enemy, and enable Joint Force freedom of movement and action. Army intelligence forces will employ advanced analytics (advanced techniques applied against complex problems) that encompass a clear analytic strategy, flexible models, and supporting tools and skills. Much of the solution may be doctrinal and training; however, analysts need tools to manipulate very large data sets, understand semantic nuances, and identify behavioral patterns.

(6) Rapid generation of user-based tools and applications. Development and operations allow Soldiers to conduct on the move operations that enable configuration changes, data curation, data exploration, data modeling, and data visualization in near-real-time based on mission need.[41]

(7) Global exchange/reach-PED[42]. Army intelligence forces conduct reach-PED and analysis to meet the commander's requirements. PED is sensor agnostic. PED is a single source intelligence activity and reach-PED allows analysts to process and exploit information from multiple sensors and maximize PED resources. Reach-PED and analysis will leverage advanced analytic software and cloud technology to provide continuous support to the commander's information requirements. Reach-PED enables continuous support to forces from peacetime activities through decisive action.

e. People: adaptive, agile, and innovative leaders, Soldiers, and Army Civilians.

(1) Talent management. People are the Army's greatest resource. The Army must identify with precision its required technical skill sets, assess the currency of those skill sets, and purposefully align those talented Soldiers, much as it identifies, assesses, and assigns linguists. The Army must determine the right additional skills for intelligence support to MDO, provide an initial and continuing education plan for Soldiers with identifiers, and properly align those Soldiers against Army requirements. The Army must identify new fields of expertise such as data scientists to recruit, assess, and develop. Increased professionalization of Army Civilians must parallel improvements in the uniformed force. The Army must reward individuals who bring specific skills needed by the Army with accessions above the entry grade level.

(2) Training and education. Army intelligence must expand training and education opportunities within the IC and civilian sources. Future training must include live, virtual, and constructive simulations to challenge Soldiers at the institution, home station, and deployed locations. The Intelligence Electronic Warfare Tactical Proficiency Trainer supports live, virtual, and collective training for MI, ISR, and PED concepts and systems. It creates a realistic, virtual GEOINT, SIGINT, all source, and HUMINT data environment for training individual and crew/collective critical system and MOS tasks. Next generation training simulations, including the ability to create massive amounts of realistic multi-disciplined intelligence data, must be included in the overall intelligence training strategy. Continuing education must evolve to support analytic abilities as well as critical and creative thinking skills.

(3) Unified action partners and allies. Army intelligence is most effective if it works with partners. Exchange assignments and education with JIIM and other interorganizational partners build relationships. Engagement deployments build expertise, capacity and capability, and relationships with partners.

3-4. Contributions to competition - Set the theater

a. Intelligence activities during competition support operations and set conditions for success during conflict. During competition, Army intelligence will organize and posture the force, develop relationships, establish the intelligence architecture, build a theater analytic base, support Army and joint targeting and targeting development to include integration of all domain lethal and non-lethal capabilities, support warning intelligence, and conduct peacetime information collection. Actions during competition establish the foundations for success across the competition continuum. This section identifies specified tasks from the MDO and EAB concepts. Appendix D provides detail on accomplishing those tasks.

b. Organize the force.

(1) Calibrate force posture across components. Army intelligence provides formations to support Army commanders from company to theater army across the components. Along with these echelons, the U.S. Army Intelligence and Security Command (INSCOM) provides access to national and reinforcing capabilities.

(2) Develop partners through interoperability and engagement. Increasing partners' capacity and capability, and interoperability allows the greater intelligence effort to support any commander continuously from competition through conflict and return to competition. Engagement builds relationships and regional expertise.

c. Establish architecture.

(1) Converge national and other capabilities through architecture. The intelligence architecture provides the data transport, storage, processing, security, applications, and governance across the intelligence points of presence that connect information collection, PED, and analysis from all sources to decision makers.

(2) Establish authorities and permissions. Authorities and permissions to share intelligence require legal and/or technical agreements between partners.

(3) Provide access to theater collection and databases. Access is an extension of permissions and authorities. Units with daily operational requirements or potential operational requirements need access to new and archived data for operations and training.

d. Prepare analytically.

(1) Conduct IPB. IPB drives planning and operations and must include all domains, the EMS, and the information environment. IPB establishes a knowledge baseline in context and identifies gaps that will drive collection and identify risk.

(2) Conduct intelligence warning assessments. Operational contingencies drive the warning intelligence process which analyzes and integrates operations and intelligence information to assess the probability of hostile actions.

(3) Analyze high volume data. Finding the relevant information in the sea of data requires automation to identify, fuse, and de-conflict data from all sources.

(4) Target A2 system. Understanding the C2, fires, IADS, and ISR systems that comprise the adversary's A2 capability is the first step to gaining access to the joint area of operations.

(5) Understand adversary's C2, long, and mid-range fires systems. U.S. forces must understand during competition what these systems can do, how the weather impacts these systems, and how adversaries employ these systems.

(6) Conduct robust operational assessment. A current assessment of all aspects of adversary national power supports warning intelligence, IPB, and targeting.

(7) Prepare for urban areas. Elements of national power come together in cities: cities are the political, economic, and informational hubs of society. The Army will need improved sensors and new analytic tools and techniques to understand urban social, cyberspace, and environmental complexities. The Army must identify adaptive threat actors and link them to their decentralized networks.

(8) Conduct open source intelligence (OSINT) activities. OSINT provides insight through PAI, business, industry, political, and economic information.

(9) Support Joint Force information operations and other nonlethal actions while defeating adversary information warfare.

e. Conduct information collection.

(1) Conduct reconnaissance and surveillance in all domains. Army intelligence must conduct intelligence operations, reconnaissance, and surveillance during competition to detect complex signatures in accessible, hazardous, and physically denied environments.

(2) Converge national, theater, and organic collection. Intelligence operations are inherently JIIM to provide the full range of capabilities to support the commander. Commanders must manage information collection across all domains and echelons.

(3) Conduct CI. During competition, CI supports protection through the conduct of CI collection, investigations, and operations to identify insider threats and to counter all-domain foreign intelligence entity threats to Army exercises, technologies, personnel, and facilities. CI

conducts liaison with partner CI, law enforcement, security agencies, and the appropriate protection elements. CI also supports counter-analysis requirements for information operations, operations security, and military deception.

3-5. Contributions to armed conflict - See deep

a. Future armed conflict against a peer threat is contested in all domains, the EMS, and the information environment at a global depth. Threat kinetic fires extend deep into the tactical and operational support areas, are layered and redundant, and there is no U.S. sanctuary from threat actions. To compete and win in this environment, Army intelligence must see deep enough to support effects and to support future planning at all echelons. Theater and national capabilities have long been able to see deep, but Army commanders must compete with other joint and national priorities to satisfy information requirements. Not since the 1990's have Army commanders been resourced to see as far as they could shoot. Army intelligence must see deep and deliver the results to decision makers to achieve tactical, operational, and strategic objectives. This paragraph identifies specified tasks from the MDO and EAB concepts. Appendix E provides detail on accomplishing those tasks.

b. Information collection.

(1) Employ Army high-altitude ISR platforms to provide deep sensing. Army intelligence requires platforms that are survivable, attritable, or expendable.[43]

(2) Employ a layered ISR network in all domains. Collection across domains provides depth and redundancy. Collection across disciplines improves accuracy, provides context, detects patterns and enemy deception activities, and supports information operations, operations security, and friendly deception efforts.

(3) Collect information in urban environments. The Army needs intelligence and weather effects for precision targeting in congested urban areas to enable U.S. influence and shaping operations and effectively compete with and counter adversary information activities. HUMINT is important to urban information collection. Nano air vehicles can provide access to restricted areas while multi-path exploitation radar can see into urban shadows. OSINT and SIGINT are rich data sources. The Army also needs to understand the urban systems that bring life to a city, systems that become more fragile as an urban area becomes larger.

(4) Integrate capabilities with EW and cyberspace. The integration of SIGINT, EW, and CO enables the commander to deliver non-kinetic fires in support of the scheme of maneuver and immediately assess effectiveness to create windows of superiority within the adversaries' decision cycles to gain a competitive advantage.[44]

(5) Provide expeditionary capabilities. Combat power required to defeat a peer competitor is based largely in the U.S. Expeditionary capabilities must be relevant immediately and continuously – distributed operations provide reach and intelligence overwatch.

(6) Link sensors to shooters enabled by AI. AI can shorten decision cycles and sensor to shooter processes.

(7) Converge national, theater, and organic collection. Expeditionary collection must integrate into the existing information collection constellation and increase the collection points of presence across intelligence disciplines.

(8) Incorporate and execute on demand direct-link tasking of space-based ISR capabilities at the appropriate echelons to sense into the deep strike area and support LRPF.

c. Analysis.

(1) Visualize the battle in all domains, the EMS, and the information environment. Information is collected from all domains against signatures in all domains, the EMS, and the information environment.

(2) Continue IPB. Analysts must update foundational intelligence databases during conflict. It must keep pace with the MDMP driving MDO against a peer threat.

(3) Conduct BDA. MDO against a peer threat require BDA across the domains and to the depth of the battlefield.

(4) Target enemy long range systems. Locating and tracking long range systems support LRPF and open windows of superiority for the Joint Force commander.

(5) Analyze high volume data. Data volume will increase during conflict. Army intelligence needs a data fabric that adheres to industry standards, can operate in the cloud and on local hardware, allows integrated data analytics and services, and can provide access to external services.[45]

(6) Identify high-priority targets on a “cluttered battlefield”. Information collection will observe relevant targets, decoys, and the vast background of the environment. Analysts must quickly identify the relevant targets in those collection results against the sea of data constantly streaming into databases.

3-6. Contributions to return to competition - Reset the theater

a. After armed conflict the theater must reset in accordance with the new security conditions. Rarely will those conditions be identical to those before armed conflict. The security situation may not stabilize immediately, partner allegiances may shift, threat capabilities and capacities will be different, and U.S. national interests may have changed. Forces must have clear and tailored missions and intelligence support to these forces. These and other factors will impact the return to competition. This section identifies specified tasks from the MDO and EAB concepts. Appendix F provides detail on accomplishing those tasks.

b. Organize the force.

(1) Adapt force posture to new security environment. The outcome of conflict may adjust the capabilities and capacities needed forward, resulting in a new mix of stationing, rotational force, and potential future requirements.

(2) Regenerate partner capacity. Changing partnerships will affect authorities and permissions for intelligence operations and intelligence sharing.

c. Architecture.

(1) Adjust architecture to the new security environment. While a competition architecture must expand to meet conflict needs, so must a return to competition architecture adjust to the post conflict points of presence of collection, PED, analysis, and decision makers.

(2) Re-establish authorities and permissions. The new security situation may change partnerships and it may change the contributions of intelligence disciplines.

(3) Continue access to theater collection and databases. Post-conflict databases are often outdated, as analysts must update holdings, and re-establish capability and capacity baselines.

d. Prepare analytically.

(1) Conduct IPB. Resetting foundational intelligence databases must be a priority.

(2) Reset indicators to support warning intelligence. The theater must reset warning sets and determine their indicators after conflict.

(3) Conduct robust operational assessment. After re-establishing the threat baseline, Army intelligence must maintain a current assessment of threat capabilities and the condition of infrastructure.

(4) Analyze high volume data. Army must continue to improve materiel and non-materiel solutions as data volume increases.

(5) Conduct OSINT activities. OSINT helps identify public sentiment in the new security environment and if the population is supportive of U.S. entities and their activities.

e. Conduct information collection.

(1) Continue intelligence operations, reconnaissance, and surveillance in all domains. Although return to competition may restrict some information collection, the Joint Force must monitor the terms of conflict termination and re-establish the operational assessment. Identity intelligence will support protection and establishment of legitimate local governance.

(2) Converge national, theater, and organic collection. As Army forces redeploy to CONUS, commanders will increasingly rely on partner intelligence collection.

(3) Conduct CI. CI continues its support to protection. CI, along with HUMINT, and civil affairs forces, will focus on factors that could lead to a return to conflict.

3-7. Integrating functions

a. Targeting. All domain targeting is critical to defeat enemy systems including A2AD capabilities and disrupt the enemy decision making cycle. Army intelligence must support the targeting process (at echelon) during competition, conflict, and return to competition. The Army's current organic sensors do not have the range, persistence, accuracy, resolution, survivability, and delivery timeliness to enable multi-domain targeting. Sensors and shooters, enabled by AI, must link to meet targeting timelines. Interoperability must be seamless between sensors and fires information systems.

b. Cyberspace and EW. Success in the future OE requires the Army to conduct multi-functional SIGINT, EW, and CO, in a holistic, synchronized, and integrated manner. The Army needs a multi-discipline, multi-modal collection and analysis capability at brigade combat team (BCT), division, corps, and theater. Across multiple domains in support of MDO, SIGINT and EW missions work to develop understanding of the threats' network structures and critical functions (to include the threat's EW, maneuver, and fire support assets); this is done in order to sense the battlefield and provide the commander intelligence estimates on threat intentions, early warning, targeting data, and identification of high value targets, high payoff targets and high value individual targets. Intelligence support to CO requires the intelligence staff to understand operations in cyberspace and the intersections between cyberspace and the physical domains. Intelligence staffs support all CO: offensive, defensive, and DOD information network operations.[46]

c. Army special operations forces (ARSOF). Army special operations directly support the IC and the Joint Force.

(1) ARSOF leverages its indigenous approach and human networks to sense deep in denied and degraded spaces. Through its extensive forward presence in the competition phase, ARSOF prepares the environment, provides deep knowledge and understanding, and strengthens partner capacity and capability enabling influence and shaping operations to provide additional options and windows of superiority for the Joint Force commander. ARSOF can enable the rapid physical control of population centers and support the rapid and comprehensive use of information to shape public opinion, discredit enemy narratives, and promote friendly narratives. Integrating this SOF-generated deep knowledge and understanding into Army intelligence systems is critical to building a holistic understanding of the operating environment throughout the competition continuum.

(2) Though capable of independent operations, ARSOF effects are maximized as part of a multi-domain, cross functional team. Converging intelligence, ARSOF, space, cyberspace, and fires capabilities enables the Joint Force to see, stimulate, and strike in the deep fires areas. To optimize this deep capability, Army intelligence and ARSOF information technology systems must be compatible with common data standards and communications protocols. MIB (T), theater special operations commands (TSOC), and joint special operations task forces must be integrated

and synchronized fully across all operations and activities. A sizeable portion of ARSOF intelligence systems are Army provided. Future programs such as Tactical Intelligence Targeting Access Node (TITAN), Distributed Common Ground System – Army (DCGS-A) Capability Drop 2 (CD2) and Terrestrial Layer System (TLS) have direct applicability to ARSOF formations.

d. Air defense. As a key component of the Joint Force collection plan in theater, Army intelligence integrates with air defense to provide IPB to the air defense artillery (ADA) sensors for likely avenues of approach, ballistic missile operations areas, and other sensor priorities in focus ADA sensor coverage. Integration also allows ADA sensors to give early warning and aerial situational awareness against high performance and rotary wing aircraft, long range enemy fires including cruise missiles, ballistic missiles, unmanned aerial vehicles, rockets, artillery, mortars, and other future aerial threats. Air defense sensors also provide critical ground location and points of origin information, enabling pre-launch destruction of enemy air and missile threats while they are still on the ground. Sensors must link to the joint air picture and air defense shooters to conduct timely engagements against air domain threats.

e. Other partners. Army intelligence shares data, information, and intelligence across the COE: sensors from all partners will share across this common platform. Intelligence staffs at echelons battalion through theater will leverage capability using apps while non-intelligence sensors will report using the COE. Future knowledge management practices will ensure the volume of available information does not overwhelm commanders. Architecture, developed before hostilities, will connect Army intelligence points of presence to decision makers at all levels through the COE. Of note, TITAN connects sensors to shooters and C2 nodes BCT and above and the intelligence analytics interface to replace DCGS-A will provide a portal using the COE.

3-8. Materiel solutions

a. The Army goal is to field the MDO AimPoint Force by 2028 and the MDO AimPoint Force 2035 by 2035. This concept is too late to drive new materiel solutions to support the 2028 MDO AimPoint Force using the Joint Capabilities Integration and Development System process: existing initial capabilities documents will not see full operational capability until fiscal year 2028. A required capability in this document may undergo a capabilities-based analysis and experimentation and generate a solution at a later date. Four existing programmed materiel solutions supporting the MDO AimPoint Force are identified below as well as potential modifications to support the MDO AimPoint Force 2035.

b. TITAN. TITAN is a scalable and expeditionary intelligence ground station that supports commanders across the entire MDO battlefield framework with capabilities tailored to echelons theater to BCT. TITAN leverages space and high altitude, aerial and terrestrial layer sensors to provide target nominations directly to fires information systems as well as providing multi-discipline intelligence support to targeting and situational understanding in support of the commander's overall operations process.[47]

c. Multi-Domain Sensing System (MDSS). MDSS will enable commanders to rapidly gain and maintain situational understanding, freedom of maneuver, and overmatch in multi-domain operations. Today, Army aerial ISR (AISR) platforms operate at a vulnerable altitude, are tied to

vulnerable runways, have limited collection range, and have limited (manned) or no (unmanned) aircraft survivability equipment.[48] "Survivable platforms include ones with small signatures, ones that can overwhelm enemy defenses through sheer numbers, those capable of penetrating enemy defenses and those able to achieve stand-off through altitude. Some of these may not survive, but will be designed to be either attritable or expendable."[49] In 2025-2040, adversaries will have the capability to challenge and deny space assets.[50] Army intelligence will continue to leverage national-level and commercial assets in the space domain for information collection.

d. TLS. Commanders require terrestrial based collection capabilities in a peer contested battlefield, which requires operations in DIL communications environments. Dedicated intelligence collection, cyberspace and EW effects, support to cross domain fires, and networked sensing capabilities will be needed to achieve relative advantage over peer adversaries, with overmatch in cyberspace and the EMS.[51] The TLS expands upon current systems, includes multiple domain network access (Non-Secure Internet Protocol Router Network [NIPRNet], Secure Internet Protocol Router Network [SIPRNet], Joint Worldwide Intelligence Communications System [JWICS] and, National Security Agency Network [NSANet]), introduces new capabilities, and finds synergies within an integrated terrestrial-layer to support commanders' decision making cycles.[52]

e. An intelligence analytics interface to replace the Distributed Common Ground System – Army (DCGS-A). An intelligence analytics interface is the modernization framework replacing DCGS-A. The interface places the emphasis on equipping the Soldier rather than manning equipment. DCGS-A currently provides the Army with support to targeting and situational understanding to commanders. It processes, exploits, and disseminates information and intelligence including threat, weather, and terrain. However, DCGS-A analytical tools are not easy to use, require substantial training and hardware infrastructure, and rely on an aging database solution that is neither scalable nor extensible to accommodate the growing volume, velocity, and diversity of data that will exist in a multi-domain environment. DCGS-A CD 2 will modernize the data fabric and analytic solution to provide the scalability and extensibility needed at all echelons, while also improving interoperability and ease of use. Looking forward, Army intelligence will need to define and deploy the capability to quickly adopt or acquire new analytics, apps, and tools, and deploy them into the common operating environment. The follow on program, Intel Apps, will focus on the process to rapidly field new apps in to the command post computing environment (CPCE) to support existing and emerging requirements beginning in fiscal year (FY) 2024.

f. Other materiel solutions.

(1) Next Generation Biometrics Collection Capability (NXGBCC). The NXGBCC enhances the overall functional capabilities of collect, match, store, share, analyze, reference, and decide/act; expands on the current biometric modalities to include voice and palm prints; reduces its current size, weight, power consumption, and costs; and is more integrated with the DoD biometric enterprise and with unified action partners.

(2) Biometric Enabling Capability 1 (BEC 1): BEC 1 provides a cloud ready consolidated, authoritative repository for biometric data. It provides face, fingerprint, palm, iris, and voice

matching to prevent adversaries from conducting counter intelligence operations, espionage, sabotage, surveillance, and reconnaissance against U.S. forces and partner nations. It enables development of actionable identity intelligence against high value individuals, biometric processing of enemy prisoners of war and detainees, enables identification of threat actors in or near population centers, sanctuary areas, critical infrastructure, and events.

(3) Army Site Exploitation Intelligence and Collection Toolset. The Site Exploitation Intelligence and Collection Toolset provides specialized collection of items of interest and initial PED on captured documents, digital information sources, and unknown substances, to the lowest levels, in direct support of the BCT commander, leveraging search techniques, biometrics, forensics, and document exploitation as part of the TLS requirement.

(4) CI and HUMINT Equipment Program-Army (CIHEP-A). The current CI and HUMINT Automated Reporting and Collection System (CHARCS) program of record migrates toward eventual end of useful lifecycle ~2024/25. The CIHEP-A enables CI and HUMINT assets to collect and report critical human-derived information, specifically source operations, identity activities, and language translation. The CIHEP-A capabilities build upon components of the terrestrial layer intelligence support (TLIS) ICD.

(5) Identity Intelligence Analytic Resource (I2AR). I2AR provides intelligence analysts and operators with a centralized capability to perform all-source biometrically-enabled identity analysis, linking, U.S. persons quarantine and management, watchlist management, and product authoring at the Secret level.

3-9. Organizational solutions

a. The Army goal is to field an MDO AimPoint Force by 2028 and an MDO AimPoint Force 2035 by 2035. Capability is the fulfillment of an organizational document, not merely the publication of that document. This concept is too late to drive new organizational solutions to support the 2028 MDO AimPoint Force using the total Army analysis (TAA) process: submissions for TAA 24-28 are in staffing, will be included in the Army structure (ARSTRUC) published in October 2021 and will begin fielding in FY 2024 and complete fielding in FY 2028. Intelligence operational and organizational concept documents are due in November 2021 after the ARSTRUC is published and will require staffing before influencing TAA 26-30. A required capability in this document may undergo a capabilities-based analysis and experimentation and generate a solution at a later date. Therefore, organizational solutions to support the MDO AimPoint Force are listed below.

b. Capabilities above theater.

(1) INSCOM is a direct reporting unit to the Army Deputy Chief of Staff, G2 that conducts and synchronizes worldwide intelligence discipline and all-source intelligence operations across all domains. INSCOM also delivers linguist support and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities to support Army, joint, unified action partners, and the U.S. IC. INSCOM leverages the Tactical Exploitation of National Capabilities program to integrate national capabilities into the Army.

INSCOM's functional brigades and groups may provide general support, general support reinforcing, or direct support to theaters through intelligence reach, or they may be force-tailored for deployment to support the joint force conduct MDO. INSCOM's brigades and groups include:

(a) The 116th MI BDE (Aerial Intelligence) provides aerial intelligence collection platforms, associated PED, and command and control at forward locations.

(b) The 902nd MI Group conducts the full range of Counterintelligence functions (operations, investigations, collection, analysis and production, and technical services and support activities).

(c) The Army Operations Group conducts global, full spectrum HUMINT operations.

(d) The 780th MI BDE conducts CO and SIGINT activities in support of Army Cyber Command and U.S. Cyber Command.

(e) The 1st Information Operations Command provides information operations support to the Army and other military forces through deployable teams, reach-back planning and analysis, and specialized training in order to support freedom of action in the information environment and to deny the same to adversaries.

(f) The 704th MI BDE and 706th MI BDE conduct SIGINT activities in support of the National Security Agency.

(g) The National Ground Intelligence Center produces science and technology intelligence, GEOINT, and general military intelligence on foreign ground forces.

(h) INSCOM provides additional support to the Army as Army level offices, including:

- Army cryptologic operations represents the Army at the National Security Agency and supports the success of Army SIGINT units from BCT to national level.
- Army Geospatial Office represents the Army at the National Geospatial Agency and supports Army geospatial intelligence (GEOINT) activities.
- Army Open Source Intelligence Office provides operational capability and advanced tradecraft training to Army elements. INSCOM is the operational proponent for OSINT in the Army, with the Office of the Deputy Chief of Staff G-2 as the functional proponent for Army OSINT.
- The Department of the Army Intelligence Information Services provides a means to discover, access, and share relevant IC reporting. It provides intelligence dissemination, access management, data brokering and intelligence production requirements management. It implements web technology solutions for quick reaction to technology and policy changes that could impact access to intelligence data. It is assigned to INSCOM and supervised by the DA G2.
- The Ground Intelligence Support Activity (GISA) provides regionally focused, responsive, reliable, and robust IT networks, services and capabilities to authorized end-users. GISA is a global organization responsible for operating, securing, and defending intelligence information technology networks, infrastructure, and services in support of the Army, joint and coalition mission partners. Led by a civilian director, GISA is not a command, but

otherwise functions like an INSCOM major subordinate command. Headquarters, GISA is located at Fort Belvoir, VA with regional nodes located at Wiesbaden, Germany; Fort Bragg, NC; Fort Shafter, HI; and at Fort Belvoir, VA.

(2) U.S. Army Special Operations Command.

(a) The 389th MI Bn conducts command and control of multi-discipline intelligence operations in support of the 1st Special Forces Command and its component subordinates units. On order, deploys worldwide to serve as the core of the J2 for a contingency Special Operations Joint Task Force[53] and conducts multi-domain intelligence operations on its behalf consisting of all-source analysis, collection management, single source subject matter expertise, and PED lines of effort for all ARSOF platforms.

(b) 75th Ranger Regiment; Regimental Military Intelligence Battalion is established to provide multi-disciplinary, multi-domain intelligence capability and capacity that is organic to the regiment's expeditionary and distributed combat operations worldwide while being closely synchronized with the joint and inter-agency communities. Two companies comprise the intelligence collection and analytic support: a military intelligence company (MICO) which comprises all HUMINT, unmanned aerial system (UAS) reconnaissance, all-source analysis, and PED operations; and a cyber electromagnetic company that combines special reconnaissance, SIGINT, EW, and CO.

(3) In joint theater operations, the Joint Force Air Component Command (JFACC) serves as commander for strategic attack, air interdiction, and airborne intelligence collection (among other missions). The Army Air and Missile Defense Command intelligence staff directly enable the JFACC, and Joint Force Land Component Commander intelligence collection planning and analysis, and support the deliberate and dynamic targeting processes.

(4) JIIM partners. Intelligence activities are inherently JIIM to provide the full range of capabilities to support the commander. Formal arrangements expand information collection capabilities and capacities beyond Army capabilities. They expand PED and analysis capabilities, capacity, and perspectives, particularly multinational partners' cultural perspectives. This inherently JIIM approach strengthens partners and supports Army commanders when Army capabilities are not positioned or available.

c. Theater. Dedicated MI support to the theater includes a MIB (T) and MI formations inside the multi-domain task force (MDTF) and the security force assistance brigade (SFAB).

(1) The MIB (T) is an INSCOM brigade assigned to the Combatant Command (CCMD) and OPCON to the Army Service Component Command (ASCC). Each conducts multi-discipline collection activities, conducts warning intelligence, produces finished intelligence assessments, and is the anchor point for regional alignment. The MIB (T) is a permanently assigned ground intelligence organization designed against competition requirements. The MIB (T) sets the theater architecture, maintains the theater tactical entity database, connects with joint and national capabilities, conducts steady state CI operations, and integrates regionally aligned and globally ready forces as they flow into theater. The MIB (T) also has limited HUMINT and SIGINT

capability. In the event there is a temporary field army in a theater, a U.S. Army Reserve (USAR) E-MIB composed of two general support (GS) battalions will provide support.

(2) Inside the MDTF is an intelligence, information, cyberspace, electronic warfare, and space battalion containing a MICO. The MICO conducts multi-discipline intelligence analysis, PED, technical SIGINT analysis, SIGINT collection, GEOINT, and OSINT in support of multi-domain situational awareness, Army and joint target development, IPB, and MDMP. In the objective design, two top secret/sensitive compartmented information (TS/SCI) communications teams can support two C2 nodes with TS/SCI communications.

(3) The MICO of the SFAB trains partner force intelligence personnel on understanding threats, conducting and synchronizing intelligence, collection and analysis, and generating intelligence reports and visualization aides to enable situational understanding for all subordinate forces.

(4) The MICO of the Special Forces Group support battalion provides multi-discipline intelligence collection and analysis to support the group. It conducts HUMINT, CI, SIGINT, GEOINT, OSINT, EW, and tactical unmanned aerial system collection and the analysis of that and other collection.

d. Corps. Each U.S. Army corps has an active component E-MIB consisting of a headquarters, a corps intelligence electronic warfare (IEW) battalion, and a division IEW battalion for each subordinate division.

(1) The IEW Battalion (Corps) analysis and PED Detachment conducts multi-discipline intelligence analysis and PED, multi-domain collection management, OSINT in support of corps multi-domain situational awareness, target development, IPB, and MDMP in support of the corps G2.

(2) The IEW Battalion (Corps) multi-domain MICO conducts multi-discipline intelligence analysis and processing, SIGINT collection support to EW and CO, PED in support of multi-domain (air, land, sea, space, and cyberspace) situational awareness, target development, IPB, and MDMP in support of corps MDO.

(3) The IEW Battalion (Corps) CI/HUMINT Company conducts CI and HUMINT operations in support of corps, division, and combined joint task force operations.

e. Division. The IEW Battalion (Division), provided in direct support from the corps E-MIB, conducts multi-discipline intelligence analysis and PED in support of the division G2 and multi-domain collection management, PED and collection in support of division multi-domain effects.

(1) The IEW Battalion (Division) analysis and PED detachment conducts multi-discipline intelligence analysis and PED, and OSINT in support of division multi-domain (air, land, sea, space, and cyberspace) situational awareness, target development, IPB, and MDMP requirements.

(2) The IEW Battalion (Division) multi-domain MI detachment conducts multi-discipline intelligence analysis and processing, SIGINT collection support to EW and CO, PED in support of multi-domain (air, land, sea, and cyberspace) situational awareness, target development, IPB, MDMP in support of division MDO.

(3) National Guard divisions receive IEW Battalion (Division) support from Army National Guard (ARNG) E-MIBs. ARNG E-MIBs are organized with four IEW Bn (Div) per E-MIB.

f. BCT. The BCT is the division's primary combined arms, close combat force and tactical fighting formation in 2028. The BCT S-2 and organic MICO facilitate the commander's visualization and understanding of the battlefield while supporting targeting and protection. In the MDO AimPoint Force of 2028, the TITAN and TLS will replace the Tactical Intelligence Ground Station (TGS) and Prophet systems in the current force. At BCT, TITAN can request, task, and receive GEOINT and SIGINT data and products from space, high altitude, aerial, and terrestrial sensors to build and share situational understanding and develop cross domain targets and support BDA. TITAN can conduct limited on the move operations while operating in a DIL environment. TLS will integrate SIGINT, EW, and CO to enable the commander to compete and win in the EMS. The S-2 can build and disseminate products through the CPCE to higher, adjacent, and subordinate units. The MICO also interrogates enemy of prisoners of war, conducts tactical HUMINT, and conducts air reconnaissance using tactical unmanned aircraft systems.

3-10. Training solutions

a. Training and education occur in all three training domains: institutional, operational, and self-development. Training prepares individuals for certainty. Education prepares individuals for uncertainty. Education enables agility, judgment, and creativity. Training enables action.[54]

b. Training is a team effort and the entire Army — Department of the Army commands, the institutional training base, units, the combat training centers, each individual Soldier, and the civilian workforce — has a role that contributes to force readiness.[55] When MI Soldiers receive institutional training in a multi-service environment, TRADOC must develop Army specific augmentation training to ensure all Army requirements are met. As doctrine adjusts to MDO and new capabilities enter the force, training will incorporate these changes.

c. The MI Training Strategy (MITS) provides a standardized certification strategy for commanders to plan training and evaluate their tactical intelligence warfighting function capabilities in an objective, quantifiable manner.[56] MITS provides a standardized certification for MI training, ensures competence in the fundamental skills of intelligence professionals and readiness to support decisive operations. The MITS tiered framework parallels the certification lexicon (maneuver gunnery) used by maneuver commands.[57]

d. BCT MITS is complete as of August 2019. Separate brigades, divisions, and corps are scheduled for completion mid FY 2020 and the E-MIBs are scheduled for completion in FY 2021.

e. MI training and education will include expanded training in areas such as data science and systems thinking. Recognizing credentials in these and other fields may impact Army accessions policies through recruiting discrete skills above the entry level.

f. The Foundry intelligence training program is a critical enabler to Army global readiness that provides commanders necessary resources to enhance the training of MI Soldiers and civilians supporting multi-domain operations at the tactical, operational, and strategic levels. It enables available and ready MI individuals and units to conduct multi-domain intelligence operations and activities to support commanders executing their missions. The Foundry program provides a venue for commanders to collectively certify MI individuals and units (team and higher) in support of regional alignment and global contingency operations and enables intelligence oversight and compliance of laws, policies, and directives for highly technical intelligence missions. It provides access to the intelligence enterprise and sensitive networks, required accreditation and technical certification and enhances command and control proficiency.

g. The steady state conduct of the CI mission requires a departure from the 'train as you fight' model. CI must be performed as a daily real world mission, synchronized for unity of effort throughout all phases of the competition continuum, and across all domains.

Chapter 4
Conclusion

a. Army intelligence has long operated from multiple domains to target threat forces and analyze environmental signatures in all domains, the EMS, and the information environment to meet the commander’s information requirements. The principal shift from The U.S. Army Functional Concept for Intelligence (2017) is the addition of organic Army deep sensing and the DOTMLPF-P impacts to process, analyze, and distribute the increased collection results. Critical to Army intelligence success are those actions during competition that help sustain U.S. objectives while deterring conflict and prevent cold starts during conflict.

b. Actions to field the MDO AimPoint Force by 2028 are already in motion – Army process to field MDO-capable organizations and equipment began before publication of this concept and adjustments to those solutions will field the MDO AimPoint Force 2035 by 2035.

c. Organizational changes to support MDO reorient the E-MIB from a BCT reinforcement focus to one that addresses the needs of the corps and division commanders.

d. Materiel changes to support MDO center on four major programs to improve situational understanding: TITAN to connect sensors with shooters and C2 nodes; MDSS to provide deep sensing; TLS to provide ground based sensing and integration with EW and CO; and an intelligence analytics interface (the follow-on program to DCGS-A) to provide the processing and analytics to support the increased sensing.

e. Training and talent management systems must keep pace with capability changes to provide the innovative leaders, Soldiers, and Army Civilians needed to support the commander.

Appendix A
References

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

Section I
Required references

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

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

TRADOC Pamphlet 525-92
The Operational Environment and the Changing Character of Warfare

Section II
Related references

Army Concept Writers Guide, 12 Nov 2019

Army Directive 2017-24
Cross-Functional Team Pilot in Support of Materiel Development, 6 October 2017.

Army Directive 2018-18
Army Artificial Intelligence Task Force in Support of the Department of Defense Joint Artificial Intelligence Center, 2 October 2018.

Army Doctrinal Publication 1-02
Terms and Military Symbols, 14 August 2018

Army Doctrinal Publication 2-0
Intelligence, 31 July 2019

Army Regulation 5-22
The Army Force Modernization Proponent System

Army Regulation 350-1
Army Training and Leader Development, 10 December 2017

Army Science Board Study, (2016) The Military Benefit and Risks of the Internet of Things

Army Techniques Publication 3-96.1
Security Forces Assistance Brigade

Blank, S. (1991). The Soviet Military Views Operation Desert Storm: A Preliminary Assessment, Strategic Studies Institute. https://apps.dtic.mil/dtic/tr/fulltext/u2/a242543.pdf

Blank, S. (2018). Moscow's Competitive Strategy, American Foreign Policy Council.

China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the PLA, Washington, D.C., CNA Corporation. 2005.

Connell M., Vogler, S., Russia's Approach to Cyber Warfare, Center for Naval Analyses. 2017. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf

Cliff, R., Fei, J., Hagen, J., Hague, E., Heginbotham, E., Stillion, J., (2011) Shaking the Heavens and Splitting the Earth Chinese Air Force Employment Concepts in the 21st Century. Rand, https://www.jstor.org/stable/10.7249/mg915af

China Military Power, DIA, 2019 https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf

DA Pamphlet 25-40
Army Publishing Program Procedures, 13 June 2018

DOD Instruction 3305.09
DoD Cryptologic Training, June 13, 2013 incorporating change 1, effective May 4, 2018

Department of Defense National Defense Strategy 2018 Unclassified Summary (Summary of the 2018 National Defense Strategy of the United States of America), 19 January 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Emerging Science and Technology Trends: 2017-2047, A Synthesis of Leading Forecasts November 2017

FM 2-0
Intelligence 6 July 2018

Gompert, D, Astrid S., Garafola, C., (2016) War with China: Thinking Through the Unthinkable. Rand. https://www.rand.org/pubs/research_reports/RR1140.html

Harrison, Todd (2018) Space Threat Assessment. CSIS. https://aerospace.csis.org/wp-content/uploads/2018/Harrison_SpaceThreatAssessment

HQDA EXORD 204-17 Identification of gaps in capability between Trojan Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) Lightweight Integrated Telecommunications Equipment (LITE) (V) 3 and the Modular Communication Node-Advanced Enclave (MCN-AE) that require mitigation.

HQDA EXORD 204-17, Transport Convergence

Intelligence Center of Excellence Force Modernization Strategy (2018)

Intelligence Center of Excellence Problem for Intelligence Force Modernization (2018)

Industry Day Slides, (22 March 2019). Retrieved from https://www.defense.gov/explore/story/Article/1747501/clear-skies-for-dod-cloud-initiative/Intelligence Community Commercial Cloud Enterprise

Network Cross Functional Team S&T Priorities, September 2019

National Intelligence Strategy of the United States of America 2019, Office of the Director of National Intelligence.

United States Army High Altitude White Paper: Exploring High Altitude for Future Army Use (2025-2040) 1 July 2019, U.S. Army Futures Command, Futures and Concepts Center

U.S. Army Intelligence Center of Excellence (USAICoE) Aerial Intelligence, Surveillance and Reconnaissance (AISR) in Multi-Domain Operations (MDO) White Paper 8/17/2018 (AISR White Paper).

U.S. Government Printing Office Style Manual, latest edition Located at https://www.govinfo.gov/content/pkg/GPO-STYLEMANUAL-2016/pdf/GPO-STYLEMANUAL-2016.pdf

Presentation, Headquarters, Department of the Army, Office of the Deputy Chief of Staff, G-2, 19 April 2017, subject: Army Intelligence 2017-2025, Intelligence at the Speed of Mission Command, 2017.

Russian Military Power - Building a Military to Support Great Power Aspirations. DIA, (2017), https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937

Strategy Document, Acting Secretary of the Army and Chief of Staff of the Army, 3 October 2017, subject: Modernization Priorities for the United States Army.

Strategy Document, United States Air Force, 2 August 2018, subject: Next Generation Intelligence, Surveillance, and Reconnaissance (ISR) Dominance Flight Plan.

Streltsov A., (2011) Basic Goals of Government Policy in Information Wars and Battles, Military Thought (English)

Military and Security Developments Involving the People's Republic of China 2019 Office of the Secretary of Defense

The Army Intelligence Plan, DA G-2, 11 October 2019

The Joint Operating Environment 2035, *The Joint Force in a Contested and Disordered*, 2016. https://apps.dtic.mil/docs/citations/AD1014117

TRADOC Pamphlet 525-4-1
The U.S. Army Functional Concept for Sustainment

Multi-Functional Intelligence and Electronic Warfare (MIEW) Concept of Operations (CONOPS)

U.S. Army Intelligence and Security Command (INSCOM) 2018 Science and Technology (S&T) RFI Priority

STP 34-35D-OFS (Officer Foundation Standards for the All-Source Intelligence Officer AOC 35D ranks 2LT, 1LT, CPT, MAJ and above) 20 July 2018

TC 2-19.400 (Military Intelligence Training Strategy) 1 August 2019

Appendix B
Required Capabilities

B-1. Introduction
This appendix reflects required capabilities (RC) necessary to conduct operations as described in this concept.

B-2. Function RCs (56 total RCs)

a. Intelligence operations (Collection) (20 total RCs). Future forces require the ability to conduct information collection in and of all domains, the EMS, and the information environment throughout the competition continuum to provide depth and redundancy to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a, 3-4d (1), 3-4d (2), 3-5a (2); AOC p 33; EAB p 19, 38)

(1) Future forces require the ability to identify the right sensor and platform and direct these platforms to the right place at the right time throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3a; AOC p. 33; EAB p. 19)

(2) Future forces require the ability to integrate expeditionary collection into the existing information collection constellation and increase the collection points of presence across intelligence disciplines throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a, 3-5.a.(5), 3-5a(7); AOC p. 23, 33; EAB p. 19)

(3) Future forces require the ability to collect information and cross-cue sensors across intelligence disciplines throughout the competition continuum to reduce susceptibility to deception and support commanders' situational understanding in all operational environments. (This concept, paragraph 2-4.d, 3-3.a, 3-5a(2) AOC p. 22, 23, 33; EAB p. 19)

(4) Future forces require the ability to provide a weather collection capability throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a, 3-5.a(3); AOC p. 33; EAB p. 19)

(5) Future forces require the ability to detect, identify, locate, and track advanced and discrete signatures across a diverse array of adversaries' organizations, systems, and capabilities throughout the depth of the battlefield throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a.(1), 3-4.d.(1); AOC p. B-2; EAB p. 35)

(6) Future forces require the ability to monitor the terms of conflict termination during return to competition to re-establish the operational assessment and support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a(1), 3-6d(1); AOC p.45; EAB p. 19)

(7) Future forces require the ability to sense deep into the battlefield across domains and the electromagnetic spectrum throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 2-4d, 3-3.a(2), 3-5.a(1); AOC p. C-6)

(8) Future forces require the ability to employ Army high-altitude ISR platforms to extend endurance beyond current aerial platforms over wide geographical areas and persistent presence and penetration of denied areas throughout the competition continuum to develop stand-off intelligence to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a.(2), 3-5.a.(1); AOC p. 33, C-6; EAB p. 43, 46)

(9) Future forces require the ability to field aerial collection platforms that are survivable, attritable, or expendable to position sensors throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a.(3))

(10) Future forces require the ability to automate sensor fusion across disciplines throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a.(4); AOC p.23; EAB p. 19)

(11) Future forces require the ability to provide direct intelligence sensor reporting to data architectures throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraphs 3-3.a.(5); AOC p. 22, 33; EAB p. 43)

(12) Future forces require integration of intelligence sensors and fires information systems throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 3-7.a.; AOC p. 22; EAB p. 38, 39)

(13) Future forces require the ability to link sensors and shooters and their fire control systems, enabled by AI, while facing a contested EMS and adversary attempts at denial and deception, throughout the competition continuum to meet targeting timelines in all operational environments. (This concept, paragraph 3-3.a.(5), 3-5a(6), 3-7a; AOC p.22, 33; EAB p. 43)

(14) Future forces require the ability to integrate SIGINT, EW, and cyberspace capabilities throughout the competition continuum to create temporary windows of superiority to seize, retain, and exploit the initiative, and support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a.(6), 3-5a(4), 3-7b; AOC p.22; EAB p. 43)

(15) Future forces require the ability to collect, match, store, share, analyze, reference, and manage iris, face, finger, palm, and voice print signatures throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a(7), 3-8.e.(1); AOC p.33; EAB p. 19)

(16) Future forces require the ability to collect and report critical human-derived information, including HUMINT operations, site exploitation, and document and media exploitation throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.a(8); AOC p.33; EAB p. 19)

(17) Future forces require the ability to conduct CI activities throughout the competition continuum to support protection and commanders' situational understanding in all operational environments. (This concept, paragraph 3-4.d.(3); AOC p. 28, 29, 31, C-5; EAB p. 19)

(18) Future forces require the ability to sense and collect information inside urban areas throughout the competition continuum to support precision targeting and commanders' situational understanding in dense urban areas. (This concept, paragraph 2-4d, 3-5a(3); AOC p. 27, 28, B-1, D-1, D-3; EAB p. 35)

(19) Future Army intelligence forces require the ability to support an expeditionary Army with capabilities able to travel inter-theater under enemy observation and within range of enemy kinetic and non-kinetic effects from multiple domains throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 2-4e, 3-5a(5); AOC p. 18, EAB p. 22)

b. Architecture (13 total RCs). Future forces require intelligence architecture that connects all points of presence -- sensors, PED, analysis, storage, decision makers, and shooters –across all echelons, domains, and multiple security levels throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 2-4c, 3-3.b, 3-3.b(1); AOC p. 22, 28, C-5; EAB p. 38-39)

(1) Future forces require the ability to manage data volume, data velocity, data variety, and data veracity of deliberately and peripherally collected data as well as the vast available data stores throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 2-4h, 3-3.b, 3-5b(5); AOC p.22; EAB p. 24)

(2) Future forces require the ability to provide the secure data transport, processing, applications, and governance across the intelligence points of presence in a contested cyberspace and electromagnetic environment throughout the competition continuum to support commanders' situational understanding in all operational environments. (this concept, paragraph 3-3.b, 3-4b(1), 3-6.b(1); AOC p. 22, 28, C-5; EAB p. 38-39)

(3) Future forward based and expeditionary forces require assured access to intelligence data at echelon and across theaters of command throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3b(1), 3-4.b(3); AOC p.22, C-5; EAB p. 24, 38-9)

(4) Future forces require the ability to update analytic holdings and re-establish capability and capacity baselines during post conflict to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-6b(3); AOC p.31; EAB p. 77)

(5) Future forces require the ability to ingest and process data from DOD, IC, commercial, open source, and publicly available information for intelligence purposes throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 3-3b(2); AOC p. 22; EAB p. 24)

(6) Future forces require a configurable automated normalization capability that converts data into the form and format needed for user understanding, that enables system processing, and allows consumption by an external system throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3b(2); AOC p. 22; EAB p. 24)

(7) Future forces require compliance with common DOD and IC data standards throughout DOD, IC, allies and partners throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3b(3); AOC p. 22; EAB p. 24)

(8) Future forces require intelligence data currency to provide seamless transitions throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3b(4); AOC p. 22; EAB p. 24)

(9) Future forces require the ability to leverage cloud infrastructure support providing intelligence data management, big-data analytics, and AI throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.b(5); AOC p. 22; EAB p. 24)

(10) Future forces require intelligence sharing authorities and permissions established in competition and updated throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-4b(2); AOC p. 22, 28, C-5; EAB p. 38-39)

(11) Future forces require seamless interoperability between Army intelligence and ARSOF information technology systems with common data standards and communications protocols throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-7c; AOC p. 22; EAB p. 19)

(12) Future forces require the ability to link sensors to the air picture and air defense shooters to provide early warning and aerial situational awareness against high performance and rotary wing aircraft; long range enemy fires including cruise missiles and ballistic missiles; unmanned aerial vehicles, rockets, artillery, mortars, and other future aerial threats to conduct timely engagements against air domain threats. (This concept, paragraph 3-7d; AOC p. 19; EAB p. 51)

c. Analysis (17 total RCs). Future forces require the ability to understand and visualize the battlefield in all domains, the EMS, and the information environment throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.c, 3-5b(1); AOC p. B-2)

(1) Future forces require intelligence analyst functions integrated within COE computing environments throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3c(1); AOC p. 22, B-2; EAB p. 38, 39)

(2) Future Army intelligence forces require high compute processing and AI to enable automation and fusion of advanced signatures and high volume data at machine speed throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 3-3c(2), 3-4c(3), 3-5.b(6); AOC p. 22; EAB p. 24)

(3) Future Army intelligence forces require the ability to find those information collection results quickly in the sea of data constantly streaming into databases throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all OEs. (This concept, paragraph 3-3.c(2), 3-5b(6); AOC p.22; EAB p. 24)

(4) Future Army intelligence forces require the ability to provide data analytics that provide data integrity, standardization, correlation, geolocation refinement, predictive, and pattern analysis

throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.c.(2), 3-5.b(5); AOC p. 22; EAB p. 24)

(5) Future forces require the ability to automate collection management throughout the competition continuum to keep pace with the military decision-making process throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3c(3); AOC p.22, 23; EAB p. 38, 39)

(6) Future Army intelligence forces require analytic workflows that support dynamic modeling and forecasting throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3c(4); AOC p. 22; EAB p. 24)

(7) Future forces require the ability to conduct intelligence warning assessments and reset assessment parameters throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3c(4), 3-4.c(2), 3-6c(2))

(8) Future Army intelligence forces require advanced analytic tradecraft supported by intuitive analyst interfaces to solve advanced problems throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3c(5); AOC p. 22; EAB p. 24)

(9) Future Army intelligence forces require rapid generation of user-based tools and applications throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3c(6); AOC p. 22; EAB p.24)

(10) Future forces require the ability to process, exploit, and disseminate collected intelligence data through a global exchange and reach network throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3c.(7); AOC p. 22, 33; EAB p. 43)

(11) Future forces require the ability to support deliberate and dynamic, lethal and nonlethal targeting throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 3-4.c(4), 3-7a; AOC p.33; EAB p. 43)

(12) Future forces require the ability to target the adversary anti-access system throughout the competition continuum to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 3-4c(4); AOC p. 31, 33, C-6; EAB p. 43)

(13) Future forces require the ability to conduct robust operational assessment throughout the competition and return to competition periods to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-4c(6); AOC p. 31; EAB p. 77)

(14) Future forces require analytic tools, techniques and models to understand the mechanics of urban areas to include political, social, and criminal organizations to determine the key signatures that develop pertinent knowledge throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-4c(7), 3-5a(3); AOC p. 27, 28, B-1, D-1, D-3)

(15) Future forces require the ability to collect open source materials and incorporate it into analytic models throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-4c(8); AOC p. C-5)

(16) Future forces require the ability to conduct battle damage assessment throughout the conflict and return to competition periods to support the targeting process at echelon and commanders' situational understanding in all operational environments. (This concept, paragraph 3-5b(3); AOC p. 31; EAB p. 77)

d. People and structure (6 total RCs). Future forces require competent, agile, and resilient Army intelligence Soldiers and leaders throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 2-4k)

(1) Future forces require the ability to calibrate intelligence force posture across components throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-4a(1); AOC p. 17; EAB p. 22)

(2) Future Army intelligence forces must identify with precision their required technical skill sets, to include knowledge and behaviors for intelligence personnel in support to MDO, assess the currency of those skill sets, provide an initial and continuing education plan, and purposefully align those talented Soldiers throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3d(1))

(3) Future Army intelligence forces require next generation live, virtual, and constructive training simulations which incorporate the ability to create massive amounts of realistic multi-disciplined intelligence data across the competition continuum to challenge Soldiers at the institution, home station, and deployed locations in all operational environments. (This concept, paragraph 3-3d(2))

(4) Future forces require the ability to develop partners through interoperability and engagement and routinely focus Army units conducting engagement operations to information gaps, capturing observations upon their return, throughout the competition continuum to support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3.d(3), 3-4a(2); AOC p. C-10; EAB p. 20, 21)

(5) Future Army intelligence forces require engagement deployments and exchange assignments and education with joint, interagency, intergovernmental, multinational, and other interorganizational partners throughout the competition continuum to build relationships and

support commanders' situational understanding in all operational environments. (This concept, paragraph 3-3d(3); AOC p. C-10; EAB p. 20, 21)

Appendix C
Science and Technology

C-1. Background

a. The Secretary of the Army and the Chief of Staff of the Army have established eight modernization cross-functional teams and two task forces aligned to the six Army modernization priorities. Modernization efforts, by, with, and through Army Futures Command guide S&T efforts, long term investments, and capability developments. The ISR task force is the Army's lead for modernization of ISR capabilities.

b. Army intelligence aligns technology focus areas to address the range of threats across the near, mid, and far terms. This set of focus areas helps refine industry, government, and academia's understanding of Army intelligence areas of interest. It also allows Army intelligence to maintain an understanding of technology trends and the realities of emerging and maturing technologies.

c. Industry continues to lower the entry barrier for advanced technology adoption. State and non-state actors operationalize new capabilities with minimal investment. Near-peer and peer competition will occur at hyper speed and scale, dominated by technologies such as robotics and autonomous systems, and AI. The internet of things, connected by 5G networks, will further democratize sensors and sensor data. Investments in self-driving vehicles will bring once niche sensing phenomenologies such as light detection and ranging, radar, and multi-spectral sensing to a wide audience. Militarization of dual-use technology will continue to challenge traditional and non-traditional indications and warning, analysis, targeting, and protection functions. Army intelligence must embrace new technology, new approaches, new ideas, and more efficient organization of knowledge and capabilities to support the Army in the near, mid, and far terms.

d. Army intelligence systems must be:
- Interoperable and integrated with Army C2 systems;
- Tailorable based on mission need;
- Interoperable with joint, special operations, C2 and unified action partners;
- Easy to learn and sustain;
- Energy efficient;
- Continuously updating and delivering to support mission.
- These objectives require rapid prototyping, and a bias towards common hardware and software solutions that can be tailored to specific mission and user needs coupled with a secure supply chain and empowered user community.

e. S&T supports MI functions through three main activities to provide operationally feasible, competitive, and relevant MI technologies:

(1) Investigate technologies that may provide intelligence advantage over future competitors and peer adversaries.

(2) Anticipate technological needs for a dynamic and uncertain future operational setting.

(3) Produce relevant and feasible technologies that can transition into new programs, improve existing programs, or go directly to MI Soldiers in the fielded environment.

C-2. Immediate Army intelligence technology focus areas for fiscal year 2020

a. Interoperability.

- Governance and common services such as application programming interface gateways, common data foundations, and common interfaces.
- Machine intelligence and enablers such as cloud and data labeling.
- Increasing computational efficiency and reducing size, weight, and power while increasing effectiveness of sensors and processing systems.
- Modeling and simulation to support AI-enabled wargaming.
- Reducing cognitive burden on analysts/cognitive dominance.[58]
- Leveraging PAI, OSINT, and non-traditional information.[59]
- Improving the ability to exchange synchronous and asynchronous data, integrating EW/SIGINT to locate and identify targets, increasing the ability to amalgamate existing complementary data and previously unavailable signal data of EW and SIGINT systems obtained by increasing range and capabilities based on adversary signals of interest.
- Countering threats from unmanned systems.
- Development of security operations and continuous integration of new data and capabilities.
- Collaborative and distributed sensing, effects, and mission management.

b. Sensors – collaborative, multi-domain, instrumented, distributed, and AI-ready: technologies to support rapid prototyping for both sensing and ground station technologies to deliver a scalable, open architecture sensing enterprise. This includes:

- AI-ready sensing with onboard processing to characterize at the point of collection.[60]
- Sensors capable of operating at extended ranges in support of automated target acquisition (LRPF and indirect fires).[61]
- Automated and dynamic sensing that can collect and characterize both threat and environmental signatures and integrate across all aspects of Army operations including deep, urban, and subterranean to provide layered sensing to counter adversary layered defense.[62]
- Open architecture sensor integration capabilities to support rapid integration of sensor data, dynamic discovery, automated collaborative collection, and automated collaborative tasking.
- A C2 sensor web that allows for control of sensors across the battlefield enabling automated cross-cueing and automated tracking.
- Collaborative and distributed sensing as well as collaborative and distributed effects delivery.
- Instrumentation and tags necessary to leverage internet of things technologies.[63]

- Instrumentation and sensed data from those instrumented technologies should allow for establishing baselines on the activity of sensors, network links, user tools, and ground stations so that adversary and anomalous activity can be identified apart from normal usage.
- Leverage novel combinations of sensors in conjunction with emerging technology to leverage traditionally manned aircraft as optionally or remotely piloted to achieve sensor penetration in A2AD environments.

c. Data – governed, accessible, secure, and interoperable: New sensors will generate new data. Novel applications of existing sensing capabilities will produce novel sets of data in novel environments against novel objects. New analytics require:

- Clean, annotated, and accessible data.
- Continuous integration, shared situational understanding, and consistent capabilities across C2 at the data level.
- Extract data from non-traditional sources such as manuals, literature, and news.
- Data governance tools to adhere to proven standards so as to remain technology agnostic.[64]
- Modular data transformation and automated ingestion tools that can be used to quickly generate statistical models for analysis.
- Sensor data fusion of dis-similar sensor phenomenologies and modalities.

d. Analysis – automated, sharable, edge-ready, and mission-tailorable: Army intelligence is interested in tools and workflows deployable on government owned platforms and infrastructure that are tailorable to refine situational understanding – particularly in DIL environments.[65] To achieve these ends requires:

- Micro-service based capabilities.
- ML models that can be used for transfer learning.
- Automation to support the IPB process.[66]
- Reduction of cognitive burden through robotic process automation and automated data triage.
- Automated order of battle analysis, course of action analysis, dynamic collection management, entity recognition, product templating, data management, and structured observation management.
- Automatically generate collection management plans, automatically recommend effects based on the environment and available capabilities, and automatically conduct and assess battle damage.
- Analysis capabilities must be edge-ready, able to prosecute data directly from sensors with pre-trained machine intelligence models and must maintain coherence with the broader enterprise to prevent data degradation.

e. Enabling technology – hybrid-cloud, synthetics, annotations, interfaces, training, and signatures: The Army MI commercial cloud service provider is the de-facto governance and tenant pipeline for Army MI commercial cloud, while the DOD establishes the DOD cloud initiative and the IC continues to expand the IC commercial cloud enterprise. Leveraging these infrastructure service providers, Army intelligence is interested in enabling technologies for:[67]

- Cognitive engineering, AI, robotic process automation, and data science.

- System on a chip to provide edge processing and host analytics on the move.
- Capabilities to train and upskill the force.
- Ability to conduct realistic training, and training that adapts based on the skills of the user.

f. Emerging S&T trends: Statistical topic modeling has incorporated 52 S&T forecasts, which after mining several hundred documents, produced a corpus of 947 trends related to the emerging S&T landscape. This was further analyzed using natural language processing techniques which identified 10 core trends that are likely to influence the U.S. Army over the next 30 years. The relative degree of risk and opportunity of the following capabilities was also looked at with a summation that there was a strong correlation between risk and opportunity, especially in robotics and AI. The U.S Army will likely benefit from many of the following capabilities, including:[68]

- Robotics, AI, and automation.
- Advanced materials and manufacturing.
- Energy production, harvesting/scavenging, storage, and distribution.
- Biomedical science and human augmentation.
- Quantum computing.
- Mixed reality and digital mimicry.
- Food and water security technologies.
- Synthetic biology.
- Space technologies.
- Climate change adaptation technologies.

C-3. Near-term Army intelligence technology focus areas – Adapt - 2020-2025

a. Big Data, All source and multi-intelligence analytics and visualization. Integration and alignment of sensor-based observations, human-based observations, and open sourced data; application of established graph metrics, data mining, and pattern matching algorithms toward satisfaction of operational needs; innovation of new graph analytics; improved entity disambiguation via graph exploitation, especially on social media or other "small" communications; and fusion and analytic models specifically to support cyberspace and insider threat operations.

b. Multi-intelligence tasking, collection, PED (TCPED) and fusion at the point of collection and beyond. Cross-cueing capabilities and target identification based upon on-platform TCPED and multi-intelligence fusion; synchronization of on-platform fusion with distributed downstream fusion and entity refinement; cooperative exploitation of entities across the full PED enterprise (expeditionary and reach); provisioning large volumes of sensor data, especially from high-fidelity and non-traditional sensors; collaborative approaches to user-machine and user-user interactions; and improved miniaturization of TCPED and fusion on-board processors.

c. Modernized tactical SIGINT technologies. Large-scale data compression and transport over intermittent communications; higher throughputs for forward wireless communications networks; intelligent applications to provide focused, mission-relevant intelligence, analysis, and situation awareness; and improved form factors for computing devices.

d. Multi-phenomena identity derivation and exploitation. Exploration of new identity phenomena (for example – infrasonic, organizational linkages, etc.); increased stand-off capabilities for multiple sensing; fusion techniques that better exploit multiple phenomenologies; identify intelligence development for organizations and pieces of equipment; and structured approaches to pattern of life development and detection of pattern abnormality.

(1) Advanced processing and analysis of text, language, and linguistics.

(2) Processing (character and word recognition) of written communications, especially handwritten or otherwise poorly formed; interpretation of "short-form text communications", (e.g., chat, tweets) that rely on localized jargon or meanings; high-volume transformation between speech and text; translation of languages and dialects generally unavailable today; extraction of entities and relationships from text; determination of sentiment and intent from a stream of text-based information.

(3) AI capabilities to support text, language, and linguistic analysis.

C-4. Mid-term Army intelligence technology focus areas – Evolve - 2025-2035 - Realm of Probable

a. Advanced multi-modal, multi-functional sensing suites for both ground and mid-altitude. The development of terrestrial multi-intelligence collection quick reaction capabilities has shown the value of multi-modal collection systems for the mission set of enemy pursuit. Full integration of multi-modal collection, to include cross-cueing and sensor collaboration, remains an area for progress. More of an issue for the airborne platforms is the physical design and implementation of antennas (both passive and active) on the airframe to avoid interference. Using a radar system for both imagery and for target indicators provides the best multi-modal use of single systems.

b. Operationalized high-resolution hyperspectral imagery exploitation: algorithms for pre-processing and exploitation, developed for both off- and on-platform use; improved fusion capabilities to exploit hi-res imagery for entity tracking; compression or chipping techniques to improve imagery transport; and operational profiles for use of hyperspectral imagery.

C-5. Far-term Army intelligence technology focus areas – Innovate – 2035-2040 – Realm of Possible

a. Advanced human-machine interfaces (HMI) for collection, analysis, and synchronization.

(1) Improved visualization, conceptualization, and interaction of users with situational data in both time and space; advanced techniques for interaction with large volumes of data; rapid improvement of market HMI capabilities into Army MI systems; and immersive training approaches.

(2) Modeling, simulation and visualization of threat entities and events.

(3) Globally-integrated knowledge management.

b. Advanced multi-phenomena collection capabilities in heavy camouflage, concealment, and deception (CCD) and stealth, A2AD environments. Improvements in ranges, particularly for identification; additional processing techniques to exploit new synthetic aperture radar (SAR) waveforms; and improved algorithms for detection and discrimination of targets in clutter and CCD.

c. Swarm and counter-swarm capabilities. Development of platforms and architecture for sensor swarms; approaches for intra-swarm and inter-swarm collaboration; and methods for swarm counter-measures against hostile swarms.

d. Novel processing paradigms and hardware.
- Quantum computing.
- Neuro-synaptic.
- Bio-computing.

e. Ad hoc networks and quantum network planning and resiliency.

f. New application spaces and capabilities.
- Autonomous high performance computing.
- Audio and visual processing.
- Red and blue force analysis.

g. Real-time large scale data analytics.

C-6. Military intelligence capabilities for system enhancement by S&T enablers
Enhancements to current and future systems are included in appendix I.

C-7. Research technical statements

a. This section recommends a sub-set of breakthrough scientific discoveries and breakthrough technological innovations that supports the central idea to transform Army intelligence against peer competitors across the competition continuum. The research efforts outlined in this section are a result of collaboration between the concept expertise about future operational needs and technical expertise about use-inspired programs. Each breakthrough scientific discovery or breakthrough technological innovation effort is also linked to the required capability categories outlined in Appendix B. This section will be revisited at least annually to reflect the anticipated and evolving needs associated with the Army intelligence force of 2028 to 2040.

b. Future forces require the ability to process and transform a high volume of data into an easy to consume format at speeds and measures of performance far beyond human capability to support commanders' situational understanding in all operational environments.

(1) Breakthrough technological innovations. Research will improve support to decision making. Research that links two approaches that use various taxonomies and variables to express imperfect information to model and represent uncertainty for different modalities of data (e.g.,

sensor time series data and/or warfighter function tasks and decision variables) and weighs the imperfect nature of the source information and influencing factors will begin to capture how commanders weigh information prior to a decision. The ability to capture uncertainty of information in possible courses of actions developed through artificial reasoning based approaches such as this, will enable commanders to understand the negative outcomes associated with different courses of action increasing commanders' situational understanding. (RCs B-2.a, B-2.b, B-2.c)

(2) Breakthrough scientific discoveries.

(a) Research into AI enabled predictive modeling of adversarial (enemy) intentions and courses of action, where AI will collect and collate enemy doctrine, training, terrain; tactics, techniques, and procedures; and personalities to produce predictive models of potential enemy courses of action will allow commanders and staffs to reduce the time for the military decision making process. This advancement will enable future forces to ingest and exploit data from various information sources to support commanders' situational understanding. (RCs B-2.b, B-2.c)

(b) Research to transform raw and processed data into actionable information, where causal inference is used to aid in determining components, objects, and signals from different modalities with complex relationships to aid in forming the "best" hypothesis, will enable the generation of courses of action and present uncertainty of information. Advances in reason-based decision making will enable commanders to quickly recognize and act upon opportunities to seize the initiative. (RCs B-2.b, B-2.c)

(c) Research in opportunistically sensing Soldier intent and interest coupled with advancing methodologies to sense and interpret Soldier behavior in the real-world environments are enabling AI to use the human brain to prioritize tactically-critical information without providing any additional burden or stress on the operator. Tactical awareness via collective knowledge will allow blue force AI to infer and integrate the intent of Soldiers as it evolves with mission execution and create a form of super-human intelligence that leverages the tactical knowledge of Soldiers with the speed and processing power of AI. (RCs B-2.c)

(d) Research on multi-timescale models of individual humans and machine learning based predictions of future human behaviors will enable AI to infer human information processing performance and will allow for future AI to weight inputs from multiple humans in making decisions. AI-inferred human long-timescale processing will allow blue force future AI to have mechanisms to non-linearly improve its integration of Soldier intelligence into intelligence mission planning and asset coordination. (RCs B-2a)

(e) Research on context-aware information filtering integrated with advanced visualization technology, where high-performance computing infrastructure is leveraged to analyze the data streams at multiple levels of context, prioritize, and visualize the analyzed data in a variety of mediums, will enable rapid decisions through the production of actionable information. This advancement will enable the integration and consumption of large quantities of data, spanning multiple data types, while reducing cognitive overload. (RCs B-2.b, B-2.c)

(f) New advancements in distributional semantics, ontological representations, data mining and representational learning are enabling the training of information extraction with limited annotations and the automatic extension of ontologies. The advancement will enable the development of robust and accurate information extraction and querying systems that can process unstructured textural data from new and rapidly evolving domains of knowledge with limited data, which will lead to improved commanders' situational understanding in all operational environments. (RCs B-2.b, B-2.c)

(g) Research to exploit knowledge of mammalian spatial reasoning neural systems which have hundreds of different sub-architectures to AI, which currently has one of those sub-architectures, to develop a completely novel class of AI will revolutionize AI spatial reasoning capabilities. Advancements in neuro-derived AI will lead to a variety of new operational capabilities in areas such as data analytics that will have human-like reasoning, but function at a rate faster than humanly possible. (RCs B-2.a, B-2.b, B-2.c)

c. Future forces will require the ability to conduct information collection in all domains and the information environment to support the targeting process and commanders' situational understanding in all operational environments. Future Forces require access to data and communication technology across echelons to support commander's situational understanding in all operational environments.

(1) Breakthrough technological innovations.

(a) Research to develop a physics-based and data-driven tool for aircraft design for extreme performance attributes, assessment of a design concept, and evaluation of technology impact on the design trade space will enable unprecedented capability in future UAS. This research will enable the realization of UAS capable of high speed, nap of the earth flight for information collection applications such as deep sensing and ISR. (RCs B-2.a)

(b) Research into hardware and protocols for alternative communication modalities for both low probability of detection and classification will allow for secure, and resilient communications at all echelons. This advancement will enable shared situational understanding across echelons for improved situational understanding. (RCs B-2.b)

(c) Research on image processing and activity recognition will rapidly train algorithms from sparse, unlabeled data rather than from large databases of labeled images since the latter is not available for all complex operational environments. This advancement will enable robust performance of assisted target recognition that can adapt to the changing operational environment. (RCs B-2.b, B-2.c)

(2) Breakthrough scientific discoveries.

(a) Research in atom interferometry, including creation of macroscopic quantum superposition states, ways to prolong coherence, spin squeezing, entanglement creation, and ways to improve size, weight, and power and resilience of existing quantum sensors, will lead to more

sensitive and robust sensors for electric, magnetic, electromagnetic and gravitational fields among other things. This advancement will enable both friendly and enemy signatures to be detected and monitored at unprecedented sensitivity in compact, resilient, and deployable packages, enabling by mid-term improved situational awareness, and in the long term sensing orders-of-magnitude beyond what is possible from traditional sensors. (RCs B-2.a, B-2.c)

(b) Research into creation, maintenance, and distribution of entanglement will be the basis of future quantum networks containing, among other things, sensor nodes that will enable distributed quantum sensing for more advanced signature detection as well as time distribution. This advancement will enable sensing for more advanced signatures, including gradients and higher derivatives, to provide a much more complete picture of the underlying structure of the field patterns being sensed, enabling enemy signatures to be detected and monitored around high-value assets with unprecedented sensitivity; and clock synchronization for situational awareness, greater bandwidth communications and networking. (RCs B-2a, B-2.c)

(c) Research into reciprocal and deterministic radio frequency (RF) hardware and low-latency techniques and algorithms for time and phase synchronization of distributed transceivers will enable complex communication and resilient EW application of ground and air platforms to degrade adversary sensors and communications allowing for extended operations within A2AD environments. This advancement will enable non-kinetic offensive EW options for commanders to shape the adversary's information environment. (RCs B-2a)

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

(e) Research in event-based imagery, where data is generated only when there has been a change in the environment, has the potential to significantly reduce the amount of data that needs to be transmitted. This alternative to computer vision, which typically requires high bandwidth, will allow for the use of communication modes that are more robust but low bandwidth. (RCs B-2a, B-2.b, B-2.c)

(f) Research in algorithms and communication approaches for developing, maintaining, and sharing situational awareness across and between humans and AI distributed across echelons are leading to the creation of mechanisms to understand gaps and inconsistencies in information flow and communications underlying decision making. Shared Human-AI awareness will allow future forces to enhance shared situational awareness throughout the competition continuum. (RCs B-2.b)

(g) Research in complex activity detection and complex event processing can provide advanced understanding of complex and evolving potential targets by exploiting multiple sensing modalities to detect activities involving interactions between multiple interacting objects captured

from spatially distributed, resource-constrained platforms. Advancements in this area will enable the use of distributed analytics to increase commanders' situational awareness, to include continuous target development of increasingly dynamic and sophisticated threats particularly, at the tactical edge and at the speed of engagement. (RCs B-2.b, B-2.c)

(h) Research in human-guided AI cycle-of-learning are integrating different forms of human interactions with AI at different stages of product development to effectively adapt a single AI's behavior and performance over time to increase the ability of blue forces to respond to adversarial actions, new technologies, environmental changes, and mission requirements; decrease training data requirements; and increase appropriate Soldier trust and use of technology. Human-guided AI across product development dramatically reduces the time to field technology and applications throughout the competition continuum potentially leading to new intelligence capabilities. (RCs B-2.c)

(i) Research in learning human-machine interface technologies, task requirement dependent models of human-AI capabilities, and interactive machine learning are all using mission data and human-led after-action-reviews to iteratively adapt AI planning and coordination technologies on a mission-by-mission basis. Human-guided AI asset coordination capabilities will enhance blue force capabilities to coordinate complex information collection operations throughout the competition continuum to overmatch enemy technologies without requiring Soldiers to be in the loop. (RCs B-2.a)

Appendix D
Contributions to Competition - Set the Theater

a. This vignette is set in 2028 in a mature overseas theater. The theater has a forward stationed CCMD, ASCC, corps headquarters, MIB (T), TSOC, and other theater enablers.

b. Other than one forward stationed BCT, maneuver forces are rotational into theater. The theater has mature alliance and coalition partners.

D-1. Organize the force

a. The newly assigned ASCC G-2 performs an initial assessment of Army intelligence capabilities in theater. The force posture includes forward, rotational, and surge capabilities from all three Army components and Department of the Army civilians augmenting the in-theater capabilities. The G-2 staff is fairly robust and has been present in theater for decades. The G-2 has a good working relationship with other staffs in theater such as the Army Air and Missile Defense Command, MDTF, Information Warfare Command, and ARSOF elements.

b. The MIB (T) is the senior MI organization supporting the ASCC, is assigned to the CCMD, and is in an operational control relationship to the ASCC. The MIB (T) anchors the intelligence effort in a geographic region, providing continuous overwatch, establishing theater intelligence architecture, and integrating intelligence forces into the theater and connecting them to the intelligence enterprise. As part of setting the theater, the MIB (T) establishes the theater

intelligence architecture to facilitate PED of collected information. The MIB (T) conducts theater army target development in accordance with the CCDR campaign plan. The MIB (T) is the entry point for INSCOM functional brigade assets into the theater and enables the integration of corps and below assets into the theater intelligence structure. Also, with longstanding relationships built from an enduring theater operational presence, the MIB (T) is postured to enable the integration of JIIM capabilities.

(1) The operations battalion provides the ASCC analysis control element (ACE) with broad coverage of the entire theater and limited capability to support a specific focus area. The battalion has single discipline and all source analytic capabilities, a watch section to provide 24 hour intelligence coverage for ASSC designated tactical units as they deploy to and within the theater of operation, and intelligence support elements that provide liaison with coalition, U.S. Army, joint or combined military organizations and their associated intelligence.

(2) The forward collection battalion provides overseas CI investigations and operations to prevent acts of espionage, sabotage and terrorism directed against U.S. facilities. CI elements work with the ASCC G-3, protection cell (including the Provost Marshal), and with available theater ARSOF in a "red team" capacity to conduct vulnerability assessments of facilities and all the nodes critical to future force flow during a crisis. MIB (T) CI coordinates with CONUS-based 902d MI Group CI to knit this assessment with force projection assessments originating in CONUS home stations. The battalion conducts liaison with local law enforcement supporting force protection. The technical surveillance countermeasures team also provides vulnerability assessments to identify weaknesses with locks, doors, alarms, telephone systems, and network and computer security.

(3) The collection detachment HUMINT teams perform intelligence interrogations, HUMINT source operations, debriefings, screenings, and intelligence liaison in English and foreign languages in all conflict phases to identify adversarial elements, activities, intentions, capabilities, and locations through the questioning of people in the OE. The document exploitation team systematically extracts information from threat documents for the purpose of producing intelligence or answering information requirements. The SIGINT collection team provides intelligence collection support by the detection, collection, processing, and analysis of foreign intelligence signal products. This team relies heavily on a robust, networked, sensor grid to provide timely, accurate information.

(4) The MIB (T) has a USAR theater support battalion (TSB) that conducts multi-disciplined intelligence analysis operations in support of the ASCC. It provides collection capabilities in support of theater level security cooperation missions. The TSB provides analytic augmentation from CONUS and provides teams into theater as part of the theater engagement plan.

(5) Finally, the MIB (T)'s status as an INSCOM subordinate command provides interior lines of communication to INSCOM HQ for identifying and coordinating the employment of available national, joint, and service level resources, capabilities, and capacities to support and reinforce validated theater requirements. In response to those requirements, the Army may direct INSCOM to employ or deploy its functional brigades, including the aerial intelligence brigade (AIB), to provide reinforcement and surge capability to the theater. The theater ACE has a daily

relationship with multiple analytic centers including the CCMD joint intelligence operations center (JIOC) and centers in CONUS. INSCOM's National Ground Intelligence Center provides current general military intelligence on foreign ground forces as well as insights into future capabilities including detailed insights into foreign equipment. INSCOM, as the Army's representative to the national agency intelligence discipline functional managers, has access to cutting edge technologies developed for unique problems. These capabilities are often made available to apply against theater problems.

c. The designated corps headquarters has a G-2 section designed to support both main and tactical command posts. Capabilities include limited analytic control elements, targeting, and operations elements at both command posts. The corps has no down trace units, but can receive rotational or expeditionary units. The corps G-2 can build regional expertise through rotational assignments of divisions and BCTs.

(1) With no down trace units, the corps expects support from a USAR E-MIB (GS). The E-MIB (GS) provides CI, HUMINT, analysis and PED capacity to the corps and serves as the senior MI C2 headquarters for the corps. The USAR E-MIB consists of two E-MI Bns (GS) with CI, HUMINT, and an all-source and PED company that conducts multi-discipline intelligence analysis, OSINT, and PED in support of multi-domain situational awareness, target development, IPB, and MDMP requirements. The E-MIB (GS) is not forward stationed or regionally aligned, so ramp-up for mobilization and theater awareness will require an extended timeline.

(2) Rotational and expeditionary divisions and BCTs will come with G-2 and S-2 sections and MI formations. BCT MI companies are found in the active component and the National Guard. Active component E-MIBs contain a division support IEW battalion for each committed division and ARNG E-MIBs contain division IEW battalions to support all eight ARNG divisions.

d. The TSOC is assigned under OPCON to its respective geographic combatant commander to meet theater-unique special operations requirements and is responsible, in part, for integrating SOF intelligence capabilities into theater operations. It provides for the planning, preparation, and command and control of special operations intelligence assets from across the joint services. The TSOC J2 ensures that SOF intelligence capabilities are synchronized fully with conventional military intelligence operations by providing the staff expertise to plan, conduct, and support special operations intelligence efforts in the theater's area of responsibility.

e. The ASCC G-2 also noted the MI capabilities found in the multi-domain task force, SFABs, and theater ARSOF.

f. The ASCC G-2 met with the theater J-2 to better understand joint assets that could support operations. For analytic support, the J-2 relies on the JIOC located in theater. The JIOC operates a fusion center that conducts current situation analysis, collection management, and long-range assessments and threat estimates. Additionally, U. S. Air Force reconnaissance assets based in theater provide multi-intelligence collection supporting the combatant commander (CCDR) and national priorities. Other service collection assets are also available. Due to the maturity and sophistication of the theater, national agencies have a footprint in theater providing SIGINT, GEOINT, and HUMINT capabilities.

g. As the ASCC G-2 continued to assess available resources, the G-2 staff presented an overview of alliance and other partner capabilities, including specific sharing agreements by country and by intelligence discipline. Partners increase capacity and capability and formal arrangements and governance strengthen interoperability with intergovernmental agencies, multinational treaty partners, and coalition partners. Many of these partners had liaison sections in the ASCC headquarters, and the G-2 met these partners to build relationships. The ASCC G-3 staff briefed the G-2 on the theater engagement plan, highlighting by country which intelligence related capabilities and capacities were targeted for improvement. Army forces conducting engagement will be a rich source of information on the OE, and the G-2 must routinely focus engagement units to satisfy information gaps and capture observations. The G-3 staff also briefed the G-2 on the CONUS-based rotational plan, allowing the G-2 to match rotational units with outstanding information requirements. Regional alignment will build understanding of normalcy and support warning intelligence to recognize when that normalcy changes unacceptably.

D-2. Architecture

a. The ASCC G-2 is responsible for integrating Army intelligence capabilities into the CCMD intelligence architecture, and the MIB (T) is the implementation agent. The Army's intelligence architecture is an integral part of the Army information network. The Army information network and other DOD information networks across multiple security levels provide the architectural backbone and connect information collection, PED, and analysis from all sources to decision makers. INSCOM provides a global backbone through the GISA, providing redundancy for storage and data transport. The MIB (T) uses a fixed site intelligence analytics interface as the foundation for data storage, processing, security, and applications. The MIB (T) operates across NSANet, JWICS, SIPRNet, coalition, NIPRNet, and unclassified internet. An intelligence analytics interface fielded through DCGS-A CD2 provides data management and data analytics that increase access to multiple sources of information across the echelons. The architecture connects all Army, joint, and national collection platforms, PED and analytic sites for decisions at theater level. The TITAN ground station brought capability across the Army echelons, bringing all domain sensor collection to Army formations. The MIB (T) also has direct connectivity with the TSOC to facilitate planning and operations.

b. The theater intelligence architecture also incorporates the CONUS-based TSB and connects Army rotational units in theater and connects to their home-stations. The MIB (T) G-6 integrates tactical rotational units down to maneuver battalion including all tactical collection platforms. Alliance and other foreign partners are integrated into the architecture within security limits. While many modern systems share common data standards, the architecture cobbles together legacy and open source data that requires additional handling for inclusion. The architecture leverages cloud technology, providing constant update of flexible, intuitive, powerful tools that help analysts anticipate adversary actions. Distributed clouds mitigate a single failure point, and support large volumes of structured, unstructured, or differently structured data to complete the threat and environmental portions of the common operating picture. The cloud provides increased access to data, including the National Security Agency cryptologic cloud, the National Geospatial-Intelligence Agency GEOINT cloud, and others for geographically dispersed elements. Maintaining this architecture is a continuous process.

c. Establish authorities and permissions. The ASCC G-2 understands the partner complexities in theater from previous assignments. The theater has a very mature alliance with dozens of formal partners. The theater also has several temporary coalition partnerships with non-alliance partners established for a specific end. These partnerships may include host nation SOF which are the purview of the TSOC and its subordinate special operations forces. Intelligence sharing, however, varies by country and by intelligence discipline as driven by the U.S. national functional manager for that discipline. Sharing of SIGINT is different from sharing of GEOINT, for example, and also varies by partner. Weaving these two-way sharing arrangements into the intelligence architecture demands cross domain solutions at the data level. In addition to sharing, some partners place restrictions on U.S. intelligence operations in their sovereign multi-domain space. The foreign disclosure officer, the MIB (T) S-3, the MIB (T) S-6, and the ASCC G-3 must consider these authorities and permissions when planning operations to include meeting the combatant commander's daily operating requirements and the warning intelligence system.

d. Provide access to theater collection and databases. Preparation during competition includes building foundational intelligence to defeat adversaries' destabilization efforts, and if that fails to deter escalation and prevent cold transitions into conflict. Data access allows the MIB (T) and other units to meet daily operational requirements or potential operational requirements. Understanding the legal permissions and authorities, the MIB (T) S-6 explained the technical authorities to operate on the theater network. Accreditation of CONUS-based systems requires constant planning to keep theater engagement forces relevant. Access into theater data stores by potential reinforcing elements down to BCT is also worked to leverage CONUS capacity and include expeditionary force planning requirements. Access extends outside intelligence elements to support operational planning and targeting. Relevant ARSOF elements extend to CONUS as well, requiring close coordination with the TSOC. Access to data also extends opportunities for creative analytics to support modeling and forecasting.

D-3. Prepare analytically

a. Conduct IPB. After reviewing the foundations of theater intelligence capabilities, the G-2 turned attention to producing support for the theater. After meeting with the ASCC G-3 to understand theater planning priorities, the G-2 met with the MIB (T) operations battalion (theater ACE) to learn how it supports planning and operations. The CCDR established multiple focus areas of actual friction or potential conflict across the theater. A thorough IPB helps commanders identify windows of superiority in each domain, the information environment, and the EMS. The theater ACE briefed the G-2 on the foundational intelligence baseline, specifically the physical considerations relevant to military operations, including infrastructure vital to friendly force flow to potential conflict areas across the domains. Alliance partners are particularly cooperative providing status and capabilities of transportation networks and ports of entry throughout the theater. The ACE briefed temporal considerations of force flow and factors that could affect strategic movement through the different domains. The ACE spent considerable time on civil considerations impacting the area. It also provided a detailed capability laydown of the major antagonists in theater and identified gaps that require further work. The ACE chief briefed how the IPB effort influences collection and identifies risk. The ACE routinely includes updates to the IPB products during its current intelligence updates. Products are widely available.

b. Conduct warning intelligence. The ACE is part of the theater warning effort and briefed the G-2 on the indicators it is tracking and how it fits into the overall warning intelligence system. The theater is tracking multiple warning problems and most could escalate into a situation that involves Army forces. Traditional indicators of troop movements and training exercises drive much of the daily collection requirements. Warning problems extend into the cyberspace domain and the information realm, and the ACE works closely with other theater assets to monitor indicators. Social media usage is another closely watched warning indicator; sudden increases or decreases of postings can signify potential crises. Other warning problems require political, economic, or medical expertise. Engagement deployments into theater generate temporary warning problems to provide oversight of small, often isolated elements. The warning cell has a close relationship with the collection management cell.

c. Analyze high volume data. At this point, the G-2 had an understanding of the magnitude of the data management problem. Data sets to support IPB and warning intelligence alone are in the petabytes and the G-2 asked for a better understanding of how analysts manage, mine, and refine this data. The theater has a GISA node that provides regionally focused, responsive, reliable, and robust information technology services and connectivity to the theater. This data center connects users to enterprise data services and seamless access to national agency intelligence networks from unclassified to top secret compartmented networks. An intelligence analytics interface organizes data management and applies advanced analytics which are accessible regardless of unit, echelon, or location. An intelligence analytics interface provides a persistent data fabric which allows data analytics and services and complies with industry standards. Multiple automated tools apply AI and expedite discovery, matching, aggregation, geolocation refinement, and correlation of data. Analysts have access to legacy and current data.

d. Target anti-access system. The G-2 understands the toughest operational problem in theater is to defeat a peer anti-access system. The ACE must understand the C2, fires, and ISR systems that comprise the anti-access system, determine the vulnerabilities of each component, decompose those components into observables that collection can target, and manage collection to establish an activity baseline. It discussed restrictions on collection access, and how authorities might change if tensions escalated. This analysis feeds into the warning intelligence system. If tensions escalate, this process will become more difficult as adversaries will attempt to confound collection. The G-2 asked what changes to collection schemes were planned if tensions escalated and how to deliver those results to C2 and fires systems. The G-2 asked if this had been exercised and if the supported communities had issues with timeliness and accuracy. The G-2 also asked about adversary ISR systems and their targeting of U.S. LRPF systems. The ACE discussed measures to achieve windows of superiority in the EMS, cyberspace, and space domains in order to counter anti-access systems. The G-2 asked what nonlethal means target the anti-access systems and if they were fully integrated into the ACE efforts.

e. Understand adversaries C2 systems and long- and mid-range fires systems. Anti-access is a system of systems, and the G-2 wanted to drill into the capabilities of each piece of the anti-access problem. The threat has an extensive air defense system, and the ACE identified the location of each system in the inventory, the specific capabilities, and the training history of the operational units. Garrison locations are part of the standing collection plan and any movement, radar testing,

and other training raises concern. The ACE closely coordinates with the theater air operations center and the CCMD joint intelligence and operations center to ensure the latest information on the air defense picture. Similarly, the ACE tracks long and mid-range surface to surface fires. The ACE has a good relationship with INSCOM's National Ground Intelligence Center to understand the systems and potential development of increased capabilities. The ACE also briefed the C2 system for threat fires and their relationship with the theater technical control and analysis element to maintain the latest information on the threat C2 system.

f. Conduct robust operational assessment. The G-2 delved into the numerous assessments the ACE had published and asked for the update schedule on each and the production schedule for other assessments. The G-2 asked the G-3 and other staff elements what assessments they needed for planning. The G-3 in return asked for a routine assessment of the effectiveness of friendly actions to defeat adversary unconventional and information warfare activities as well as counter adversary ISR activities. The G-3 also asked for assessments of friendly deception activities.

g. Prepare for urban areas. The G-2 was not satisfied the ACE had prepared properly for urban areas included in some of the potential crisis spots in theater. There were not adequate analytic models to understand the mechanics of political, social, and criminal organizations. The ACE could not determine the key urban signatures that develop pertinent knowledge and the techniques to capture those signatures. While the Army may want to avoid combat in urban areas, urban areas are fertile areas for competition activities. The G-2 asked which urban areas in the operational support area were susceptible to peer intervention in the competition period. The G-2 asked how existing analytic models supported friendly information campaigns and their effectiveness. The G-2 asked if the ACE coordinated with local authorities on vulnerability assessments of urban infrastructure and suggested this may be an additional task for CI teams and their local liaison. The G-2 asked for profiles of criminal elements that could interfere with force flow into and through the theater. Turning to urban areas that would fall in potential combat zones, the G-2 asked about support to lethal and nonlethal target planning and the complexities of precision collection inside the urban areas. The OSINT section in the operations battalion did offer insights into urban problem sets.

h. Conduct OSINT activities. Open sources possess much of the information needed to understand the physical and human factors of the theater OE. The MIB (T) OSINT section, in the operations battalion, conducts OSINT for the ASCC. The section is organized based on operational variables (political, military, economic, social, infrastructure, information, physical environment, and time) and monitors mass media, both of friendly and adversarial nations, to better understand the theater. The OSINT section provides insight into populations, including social media, search-engines, databases, governmental and nongovernmental organization information sites, biographical data, PAI, business, industry, political, and economic information. The section monitors theater information requirements and is integrated into the collection strategy. The OSINT section has developed distributed capabilities incorporating regionally aligned CONUS-based forces into their efforts. It has relationships with partner OSINT capabilities, such as the TSOC's OSINT element, supported by SOF's OSINT capabilities in CONUS, and U.S. national agency partner capabilities. The OSINT section closely monitors adversary social media and looks for spikes or sudden decreases in activity that may indicate impending hostile actions. It also tips and cues other collection assets when appropriate. The G-2 asked how the section evaluates the

reliability of open sources in order to distinguish objective, factual information from biased and deception efforts. While impressed with the OSINT section activity, the G-2 challenged it to create an internal training program to stay on the edge of public information and social media trends.

D-4. Conduct information collection

a. Conduct reconnaissance and surveillance in all domains. Theater collection capabilities are never at rest and extend beyond the MIB (T) to detect complex signatures in accessible, hazardous, and physically denied areas. The Army theater strike effects group, multi-domain task force, and other organizations have non-standard collection capabilities to satisfy the commander's information requirements. Additionally, the theater has an aerial exploitation battalion (AEB) from the AIB to collect SIGINT and GEOINT using manned and unmanned platforms. Rotational engagement forces are also included in the collection strategy as they observe the physical environment and may be in range to collect against adversarial countries. HUMINT teams use the competition period to develop sources throughout the theater. Source development requires long lead times, but could pay dividends during conflict. Similarly theater ARSOF requires long lead times to set conditions for deep sensing contributions.

b. Converge national, theater, and organic collection. The JIOC is the focal point for integrating joint and national intelligence collection, and the MIB (T) has a liaison to the center to ensure Army interests compete with other requirements. The theater has robust Air Force and Navy collection assets that routinely collect from aerial and maritime platforms. National intelligence agencies also have robust fixed and mobile collection capabilities across the intelligence disciplines. Although peacetime conditions limit the sensor range of many assets, national technical means extend that range for high priority targets. Warning intelligence consumes much of the theater collection capability. Collection constantly builds EOB databases for further collection and to support potential EW activities. The ACE maintains visibility of asset availability and missions. Many assets incidentally collect information of value based on their proximity to targets. Access to what otherwise may be superfluous adds to theater databases. The JIOC also has visibility of alliance and other partner collection within sharing agreements.

c. Conduct CI. MIB (T) and special operations CI teams are an integral part of the multi-discipline approach to intelligence operations. Army's CI mission is to detect, identify, deter, disrupt, exploit, or neutralize foreign intelligence entity collection and terrorist activities against U.S. interests. MIB (T) CI teams fuse intelligence, security, and law enforcement type techniques into a single element that analyzes the foreign intelligence threat and employ a broad range of functions to protect Army personnel, operations, facilities, information, technology, and networks. They provide CI operations, investigations, collection, analysis and production, and technical services. They also conduct counterespionage, CI support to protection, and CI support to CO. MIB (T) CI teams provide support to deployment and movement operations and are always vigilant against any insider threat. CI teams support planning and security of inter and intra-theater force flow (fort-to-port), and are also part of the theater counter special operational forces effort. They also conduct liaison with U.S., host-nation, and multinational military and civilian intelligence, law enforcement agencies, security agencies, and the appropriate protection elements for information-sharing and operational coordination. The MIB (T) routinely incorporates CONUS-based CI elements that rotate through the theater on engagement missions.

Appendix E
Contributions to Armed Conflict - See deep

a. The CCMD has been active and successful countering peer unconventional and information warfare activities. Alliance partners enjoy peace and stability while some peripheral countries have become less stable.

b. The peer threat believes conditions support territorial expansion to restore historical boundaries. The peer threat begins mobilization and posturing along its border. Political tensions are high.

E-1. Information collection

a. Employ Army high-altitude ISR platforms to provide deep sensing. In reaction to the increased activity, the combatant commander orders increased surveillance into the peer threat. Joint and national collection platforms surge to increase persistent coverage of the crisis area. The systems are planned and coordinated with the airspace control authority and/or the space coordinating authority for de-confliction and integration, to include synchronization of multiple ISR platforms and systems for each component and multinational partners. Collection platforms operating near the alliance border note increased activity from threat air defense systems. As a precaution, more vulnerable platforms adjust their patterns with Army medium altitude aerial systems reorienting to rear area surveillance to counter the unconventional threat. Meanwhile, the Army and partners employ high altitude MDSS platforms that can see deep into threat territory while remaining outside their air defense umbrella. These platforms move into position and establish reporting links, both high altitude relay and satellite relay. High altitude platforms have both onboard sensors and can release swarms of unmanned sensors that are expendable and can penetrate the sophisticated anti-access system. As tensions increase, the Army works with partners to maintain resilient satellite constellations and requests additional support as required.

b. Employ a layered ISR network in all domains. A layered ISR network increases opportunities for cross-cueing to improve fidelity and accuracy of information. National technical means, high altitude, and low earth orbit systems provide SIGINT, GEOINT, and measurement and signature intelligence (MASINT) coverage and detection of select targets to support LRPF. Medium altitude collection monitors activity along the border and develops situational understanding, templating threat systems that will impede penetration operations. Low altitude and ground-based collection focus on immediate targets that could impede cross-domain maneuver and identify opportunities for Joint Force success. Collection in cyberspace supports OCO and develops insights into threat intentions. HUMINT and CI forces look for threats to the force and force flow as well as look to intentions. HUMINT sources developed during competition provide deep sensing. Reporting to the theater ACE and JIOC speed cross-cueing and fidelity of information. Alliance partners improve context and often provide access unavailable to U.S. only organizations. Partners increase their activities in both technical and human collection, coordinating activities through the JIOC. As tensions transition into conflict, fifth generation aircraft and select unmanned aerial systems penetrate the enemy anti-access system providing

reconnaissance and battle damage assessments. More vulnerable aerial platforms adjust their flight profiles.

c. Collect in urban environments. The G-2 realized there were two distinct urban collection problems: urban areas in the operational support area threatened by unconventional forces, and urban areas in the close maneuver area and beyond. In the operational support area, the MIB (T) employed CI and HUMINT assets while the AEB flew SIGINT and some GEOINT collection missions targeting enemy special purpose forces. Precision target location in the close and deeper areas used high altitude, space, cyberspace, developed HUMINT sources, and ARSOF assets. Special built sensors filtered signal echo to improve SIGINT geolocation, and exploitation software templated activity where GEOINT collection was shadowed or masked. The volume of social media and cellular phone traffic and subterranean infrastructure challenge conventional collection. The internet of things also provided surveillance where U.S. or alliance forces had no access.

d. Integrate capabilities with EW and cyberspace. The threat employed significant EW and cyberspace activity in the close and support areas, attacking critical infrastructure, military and civilian networks, vehicles, ships, and aircraft. In response, TLS provided a multi-discipline, multi-modal collection and analysis effort while providing non-kinetic fires in support of the BCT and division commanders. Using established EOB, TLS teams used SIGINT and electronic support (ES) collection and support from aerial assets to refine frequencies of interest. The cyberspace electromagnetic activities section, in coordination with the Technical Control and Analysis Cell, presented non-kinetic options to the targeting fires cell. To create windows of superiority, TLS conducted EA and offensive CO against threat C2 and fires systems to deny, disrupt, degrade, destroy, and manipulate threat electromagnetic and cyberspace dependent capabilities.

e. Provide expeditionary capabilities. As tensions elevated, CONUS-based forces mobilized and began strategic movement to theater. Rotational forces already in theater reoriented to the newly designated joint operational area. The corps headquarters updated planning to incorporate expeditionary collection capabilities designated for deployment into theater. As tensions began to rise the USAR E-MIB aligned with the corps sent an advanced party and began split based operations until the main body could arrive in theater. Theater CI forces increased operations in ports of entry and along possible movement routes, working with host nation law enforcement and intelligence agencies. The USAR TSB aligned with the MIB (T) deployed to theater, reinforcing collection and analytic capacity. MIB (T) CI teams also coordinate with CONUS-based 902d MI for a smooth transition of support to deploying forces. USAR E-MIB CI teams plan for CI coverage in the corps area.

f. Link sensors to shooters enabled by AI. Sensor to shooter linkages proved successful during conflict. Increased processing at the point of collection made sensor data immediately usable by fires systems. TITAN ground stations at echelons BCT to theater fed MDSS and national collection into fire control systems for immediate action. AI automated cross cueing for greater automatic target recognition (ATR) and target location precision.

g. Converge national, theater, and organic collection. As large scale combat erupted there was an enormous amount of information collection in the joint operational area. While all levels of command competed for non-organic collection, collection results were available to all echelons BCT and above using TITAN ground stations. National, theater, and Army MDSS sensors detect and report through TITAN supporting targeting and decision-making at all echelons. TLS collection integrated into the theater collection structure and provide continuous support to maneuver units during DIL operations while on the move. Sensors report to intelligence, C2, and fires information systems to speed targeting and decision cycles. Conventional civil affairs and ARSOF reporting is integrated into theater collection and supports LRPF and cross-cueing other sensors.

E-2. Analysis

a. Visualize the battle in all domains, the EMS, and the information environment. The enemy was active in every domain and had clearly coordinated initial activities across domains to maximize initial success. Commanders at all echelons, including down to battalion level, demanded situational awareness across domains to create windows of superiority for decisive action. Intelligence assets and other sensors surveilled from all domains into all domains, the EMS, and the information environment, reported to TITAN ground stations, feeding the common operating picture in the command post CE. Understanding weather, to include micro-weather, identifies windows of superiority for friendly actions.

b. Continue IPB. As each level of command energized the MDMP, the IPB effort increased. The IPB effort supported current and future operations including sequels and reactions to branches. A solid foundation of terrain and infrastructure aided the effort. Automation expedited the routine steps in the process. Connection with the CEs facilitated sharing and distributed production.

c. Target enemy long range systems. The collection manager heavily weighted the collection effort against enemy long range systems and their support forces during the initial anti-access fight. After success against those targets, priority shifted to mid-range fires to support the area denial fight.

d. Identify high-priority targets on a “cluttered battlefield”. Analysts, aided by advanced tools, identified the unique signatures of the highest priority targets and filtered incoming collection accordingly. Cross cueing sensors confirmed the high priority targets and improved the targeting accuracy. Connectivity with fires systems improved the sensor to shooter speed allowing fires to service the fleeting targets.

e. Conduct BDA. As the conflict continued, tracking enemy battle losses became problematic. The collection manager dedicated collection missions against high priority targets. Fifth generation fighters provided BDA on their missions and along their routes. Analysts used foundational system assessments aided by AI, and inventories as a baseline and decreased holdings accordingly. The ACE had direct communication with the fires commands at all echelons to provide feedback on fire missions. Additionally, ARSOF was a highly reliable source of BDA reporting.

f. Analyze high volume data. AI and ML aided the data management problem as collection volume rose. Dedicated data scientists were invaluable in this regard. Pre-hostility algorithms and ML helped analysts organize and prioritize the volume of data and helped verify the veracity of data by identifying patterns consistent with enemy deception efforts.

Appendix F
Contributions to Returning to Competition - Reset the Theater

F-1. Organize the force

a. After favorable conflict resolution, the ASCC G-2 had to reset and reorganize the theater's intelligence organizations and operations to support the new normal for providing intelligence support in theater. Although the peer threat maintains significant capabilities, no international boundaries shifted as a result of the conflict. Non-alliance countries in the former joint operational area are less stable than before the conflict.

b. Adopt force posture to new security environment. Much of the surge in intelligence capabilities and capacities will be relevant in the near term security environment. The corps requested the USAR E-MIB remain in theater to provide analytic capacity to monitor conditions of hostilities cessation. The USAR E-MIB CI and HUMINT teams will also provide significant support to protection. When faced with gaps in internal theater capabilities and capacity, the MIB (T), in coordination with the ASCC G-2, can request tailored support from INSCOM functional brigades to monitor post hostility conditions and indicators of civil unrest in the new environment. MIB (T) CI teams will work closely with civil affairs and law enforcement elements to maintain order. The G-2 coordinated with the G-3 as the theater reset the rotational force and engagement strategies.

c. Regenerate partner capacity. Alliance partners performed well during the conflict, but operations revealed many shortfalls in intelligence sharing. The G-2 charged the deputy G-2 to lead a team in identifying sharing problems to include processes, policies, and interoperability. The G-2 charged the deputy to look at foreign military sales and U.S. national agency programs to improve interoperability. Additionally, the State department approached non-alliance countries in an effort to improve relations and build capacity that will stabilize the countries and improve their self-reliance. The theater SFAB reached to the MIB (T) for assistance as needed.

F-2. Architecture

a. Adjust architecture to new security environment. The conflict stressed the theater architectures, including the intelligence architecture. As units redeployed, returned to garrisons in theater, or settled into temporary stationing, the intelligence architecture returned to a smaller, more fixed footprint. The post conflict architecture adjusted to the new points of presence as part of the CCMD architecture. Several national intelligence agencies established temporary task forces during the conflict. Other Army analytic centers provided reach support. These centers will remain in the architecture until their parent disconnects them.

b. Re-establish authorities and permissions. Certain partner authorities during conflict will return to pre-conflict status. Other authorities may change due to partner performance during the conflict. New partners provide proximate access to formerly denied areas. As U.S. national agencies evaluate partner performance and reliability during the conflict, they may adjust (increase or restrict) sharing agreements. U.S. national agencies eased certain authorities during conflict, and these may return to pre-conflict procedures, specifically access to NSANet.

c. Continue access to theater collection and databases. The ACE chief was concerned with the enormity of updating databases to reflect conflict outcome. Working with the USAR TSB and other CONUS-based, regionally aligned analytic centers, the ACE chief established a federated production plan to share production tasks, reduce redundant effort, and speed up currency of foundational knowledge. All collection requests supporting database update came through the theater ACE for prioritization.

F-3. Prepare analytically

a. Conduct IPB. As operational planning begins at conflict termination, so does IPB. Post conflict IPB will identify information gaps and drive information collection to monitor the peace and re-establish the foundational databases. The G-2 planner is working support for the many G-3 post conflict contingencies.

b. Reset indicators to support warning intelligence. Return to competition is a very fluid time for warning intelligence. Initially, warnings sets focus on hostility resumption and other regional players that may want to take advantage of the new environment. Criminal activity and trans-national organizations will seek opportunities in the region. Host governments will need to ensure their integrity. As the environment stabilizes, so will warning sets. Indicators will rely on a rebuilt foundational knowledge of regional players.

c. Conduct robust operational assessment. The ACE must reset the foundational baseline of capabilities and infrastructure for all affected parties of the recent conflict. Damaged infrastructure, particularly along major lines of communication, impact future operational planning. The U.S. State department is also interested in potential aid packages. Adjusting regional player order of battle is a priority task. Resets of political and economic status will impact recovery efforts. Rebuilding EOB is important for current intelligence collection and future planning.

d. Analyze high volume data. To reestablish the theater database, the ACE must manage the vast amount of data collected during the conflict and determining its relevance. Post conflict collection will continue to populate databases as the ACE rebuilds foundational data and monitors the conditions of conflict resolution.

e. Conduct OSINT activities. The MIB (T) OSINT section detected a surge of new and contradictory PAI as civilian communications infrastructure recovered for the conflict. Rumors dominated social media and press reporting lacked the verification standards of pre-conflict reporting. The OSINT section requested CI support to screen additional local hires to translate media reporting. The OSINT section provided tailored reporting to civil affairs units in response

to stability-related RFIs. The section read daily U.S. embassy reporting to confirm or deny public sentiment as it relates to the official U.S. government position.

F-4. Conduct information collection

a. Continue reconnaissance and surveillance in all domains. Maneuver formations begin consolidating gains after achieving a minimum level of control and large scale combat has ceased. As freedom of movement increases, awareness of local activity increases as affected areas return to a state of normalcy. Reconnaissance of infrastructure, rule of law, and capacity of services all impact return to normalcy. Intelligence collection platforms confirm conflict resolution terms and conduct detailed damage assessments. Conflict cessation somewhat restricts aerial collection as civilian air traffic resumes in the joint operating area.

b. Converge national, theater, and organic collection. Cessation of large scale combat resets priorities for national systems and CONUS forces will begin redeployment. U.S. national agencies developed purpose built collection systems to monitor conflict resolution terms, and those sensors are incorporated into collection planning and the intelligence architecture. Theater collection refocuses over time to combatant commander's daily operational requirements. As priorities adjust, the ASCC G-2 adjusted collection taskings to the MIB (T) to balance national, theater, and partner collection.

c. Conduct CI. CI continues its support to protection, including stationing, redeployment, and monitoring conditions of conflict resolution. Liaison with host nation law enforcement and security elements remains key as does liaison with non-DOD U.S. agencies operating in theater. Instability in the former joint operating area is of particular interest as it serves as a breeding ground for foreign intelligence entities. CI, along with HUMINT, and civil affairs forces, focus on factors that could lead to a return to conflict.

Appendix G
Implications of the Five Multi-Domain Problems

G-1. How does the Joint Force compete to enable the defeat of an adversary's operations to destabilize the region, deter the escalation of violence, and should violence escalate, enable a rapid transition to armed conflict?

a. Setting the theater during competition is critical to success during competition and transition to conflict if the need arises. For the IC, competition is a period of intense assessment and preparation supporting combatant commander priorities. Extensive preparation prevents cold starts and could prevent conflict altogether. Setting the theater involves intelligence architecture, building theater knowledge, warnings intelligence, supporting operations into theater including nonlethal operations, and protecting the force through CI.

b. Establishing the intelligence architecture is fundamental to setting the theater for intelligence. All available information collection must be connected to the PED, analysis, and decision-making capabilities of the theater. Intelligence architecture requires interoperability, security, policies, and procedures. The intelligence architecture and knowledge management enable intelligence

reach, collaborative analysis, data storage, processing, analysis, and intelligence production between theater and other forces. Architectures incorporate different intelligence partners in each operational circumstance. The ASCC G-2, in coordination with the G-3 and G-6, establishes the architecture and the MIB (T) implements and executes the plan.

c. Building theater knowledge establishes a baseline of threat and environmental factors that could impact competition or armed conflict military operations. During competition, intelligence forces build a robust knowledge base to prepare for contingencies and engagement and to prevent cold starts. To protect U.S. interests abroad, Army forces as part of a whole-of government approach understand the complex nature of the world and the potential ramifications of a given situation. OSINT and cooperation with commercial industry contribute significantly to building knowledge. Conventional and ARSOF teams that rotate through a region gain valuable insights, but must be interviewed methodically to capture insights. This is a collection management problem. Intelligence helps the force understand peoples and cultures as well as the military aspects of the operating environment.

d. Competition activities include building capability and capacity to gain and maintain operational advantage. Intelligence must support the range of activities from engagement to flexible deterrent options. U.S. forces travelling into a region must prepare for potential threats. Teams must prepare for public health challenges, cultural differences, and language issues. Engagement strengthens partners and builds knowledge of infrastructure and regional forces and other actors. INSCOM's Project Foundry provides target area immersion training to enhance the MI technical skills for designated Soldiers assigned to tactical units prior to deployment. INSCOM fields and trains personnel on purpose-built MASINT and SIGINT sensors for use in the area of responsibility. INSCOM manages the DOD contract linguist program. The ASCC G-2 must oversee all activity in the region to influence preparation, provide overwatch, and satisfy information gaps.

e. MI provides CI support to competition activities and to transition to conflict. The MIB (T), in coordination with the protection cell and civil affairs forces, coordinates with local authorities to protect forward postured forces and nodes critical to expanding the force presence. MIBs (T) conduct CI scope polygraphs, technical support countermeasures, and screening activities in support of Army units.

G-2. How does the Joint Force penetrate enemy A2 and AD systems throughout the depth of the support areas to enable strategic and operational maneuver?

a. The Joint Force targets enemy long range systems beginning with forward presence forces operating across all domains, the EMS, and the information environment. Connecting intelligence capabilities to decision makers supports this effort.

b. Deep sensing of long range systems. Joint and national capabilities have long been able to sense deep selectively. They primarily support the combatant commander and national decision makers while Army commanders compete for these scarce resources. Adding high altitude and increasing access and responsiveness of low earth orbit surveillance to the Army inventory will dedicate resources to the Army commander's priorities. A scalable ground station assigned at

echelon from BCT through theater army will deliver collection results of Army, joint, and national assets. Forward presence of these capabilities allows the Joint Force to immediately contest enemy actions.

c. Common standards and interoperability facilitate data management. Common data standards allow for ground stations that receive data from multiple collection platforms. Common standards facilitate expeditionary capability integration. Common standards extends to fires and C2 systems to seamlessly link sensors to shooters.

d. The Joint Force needs common situational awareness across the force. Forward presence and expeditionary forces must have a common awareness across all domains, the EMS, and the information environment. Expeditionary forces require awareness during inter and intra theater movement.

G-3. How does the Joint Force dis-integrate enemy A2 and AD systems in the deep areas to enable operational and tactical maneuver?

a. The Joint Force defeats the enemy A2AD systems through cross domain fires directed at long range and mid-range systems.

b. Army high altitude and low earth orbit systems, complemented by joint and national collection support the targeting of enemy long and mid-range fires systems. These systems also find the enemy's maneuver formations before they can arrive at a position of relative advantage. As deeper targets are neutralized, these systems move to enemy mid-range systems and activities.

c. A ground station connected to fires and C2 networks reports collection for decisive action.

G-4. How does the Joint Force exploit the resulting freedom of maneuver to achieve operational and strategic objectives through the defeat of the enemy in the close and deep maneuver areas?

a. Army intelligence must continue the all domain information collection and reporting of that collection to appropriate decision makers.

b. After dis-integrating the enemy anti-access network, information collection systems proliferate across all domains with relevant collection. Layering more vulnerable and shorter range systems supports close and deep maneuver as deep collection continues. All collection must be available to decision makers.

c. Although not unique to supporting maneuver, integration of EW and CO with information collection exploits weaknesses in the enemy's C2 system. Integrating intelligence, EW, and cyberspace capabilities enable the Joint Force commander to exploit the EMS and compete in the information environment.

G-5. How does the Joint Force re-compete to consolidate gains and produce sustainable outcomes, set conditions for long-term deterrence, and adapt to the new security environment?

a. Consolidating gains in a new security environment involves more than returning to competition. Partner relationships and warning intelligence will be different after conflict and the competition points of presence will be different after a conflict.

b. After conflict the theater will reset. The architecture must include new security partners and collection means left behind to monitor the terms of the new security environment. As part of this reset, theater intelligence must understand the conditions of the new normal and what triggers may change that normality. The MIB (T) must update databases of forces, warning intelligence indicators, facilities, and other environmental factors. Information collection must confirm conditions of conflict termination and monitor new warning indicators.

c. The new security environment requires new protection measures to include CI. MIB (T) CI elements must reestablish host nation liaison and adjust critical infrastructure assessments. CI elements must work with other protection forces to sustain the new security environment.

Appendix H
Materiel Solutions

The Army will field four new systems to support the MDO AimPoint Force by 2028 and the MDO AimPoint Force 2035 by 2035.

H-1. Multi-Domain Sensing System (MDSS)

a. 2028 MDO AimPoint Force. MDSS will deliver the right information at the right time to the right decision makers as a critical enabler for LRPF, EW, cyber effects, and C2 functions. MDSS will provide commanders with an agile, interoperable and self-healing network of highly relevant and integrated systems from the support areas through the deep fires area, and from low altitude to space. MDSS-1000, a high altitude collection capability, is an initial capability under the MDSS umbrella. In order to do so, MDSS must develop, and where available leverage, the following foundational and inter-related capabilities.[69]

(1) MDSS will include a flexible mix of new and existing platforms operating from low altitude to space.

(2) Sensors will collect, process, correlate, attribute, and analyze modern emissions and signatures through the depth of the battlefield and inform multiple networks in near real time.

(3) MDSS will use quantum communication and information technology, AI, and other autonomous solutions to rapidly ingest, sort, process and archive data at speeds and measures of performance far beyond human capacity.

b. Schedule. The Joint Requirements Oversight Council validated and the Army approved the MDSS Initial Capabilities Document. The MDSS-1000 capabilities development document (CDD) is scheduled for completion in FY 2020 and focuses on a survivable and attritable capability in the high-altitude domain. The Guardrail Common Sensor, a current, medium altitude platform, reaches end of useful life in 2025. The Guardrail capability may merge into the Enhanced Medium Altitude Reconnaissance and Surveillance System (EMARSS) or the Army will replace it with a future AISR platform. MDSS prototyping is expected from FY 2022 through FY 2023 with fielding from FY 2024 through FY 2028.

c. MDO AimPoint Force 2035. In 2028 MDSS will include a host of platform and sensor packages aimed at addressing intelligence requirements in MDO. Examples may include: low and medium altitude systems such as the EMARSS and Airborne Reconnaissance Low - Enhanced, high altitude unmanned capabilities that may include balloons, airships, or fixed wing platforms. Current S&T initiatives listed in the below sub-paragraphs may inform or improve these systems for the MDO AimPoint Force 2035. Descriptions are available in Appendix I.

- Defense Advanced Research Projects Agency (DARPA) Converged Collaboration Elements for RF Task Operations (CONCERTO)
- Extensible PED (ExPED)
- Stand-in Passive Collection, Targeting and Exploitation Radar (SPECTER) (collaborative ISR sensors)
- Synchronizing High OPTEMPO Targeting (SHOT)
- Airborne Radar for Counter-Concealment Moving Target Indicator (MTI) (ARCM)
- Multi-threat IR/RF Advanced Generic Effects (MIRAGE)
- Reconfigurable Aperture for Precision Targeting Radar (RAPTR)
- Scalable Multi-function Adaptive RF Technologies (SMART)
- DARPA Mosaic warfare program (kill webs vs. kill chains) *Possible

H-2. Terrestrial Layer System (TLS)

a. 2028 MDO AimPoint Force. TLS will provide rapid employment of an operationally tailored, multi-intelligence and multi-functional suite of capabilities to austere locations to provide early warning, identify opportunities, and optimize maneuver. TLS configurations will include mounted, dismounted, and tethered versions to provide tailored support to maneuver forces at BCT and a version for echelons above brigade. It will provide on the move, close access collection from multiple intelligence disciplines, improved timeliness, and persistence; complement aerial and space layer collection capabilities or operate independently from the enterprise when disconnected; and provide intelligence support to CO.[70] TLS will deliver the following capabilities in a DIL environment:[71]

(1) TLS will provide close access tactical collection and delivery of cyberspace effects remotely or locally.

(2) TLS will collect and exploit legacy, modern, and emerging signal types.

(3) TLS will provide an all-weather, terrestrial-layer, SIGINT/EW/CO collection capability.

(4) TLS will provide advanced data pre-processing and resilient data interface to data stores.

b. Schedule. After joint requirements oversite council validation, TRADOC approved the TLS initial capabilities document (ICD) on 22 Feb 2018. TLS will support commanders BCT and above and is scheduled for a capability development document in FY 2020. The Army Requirements Oversight Council approved the Army-CDD for prototype during 2^{d} quarter FY 2020. TLS prototyping is scheduled through the end of FY 2020 with fielding scheduled to occur from 4th quarter FY2022 through 4th quarter FY2032.

c. MDO AimPoint Force 2035. In 2028, TLS will have replaced most Prophet systems and other programs in the Army inventory. Current S&T initiatives listed in the below sub-paragraphs may inform or improve these systems for the MDO AimPoint Force 2035. Descriptions are available in Appendix I.

- SPECTER
- ExPED
- SHOT
- Advanced Intelligence Services (AIS)
- Data Analytics to Identify and Correlate Events (DICE)
- Rainmaker Data Fabric (RDF)
- Ensemble Analytic Generation for Effective Response (EAGER) *Possible
- Multi-intelligence modernization supporting multifunction operations (MIMFO) *Possible
- Electronic warfare maneuver operations (EMO) *Possible
- Mosaic warfare program (kill webs vs. kill chains) (DARPA) *Possible

H-3. Tactical Intelligence Targeting Access Node (TITAN)

a. 2028 MDO AimPoint Force. TITAN will provide a scalable and expeditionary intelligence ground station that supports commanders across the entire MDO battlefield framework with capabilities tailored to echelon. TITAN leverages space and high altitude, aerial and terrestrial layer sensors to provide target nominations directly to fires information systems as well as multi-discipline intelligence support to targeting and situational understanding in support of the commander's overall operations process. The expeditionary and mobile ground station enables cross-domain fires with AI shortened kill-chains and provides assured access to current and future national, commercial and Army space-based assets as well as ground based and aerial sensors to include high altitude platforms. The TITAN family of systems will consist of common hardware and software architectures, improved interoperability, cost savings opportunities, a smaller hardware footprint, and a more consistent user experience across all echelons.[72] TITAN will deliver the following capabilities:[73]

(1) TITAN will analyze, produce, and disseminate intelligence and non-intelligence sensor data, aided by AI, to support targeting and situational awareness.

(2) TITAN will provide automated ingest, integration, data and intelligence exchange capability from and transmit data to national, joint, Army, mission partner, and commercial tactical space, high altitude, aerial, and terrestrial sensors.

(3) TITAN will communicate simultaneously with multiple ISR platforms, broadcast systems, ground stations, and commercial systems.

b. Schedule. TITAN is using operational needs statements from USAREUR and USARPAC, the MDSS and TLIS ICDs, and the Tactical Exploitation of National Capabilities General Officer Steering Committee to inform an Army CDD. Prototyping is expected from FY 2021 through FY 2022 with fielding from FY 2023 through FY 2024.

c. MDO AimPoint Force 2035. By 2028, TITAN will have replaced the TGS, Operational Intelligence Ground Station (OGS), Remote Ground Terminal, and the Advanced Miniaturized Data Acquisition System Dissemination Vehicle (ADV) in Army formations.[74] Current S&T initiatives listed in the below sub-paragraphs may inform or improve these systems for the MDO AimPoint Force 2035. Descriptions are available in Appendix I.

- SPECTER
- SMART
- Combat Operations Battlefield Radar (COBRA)
- Mosaic warfare program (kill webs vs. kill chains) (DARPA) *Possible
- Foresight and Understanding from Scientific Exposition (FUSE)
- Naval Integrated Fires Element (NIFE)
- System of systems (SoS) Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES)
- SHOT

H-4. Future intelligence analytics interface replacing DCGS-A

a. 2028 MDO AimPoint Force. A future intelligence analytics interface will provide fully interoperable all-source and single source support to targeting and situational understanding. Intelligence apps and tools will reside on the command post CE. Data will reside in a cloud framework with three data centers augmented by deployable edge nodes for redundancy and operations in a DIL environment. The battalion solution will support maneuver commanders in a DIL environment with appropriate all-source tools on a reduced footprint. Key developments include:

(1) Provide a data fabric solution that will provide an accessible centralized data repository containing diverse data sets and formats.

(2) Provide a data infrastructure tailorable to any organization at any echelon to meet their targeting and situational understanding needs.

(3) Provide data analytics that provide data integrity, standardization, correlation, geolocation refinement, predictive, and pattern analysis.

(4) Ingest data from legacy and future sources, support reach operations, and can operate in a stand-alone configuration when needed.

(5) Support single discipline exploitation and analysis to support targeting and inform all source analysis.

b. Schedule. DCGS-A operates on an approved information system capability development document. Beginning FY 2023 future intelligence analytics interface solutions will incorporate into the command post CE with cloud infrastructure support providing data management, big-data analytics, robotic process automation, and AI.

c. MDO AimPoint Force 2035. By 2028, an intelligence analytics interface will provide enhanced capabilities from battalion through theater. Current S&T initiatives listed in the below sub-paragraphs may inform or improve these systems for the MDO AimPoint Force 2035. Descriptions are available in Appendix I.

- RDF
- ExPED
- SHOT
- DICE
- Adapting Cross-domain Kill Webs (ACK)
- Collection and Monitoring via Planning for Active Situational Scenarios (COMPASS)
- AIS
- Geospatial Research Lab Initiative/Enhanced Terrain Processing Toolkit (GRLI/ETPT)
- Mosaic warfare program (kill webs vs. kill chains) (DARPA) *Possible
- STITCHES

Appendix I
System and Technology Descriptions

I-1. Current and projected systems.

These are descriptions of current systems or systems expected to be operational by 2028. **Projected systems are in bold.**

a. Advanced Miniaturized Data Acquisition System (AMDAS) Dissemination Vehicle (ADV). ADV provides deployed warfighters at corps an assured access and processing capability of national level sensor data. The ADV organic capabilities allow analysts to provide the commander with timely, accurate, predictive, and tailored intelligence. The ADV receives, processes, analyzes, and disseminates time dominant GEOINT.

b. Airborne Reconnaissance Low (ARL) Enhanced (ARL-E). The ARL-E is a worldwide, self-deployable AISR system which finds, identifies, tracks, and targets threat entities using EO/IR, dismount moving target indicator radar, long range radar, hyperspectral imagery, and communications intelligence (COMINT) sensors. ARL-E provides onboard collection, analysis, and sensor cross-cueing and real-time dissemination from DCGS-A workstations or a future intelligence analytics interface and provides network connectivity via common data link and Ku/KA beyond line of sight links.

c. **Biometric Enabling Capability Increment 1 (BEC 1)**. The BEC 1 will enhance the DOD automated biometric information system v1.3 and provide DOD and U.S. Government (USG) agencies, and international partners with an authoritative biometrics source that receives multi-modal biometric submissions on adversarial and neutral or unknown individuals to include fingerprints, iris, palm prints, latent fingerprints, facial images, voice, and associated contextual data. The BEC 1, will match biometric data against its authoritative DOD source and submit biometrics to additional other government agency authoritative sources as required to positively identify an individual. The BEC Inc 1 will also provide any associated DOD biometric enabled watchlist match or no match response back to inform decide and act activities. The BEC Inc 1 will provide an integrated web-based interface, cross domain capability, interoperability between DOD and USG biometric data sources to identify threat actors and promote better situational understanding.

d. **CI and HUMINT Equipment Program-Army (CIHEP-A)**. CIHEP-A replaces the CI and HUMINT Automated Reporting and Collection System (CHARCS) which is in sustainment until 2025. CIHEP-A is a scalable and modular equipping program which includes credibility assessment tools; tagging, tracking, and locating capabilities; still photo and video capture; media and document exploitation; language translation; and will leverage biometrics and forensics tools from complementary programs.[75]

e. DCGS-A and the **future intelligence analytics interface**. DCGS-A is a 'system of systems' that includes fixed sites, deployable ground stations, and servers and laptops that provides ~60 intelligence analysis tools and access to ~700 data sources, which deliver actionable information to warfighting commanders. DCGS-A provides a common platform link to DOD and intelligence agencies. It is interoperable with DCGS-A fixed, mobile, and embedded systems, C2 information systems, and selected joint C4ISR systems and sensors. It introduces the IC widget framework, provides a suite of core PED applications, provides the abilities to evaluate technical data and information, and provides a robust multi-intelligence database management and replication capability.

(1) CD1. The DCGS-A Bn Solution is designed to replace the current DCGS-A baseline system at the battalion (a server and two workstations) with a two or three workstation suite. CD1 provides support to MDMP, refines threat common operational picture, receives warnings, provides intelligence support to targeting, manages data, and exchanges data with C2 information systems. These workstations will enable the Bn S2 to operate in a DIL environment, discover data, and permit users to maintain the workstation and its network connectivity without maintainers.

(2) CD2. CD2 transforms and organizes data management and applies advanced analytics which are accessible regardless of unit, echelon, or location to enable C2. CD2 assures access to tactical, joint, or national data sources and reduces the analytical burden through a common intelligence picture, seamless transitions from the strategic support area into a theater, and the ability to operate in a DIL environment. CD2 integrates intelligence into the command post CE in the mission partner environment. The Army will equip the first unit by the end of FY 20.

(3) Intelligence applications. Intelligence applications will insert as software into the command post computing environment to enhance all source intelligence, PED, CI, HUMINT,

SIGINT, and GEOINT capabilities from the tactical to the strategic level. This will enable a gradual reduction of legacy DCGS-A hardware and software through 2026, mitigating any loss of capability as DCGS-A phases out of the inventory. These applications will leverage AI tools and advanced fusion software to automatically fuse sensor data with terrain, weather, and threat to identify patterns and support predictive intelligence. Subsequent application drops will include improved all source intelligence, weather services, collection management, and intelligence support to targeting applications.

(4) Three primary future S&T challenges face DCGS-A as it evolves into a future intelligence analytics interface that Army MI must address:[76]

(a) HMI will be the user interface that connects an operator to the controller for an industrial system. Possible HMI are dependent primarily on interface devices; interfaces involved can include motion sensors, keyboards, input pads, speech-recognition interfaces and modalities of interaction in which information is exchanged using sight, sound, heat, and other cognitive and physical modes enabling HMI. Possible uses are optical interaction to select and/or track entities on a display, interactive optical display glasses, contact lenses, interactive holographic display, and interactive mixed reality.

(b) ML used as a method to devise complex models and algorithms that lend themselves to predictive analysis. Continued S&T development is required to mature the technology and provide the volume of curated data to the point of practical utility for intelligence analysis and predictive modeling. ML would be utilized across the foundation layer from the analyst work station at the company or battalion, to the data warehouse capabilities at the ASCC. ML would greatly improve analytic capacity, quickly identifying patterns and trends, enabling much more rapid situational understanding and targeting.

(c) Qubits, unlike classical computers that encode information in bits, operates in a state of superposition where each qubit can represent both a 1 and 0 at the same time and entanglement where qubits in superposition can be correlated with each other (the state of a qubit whether it is a 1 or a 0 can depend on the state of the other). Quantum computing will have the potential to increase situational understanding, situational awareness, knowledge management, and decision making for commanders and staffs by enabling ultra-efficient data processing to untangle the data complexities of future environments (MDO and dense urban environment).

f. Enhanced Medium Altitude Reconnaissance and Surveillance System (EMARSS). EMARSS is a worldwide self-deployable AISR system which finds, identifies, tracks, and targets threat entities and individuals using a mix of EO/IR, COMINT, radar, light detection and ranging (LiDAR), and wide area motion imagery (WAMI) sensors. It is capable of cross-cueing on and off-board sensors within the defense intelligence information enterprise.

g. Gray Eagle. Gray Eagle is a long endurance, persistent AISR system which provides EO/IR, SAR/MTI, and potentially COMINT support directly to tactical commanders across the full range of military operations. Gray Eagle provides the AIB with a responsive, agile, and flexible capability to perform ISR, shaping, setting of conditions, targeting, and attack throughout the area of operations.

h. Guardrail Common Sensor (GRCS). GRCS is an AISR system which finds, identifies, tracks, and targets threat entities using stand-off or close-in COMINT and ELINT intercept with direction finding and cooperative precision geolocation. GRCS conducts cooperative operations with national and joint sensors via theater net-centric geolocation (TNG). GRCS is scheduled to be out of the Army inventory by 2025.

i. **Identity Intelligence Analytic Resource (I2AR)**. I2AR provides intelligence analysts and operators with a centralized capability to perform all-source biometrically-enabled identity analysis, linking, U.S. persons quarantine and management, watchlist management, and product authoring at the Secret level. I2AR is an information aggregator, authoring tool and publisher focused on augmenting analysts' ability to exploit data from disparate sources including contextual data from the Biometrics Automated Toolkit together with over 40 different sensors in order to create a unified view or person of interest.

j. **Intelligence Collection Exploitation Toolkit (ICE-T).** ICE-T integrates a common suite of commercial off the shelf hardware and software components able to provide Army military police, intelligence and maneuver elements with combat proven capabilities to develop actionable information or warning intelligence on or near an objective, in both permissive and non-permissive environments. ICE-T enables collecting, processing, and exploiting unique sources of information derived from captured materials and captured enemy documents and media on or near an objective; documenting collected materials; collecting forensic materials; associating people, objects, events and locations; and support identity actions against actors, entities or forces.[77]

k. Modular Communications Node-Advanced Enclave (MCN-AE). MCN-AE is a commercial off the shelf, small and lightweight expeditionary enclave that provides TS/SCI access to both TROJAN Data Networks 2 and 3, with tunneling reach-back over the tactical network backbone to the TROJAN Network Control Center Enhanced Gateway.[78]

l. **Multi-Domain Sensing System (MDSS)**. MDSS provides extended endurance over wide areas to counter A2AD and DIL environments. MDSS supports deep fires over denied airspace providing precision target location in fluid environments. The High Altitude Detection Exploitation System, the next generation medium altitude collection platform, is the first instantiation of MDSS. The second instantiation, the MDSS-1000 system, consists of 24 pairings of sensors and platforms. Sensors include ELINT, COMINT, SAR/MTI, potentially WAMI, EO/IR, EW, and could include other purpose built sensors. One MDSS-1000 system is planned for USAREUR (providing initial operational capability in 2023) and a second system is planned for USARPAC (providing full operational capability in 2026). Three primary future S&T challenges facing MDSS that Army MI must address:[79]

(1) Real time measurement of stratospheric winds in support of mission planning and mission execution (navigation).

(2) Lift gas (helium or hydrogen) supplies in an expeditionary environment.

(3) Precision recovery of payloads to include maritime recovery which enables refurbishment and reuse of payloads.

m. **NXGBCC**. NXGBCC replaces the Biometric Automated Toolset – Army which is in sustainment until 2022. NXGBCC is a forward biometrics collection and matching system. The system is designed to support access control, identify persons of interest, and provide biometric identities to detainee and intelligence systems. NXGBCC collects, matches, and stores biometric identities and is comprised of three components: a mobile collection kit, static collection kit, and a local trusted source. The local trusted source provides an additional analysis capability to assist in decide and act activities. NXGBCC is an integrated system of commercial-off-the-shelf hardware and software to ensure the end-to-end data flow required to support different technical landscapes during multiple types of operational missions. To support these operational missions, NXGBCC will be capable of operating on both organic and non-organic infrastructures to support varying technical and communication environments, and be capable of achieving efficient, three minutes or less identity match times and data updating. [80]

n. Operational Intelligence Ground Station (OGS) (AN/TQ-224B). The OGS provides a common, centralized PED capability for multi-intelligence airborne sensors on the DCGS-A enterprise. OGS provides Army aerial and national SIGINT, national and theater imagery intelligence (IMINT), and full UAS interoperability supporting corps and AEBs.

o. Prophet POR B (An.MLQ-44B v1). Prophet provides dedicated, all weather, 24/7, ground-based tactical SIGINT from fixed-site, mobile, and man-pack configurations. Prophet connects the BCT to the intelligence enterprise as a node for TNG, leveraging joint and national sensors and extending the range of SIGINT collection well beyond the organic capability. Prophet accepts technology insertion capabilities to provide intelligence support to CO. TLS will eventually replace Prophet throughout the force.

p. **Terrestrial Layer System (TLS)**. TLS is a terrestrial, globally deployable, integrated SIGINT, EW, and CO enabled system with capabilities to detect, identify, locate, exploit, deny, and disrupt communications and non-communications systems in support of the BCT commander. TLS enables EA, ES, direction finding, RF-enabled CO, SIGINT terminal guidance, SIGINT survey, and TNG. TLS will prosecute modern peer, and below-peer signal sets, support counter-UAS, EW effects, and CO. TLS modernizes the terrestrial layer providing a capability to digitally interface directly with brigade, division, corps, army and joint collection and analysis elements and with C2 systems. Three primary future challenges facing TLS that Army MI must address:[81]

(1) The ability to collect and exploit ELINT data from a terrestrial location.

(2) The ability to collect and exploit SIGINT data from greater distances than can be done today. The Army will develop the TLS EAB to satisfy division and corps terrestrial sensing requirements.

(3) The ability to communicate with the global SIGINT enterprise to transmit intelligence data and to use tools and applications that are available on the global SIGINT enterprise.

q. Tactical Intelligence Ground Station (TGS). TGS provides the commander with near real time feeds for MTI, weather, full motion video, and EO/IR. It receives direct feeds from unmanned aerial system EO/IR and MTI sensors, joint surveillance target attack radar system, integrated broadcast service, and global broadcast service. The TGS retains the capability of operations on-the-move (OTM). TGS is fielded to BCT, division, corps, and E-MIB battalions.

r. **Tactical Intelligence Targeting Access Node (TITAN).** TITAN is a family of next generation mobile ground stations to support MDO and LRPF during large scale combat. TITAN will provide timely assured intelligence in support of LRPF and maneuver in connected, DIL, and A2AD environments. TITAN will ingest, process, fuse, disseminate, and store sensor data from joint, space, high altitude, aerial, or terrestrial assets supporting the tactical, operational, or strategic fight. Three primary future S&T challenges facing TITAN that Army MI must address:[82]

(1) Multi-link and multi-band antennas with the ability to combine antennas through unified RF capabilities, antennas that can support multi-common data links simultaneously, and multiple SATCOM links simultaneously. The main purpose behind this is to reduce the overall footprint of the systems integral to the ground station; reduce the burden on the soldiers; reduce size, weight, and power and reduce set-up/tear-down times.

(2) AI models with the ability to support targeting of specific target areas of interest and named areas of interest; automated methods of detecting, identifying and recognizing targets using various sensor data sets. AI models will need algorithms that assist in autonomous detection, identification, and recognition tasks and methods for training the AI algorithms for updated, variant and new targets. This includes ATR for electro-optical/infrared (EO/IR) imagery and SAR imagery and automated ways to correlate and fuse the data from multi-intelligence sources to refine the target location.

(3) Distributed data architecture C4ISR/EW Modular Open Suite of Standards (CMOSS) technology solutions is a set of standards that can support the reduction of the system size, weight, power and cost, reduce the system footprint, and the burden on the operator, and the use of CMOSS format transceiver cards to reduce the numbers of standalone radios.

I-2 Actionable technologies

These technologies may enhance current or future systems. Technologies listed in appendix H are **bolded**.

a. **Adapting Cross-domain Kill Webs (ACK).** ACK is a solution approach that allows commanders a quality of C2 known as "optionality" by connecting platforms having the timely means to either stimulate, see, or strike with each other in a virtual marketplace before the opportunity is no longer there. The kill web in essence hybridizes sensor-to-shooter, cross-domain fires, multi-domain warfare, and cross-domain warfare into one overlapping web of kinetic and non-kinetic effects reducing the time it takes to render the adversary defunct. Technology readiness level (TRL) 5

b. Anomaly Detection at Multiple Scales (ADaMS). ADaMS allows CI personnel at echelons corps and above to detect insider threats or potential traitors before the insider threat "turns," or

shortly after they turn, but before they cause serious harm to national and/or unit security. The algorithm detects when an individual strays from "need to know" by continuously monitoring DOD email, information system use logs, file accesses, and many other forms of cyberspace-observable behavioral data. TRL 4

c. Active Interpretation of Disparate Alternatives (AIDA). AIDA is a semantic engine that automatically generates multiple alternative analytic interpretations and multiple hypotheses of a threat situation based on multiple data sources, many of which are noisy, conflicting, or deceptive. TRL5

d. **Advanced Intelligence Services (AIS)** (AI enabled PED). AIS is a shared, unified, harmonized, and cross-functional semantic data framework with common, consistent indexing, data storage by modality, universal pedigree and provenance necessary for deep learning to enable visualization and analytic processes. TRL 6

e. **Airborne Radar for Counter-Concealment Moving Target Indicator** (MTI) **(ARCM).** ARCM is a technology with a specific set of algorithms for a fixed-wing aircraft counter-concealment and moving target indicator capability that will provide persistent surveillance denying adversaries the ability to maneuver and hide under foliage. TRL 6

f. All-Signal Tactical Real-Time Analyzer (ASTRAL). ASTRAL develops and demonstrates a hybrid analog, digital photonic, electronic processor demonstrating real-time nonlinear cyclo-stationary and convolutional processing and low-probability-of-intercept signal processing gain over input electromagnetic signals filling a bandwidth of 1 to 10 GHz. TRL 3

g. Blackjack. Blackjack demonstrates a distributed low earth orbit constellation that provides global persistent coverage with a total cost of ownership that is less than a single exquisite satellite. TRL 6

h. Big Open Source Social Science (BOSSS). BOSSS regularizes and automates social science analysis by exploiting open-source news and social media platforms. TRL 4

i. **Combat Operations Battlefield Radar (COBRA).** COBRA develops next generation radar technologies in support of a modular active protection suite that addresses simultaneous, hemispherical detection, identification and tracking of threats (direct fire, indirect fire, UASs) to ground combat vehicles while on the move. Resource management and processing algorithms support simultaneous detection, identification, tracking and point-of-origin location for an expanded and emerging list of threats. TRL 6

j. **Collection and Monitoring via Planning for Active Situational Scenarios (COMPASS).** COMPASS develops analytical tools and decision aids designed for competition operations. These tools will help commanders, staff, analysts understand and explain the enemy's use of information confrontation, misinformation, intimidation, pressure, and psychometrics to set advantageous conditions for enemy actions that are just short of war. TRL 5

k. **Converged Collaboration Elements for RF Task Operations (CONCERTO).** CONCERTO converges a RF system with radar and EW for UAS. CONCERTO will develop a converged RF system with radar, electronic warfare, and communications modes to enable new approaches to tactical RF missions. This will allow more capability on smaller UAS platforms, an RF virtual machine that supports portable RF modes, an intelligent system and sensor resource manager, and a unified and scalable design which allows dynamic maneuver in the EMS, time and space. TRL 5

l. DARPA long duration heavy-fueled UAS (Vanilla UAS). Vanilla UAS hosts the same payload weights and types as other group 3 UAS (Sperwer B, Shadow, Tiger Shark), but provides an extended (10-day vice several hour) endurance. Detection of low acoustic and visual signatures allows close-in collection and collection operations below the cloud deck even when the ceiling is low. System characteristics include a maximum collection altitude of 15,000 ft. above ground level, a payload of 40 lbs., a cruise speed of 75 knots, and a wingspan of 36 feet. TRL 5

m. DARPA Hedgehog and Distributed RF Analysis and Geolocation on Networked Systems (DRAGONS). Hedgehog (the receiver) replaces limited-band, limited function systems with a receiver that is small enough to mount on a group 1/2 UAS and capable of a wide operating range (10 MHz-4GHz) and operates over 16 channels with 10 microsecond hop rates. It provides both general processing unit and field programmable gate arrays integrated processing able to host modern AI-enabled applications such that a single platform can perform the functions of several radios, also enabled beamforming radar to reduce the probability that the enemy detects the Hedgehog user. This is networked with the DRAGONS standard RF heat map display to provide signal survey to include active internet of things device survey across a couple of square kilometers in support of TLS or a U.S. ARSOF element. It provides near real time situational understanding of threat and non-threat signals in a sector. It demonstrates cognitive radio low-energy signal analysis sensor integrated circuits, RadioMap, and Jackhammer on the receiver. TRL 5

n. Deep Exploration and Filtering of Text (DEFT). DEFT develops the ability to see through language to develop contextual meaning in text, (by using natural language processing), to make use of key information contained in text documents, to cue up information sources that contain new developments for analysts, and to automate the initial stages of report writing. TRL 4/5

o. **Data Analytics to Identify and Correlate Events (DICE).** DICE researches and develops algorithms and analytics that harvest, correlate, and exploit tactical RF receiver sources with new and emerging data sources to enhance the electromagnetic environment, EOB and cyberspace terrain picture. TRL 4

p. **Ensemble Analytic Generation for Effective Response (EAGER).** EAGER is an interactive HMI for a comprehensive red common operating picture that correlates sensor-receiver data, leveraging past and current micro-trends and EOB. TRL 4

q. **Electronic Warfare Maneuver Operations (EMO).** EMO allows EW technologies to sense, locate, and target A2AD systems allowing for continuous maneuver operations. TRL 6

r. Every Receiver a Sensor (ERASe). The ERASe program aims to broaden and deepen the Army's ability to sense the cyber-electromagnetic environment in a congested and contested theater of operations, allowing for the acquisition of relevant data and the subsequent processing and analytics necessary to achieve cyberspace situational understanding requirements and mitigate known capability gaps. TRL 6

s. **Extensible Processing Exploitation and Dissemination (ExPED).** ExPED provides advanced analytics for correlation and fusion of multi-intelligence data which enable distributed workflows, tailored by mission, sensors and available users. It provides scalable PED workflows that maximize the use of human and computing resources. ExPED applications are capable of operating at the sensor, at the ground station (i.e., TITAN), or within a larger data center such as the 116th AIB. TRL 6

t. Fast Short Tandem Repeat LL-30 DNA profiling system (FaSTR DNA). The system is able to collect, match, and associate DNA against known exploited multi-modal biometrics records on a DNA device. TRL 6

u. **Foresight and Understanding from Scientific Exposition (FUSE).** FUSE provides automated detection that aids in the systematic, continuous, and comprehensive assessment of scientific and technical development using information found in published scientific, technical, and patent literature by identifying and extracting observables from tens of millions of full-text documents in multiple languages. TRL 5

v. Gateway on the Move – Biometrics (GOTM-B). GOTM-B provides non-contact on-the-move multi-modal biometric, forensics, and threat detection for force protection and physical access control. TRL 6

w. **Geospatial Research Lab Initiative/Enhanced Terrain Processing Toolkit (GRLI/ETPT).** GRLI//ETPT will ingest and process the newest spatial and temporal high resolution 2 and 3 dimension sensor data. Uses Esri products for geospatial information system processing and analysis and Envi products for remote sensing image processing and hyperspectral remote sensing. TRL 5/6

x. GunSmoke. Gunsmoke is a mission partner program that provides the ability to look for low band transmissions on the earth. TRL 6/7

y. High altitude airship (HAA). HAA has a long-endurance mission capability at 65,000 ft. with multiple mission payloads to simultaneously address Army wide-area C4ISR and positioning, navigation, and timing (PNT) requirements. It is a force multiplier for dedicated, surge, and augmentation of C4ISR and PNT functions that reinforce MDO. When space-based assets become degraded or lost, the HAA can reconstitute communications, ISR, and PNT effects. The HAA's persistent stare can provide fires with greater opportunities for launch detection, tracking, BDA, and deep-strike targeting. The HAA is a recoverable, unmanned, solar-powered system with global reach. TRL 5

z. High altitude balloons (HAB). HAB is free-floating balloons that provide the commander with a semi-persistent, multi-functional capability that can include ISR, communications-relay, and data-exfiltration capabilities. TRL 6 (latex), TRL 8-9 (super pressure), TRL 6 (zero pressure)

aa. High altitude long endurance fixed wing UAS (HALE-FW). HALE-FW provides the capability to exercise C2 at all echelons in all conditions including denied and/or degraded conditions, such as disruptions to satellite, line-of-sight, and beyond-line of-site communications, and PNT data to C2 widely dispersed operations. TRL 6 (solar), TRL 3-4 (fueled)

ab. Highly distributed sensors (HDS) (aka unattended ground sensors (UGS) or Skittles). HDS are intended to be disposable, air, artillery, or ground deliverable to increase collection in A2AD areas. TRL 5

ac. Hierarchical Identify Verify Exploit (HIVE). HIVE creates a global analytics processor that achieves a 1000X improvement in processing efficiency, so that analysts will be able to discover relationships between threat entities and other entities in the OE via a tactical data fabric as opposed to relying on forensic analysis conducted at a large data center hours later. TRL 5

ad. LoneStar. Lonestar is a mission partner program that provides health and welfare of the global navigation satellite system. TRL 5

ae. Multi-spectral Advance Reconnaissance Video Imaging Notator (MARVIN). MARVIN provides the warfighter with new capabilities for real time threat material detection and identification at stand-off ranges. TRL 4/5

af. Multi-intelligence Modernization Combined Action (MIMCA). MIMCA develops algorithms and software that will coordinate EW, SIGINT, CO, and communications capabilities to ensure the optimal allocation of available resources for systems implementing CMOSS and sensor open systems architecture interfaces. TRL 6

ag. **Multi-intelligence Modernization Supporting Multi-function Operations (MIMFO).** MIMFO uses multiple sensors to detect, intercept, identify, locate, and localize other radiated electromagnetic energy sources to enable SIGINT and ES in coordination with EW and OCO. TRL 6

ah. **Multi-threat IR/RF Advanced Generic Effects (MIRAGE). MIRAGE** enables countermeasures against agile RF threats using tiered technologies for survivability that encompass passive and persistent, active and adaptive, active and indiscriminant technologies to defeat advanced EO and RF threats to aircraft. TRL 6

ai. **Mosaic warfare.** Mosaic warfare provides a strategic shift away from a tightly networked, centralized C2 infrastructure to an architecture that provides the ability to compress the time it takes to develop capabilities and enablers from years down to months, to configure system architectures at campaign speed, and ultimately to piece together new effects "on the fly" at mission speed with a cultural shift away from kill chains to dynamic all domain kill webs. TRL 4

aj. **Naval Integrated Fires Element (NIFE).** NIFE provides integrated fire control that will leverage networks, cyberspace, and space capabilities to enable the naval integrated fire control-counter air (NIFC-CA) effort. NIFC-CA provides the Navy with extended over-land and over-water engagement ranges, and extends the over the radar horizon on the firing surface ship. NIFC-CA is a program executive office Integrated Warfare Systems program and integrates the Navy's Aegis combat system, cooperative engagement capability, SM-6, and E-2D aircraft.

ak. Sentient. Sentient automates the coordination of tipping and cueing for multiple platforms at machine speed allowing for targeting and mensuration previously done by human analysts. It transforms intelligence synchronization, collection management, tasking, collecting, and PED from largely stove-piped and human-driven processes to an enterprise orchestrated and largely automated process enabled by AI and multi-sensor data fusion technologies. The Sentient interface helps collection managers with problem decomposition, pertinent collection strategies, sensor tasking, multi-intelligence data fusion of collection, and ultimately analytics for object detection, threat behavior recognition, and anomaly detection. TRL 9

al. Near Real Time Identity Operations (NRTIO). NRTIO provides near real time identity response with less than three minutes response time for biometric matching. TRL 7

am. Offensive cyberspace operations (OCO) Mirror. OCO Mirror provides the Army the necessary capabilities to arm cyber mission forces, and cyberspace electromagnetic activities support to corps and below, with the offensive capabilities they will require to dominate within the cyberspace domain and keep abreast with adversary technological advancements. TRL 6

an. Psychometrics. Psychometrics collect data about personnel and organizations from daily social media, expose the data to ML algorithms to discern exploitable weaknesses, and then design information confrontation campaigns for a specific purpose. This is a convergence of the cognitive, physical, and digital dimensions. TRL 3

ao. **Reconfigurable Aperture for Precision Targeting Radar (RAPTR).** RAPTR is a next generation reconfigurable antenna designed to enable highly-interpretable imagery and precision targeting functionality in Army ISR radars. It provides detection and tracking performance well beyond current AN/ZPY-1 (STARLite) and AN/ZPY-5 (VaDER). TRL 6

ap. **Rainmaker Data Fabric (RDF).** RDF is a scalable data fabric that enables a unified data architecture that scales across multiple echelons and the different states of the network. It coordinates data transport, mobility, data storage, and computing power that exist from echelons above corps down to maneuver and fires battalions. RDF will reduce network load requirements, integrate disparate data silos, improve analytical accuracy, enrich data, and reduce data access time. RDF manages all data types (structured, unstructured, tables, streams, or files) from any source. RDF enables data created in different warfighting functions to be used immediately by information and/or weapons systems resident in any other warfighting function. Operationally, RDF enables multi-domain kill webs to drive operations at the speeds imagined when robotic and autonomous systems, hypersonic missiles, and AI/ML-enabled decision tools will be present on the battlefield in a fight versus a peer enemy. TRL 6

aq. **Synchronizing High OPTEMPO Targeting (SHOT).** SHOT enables data aggregation at speeds necessary to shorten the kill chain, which is particularly important to operational or strategic fires. SHOT also shortens fires coordination, thus further shortening the kill chain from initial sensing to steel on target. TRL 5/6

ar. Simultaneous Countermeasures for Active Reconnaissance and Surveillance (SCARS) (also known as intelligence support to military deception). SCARS will develop and demonstrate advanced offensive EW technologies that deceive or create uncertainty in adversary active sensing systems to create windows of superiority for blue forces in A2AD environments. It employs AI-tailored and coordinated false signals across the EMS to confuse the enemy just long enough to allow the Joint Force to effect the desired stimulate, see, and strike action. TRL 5/6

as. **Scalable Multi-function Adaptive RF Technologies (SMART).** SMART investigates solutions that expand multi-function capabilities in current and future RF systems, including air and ground passive and active radar, EW and SIGINT technologies to develop sensors that are more survivable, less redundant and are more cost effective for the host platforms. TRL 5

at. **Stand-in Passive Collection, Targeting and Exploitation Radar** (**SPECTER)** (collaborative ISR sensors). SPECTER provides the ability to perform stand-in cooperative sensing and will allow increased airborne ISR stand-off and survivability via sensor teaming. It will design and demonstrate technologies to enable the teaming of airborne and ground based radar systems to enable enhanced survivability and increased target detection performance. It will investigate and design technologies to enable the teaming of ground and airborne radar systems with one or more forward on-the-move ground vehicles to enable enhanced survivability and increased target detection performance when operating near or beyond the forward line of troops. TRL 5

au. Stand-in Advanced Radio Frequency Effects (STARE) (formerly known as Robust Grey C3I). STARE is a research and development effort to develop a distributed, coordinated, networked EW capability using low-profile unattended systems and networks by leveraging existing DOD, internet of things, and civil infrastructure. STARE would provide the additional ability to identify and geo-locate targets to facilitate targeting and precision fires, enable discrete sensor deployment and data exfiltration to inform planning prior to mission operations, provide further shaping to tactical operational objectives through large scale distributed effects, EMS awareness, and planning. TRL 6

av. **SoS (system of systems) Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES).** STITCHES provides the ability to combine messages from multiple sources and to transmit data between ground stations, ATR software, and the APG-81 radar currently used on the F-35 to produce a comprehensive picture of the battlefield. STITCHES is a technology shift from local message standards and global open standards to the use of incremental standards allowing the ability to add new messages easily in a flexible architecture that is able to interoperate with legacy systems. It will be one of a few proposed SoSs within the larger concept of mosaic warfare.

aw. Social Understanding and Reasoning Framework (SURF). SURF exploits social media to identify persons of interest. It is currently installed on the Amazon commercial cloud services government cloud for the IC. TRL 4

ax. Tethered UAS. Tethered UAS provides the armored BCT and Stryker BCT with the ability to integrate unmanned air platforms onto existing vehicles, allowing them to perform a number of missions that either ground vehicles, or free-flying unmanned aerial vehicles are unable to perform. TRL 9

ay. Voice Identity Biometrics Exploitation Services (VIBES). VIBES provides the ability to collect, match, and associate voice prints against known exploited multi-modal biometrics records at the regional forward server. TRL 7

az. Army Research Laboratory weather initiative (WI). WI will aid service components with weather effects planning. It has man portable LiDAR and radar tools that will collect weather data in the operational area, operating independently of networks. TRL 6

Glossary

Section I
Abbreviations

A2	anti access
AD	area denial
ACE	analysis control element
ACK	adapting cross-domain kill webs
ADA	air defense artillery
ADaMS	anomaly detection at multiple scales
ADP	Army doctrine publication
ADV	advanced miniaturized data acquisition system dissemination vehicle
AEB	aerial exploitation battalion
AI	artificial intelligence
AIB	aerial intelligence brigade
AIDA	active interpretation of disparate alternatives
AIS	advanced intelligence services
AISR	aerial intelligence, surveillance, and reconnaissance
AOC	Army operating concept
ARCM	airborne radar for counter-concealment MTI
ARL-E	airborne reconnaissance low - enhanced
ARNG	Army National Guard
ARSOF	Army special operations forces
ARSTRUC	Army structure
ASCC	Army service component command
ASTRAL	all-signal tactical real-time analyzer
BCT	brigade combat team

BDA	battle damage assessment
BEC	biometric enabling capability
Bn	battalion
BOSSS	big open source social science
BUR	bottom up review
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance, reconnaissance
CCD	camouflage, concealment, and deception
CCMD	combatant command
CD	capability drop
CDD	capabilities development document
CE	computing environment
CI	counterintelligence
CIHEP-A	counterintelligence and HUMINT equipment program-Army
CHARCS	CI and HUMINT automated reporting and collection system
CMOSS	C4ISR/EW modular open suite of standards
CO	cyberspace operations
COBRA	combat operations battlefield radar
COE	common operating environment
COMPASS	collection and monitoring via planning for active situational scenarios
COMINT	communications intelligence
CONCERTO	converged collaborative elements for RF task operations
CONOPS	concept of operations
CONUS	continental United States
CPCE	command post computing environment
DA	Department of the Army
DARPA	Defense Advanced Research Projects Agency
DCGS-A	distributed common ground system - Army
DEFT	deep exploration and filtering of text
DICE	data analytics to identify and correlate events
DIL	disconnected, intermittent, limited
DOD	Department of Defense
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policies
DRAGONS	distributed RF analysis and geolocation on networked systems
EA	electronic attack
EAB	echelons above brigade
EAGER	ensemble analytic generation for effective response
ELINT	electronic intelligence
EMARSS	enhanced medium altitude reconnaissance and surveillance system
EMO	electronic warfare maneuver operations
E-MIB	expeditionary military intelligence brigade
EOB	electronic order of battle
EO	electro optic
EO/IR	electro optic/infrared

ERASe	every receiver a sensor
ES	electronic support
EW	electronic warfare
ExPED	extensible PED
FaSTR DNA	fast short tandem repeat LL-30 DNA profiling system
FM	field manual
FUSE	foresight and understanding from scientific exposition
FY	fiscal year
GEOINT	geospatial intelligence
GIG	global information grid
GOTM-B	gatekeeper on the move-biometrics
GRCS	Guardrail Common Sensor
GRLI/ETPT	Geospatial Research Lab initiative/enhanced terrain processing toolkit
GS	general support
HAA	high altitude airship
HAB	high altitude balloon
HALE-FW	high altitude long endurance – fixed wing
HDS	highly distributed sensors
HIVE	hierarchical identify verify exploit
HMI	human machine interface
HUMINT	human intelligence
HQ	headquarters
HQDA	headquarters, Department of the Army
I2CEWS	intelligence, information, cyber, electronic warfare and space
IADS	integrated air defense system
IC	intelligence community
ICD	initial capabilities document
ICE-T	intelligence collection exploitation toolkit
IEW	intelligence electronic warfare
IMINT	imagery intelligence
INSCOM	U.S. Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
ISR TTX	intelligence, surveillance, and reconnaissance table top exercise
JADO	joint all-domain operations
JIOC	joint intelligence operations center
JIIM	joint, interagency, intergovernmental, and multinational
JWICS	joint worldwide intelligence communications system
LiDAR	light detection and ranging
LRPF	long range precision fires
MARVIN	multi-spectral advance reconnaissance video imaging notator
MASINT	measurement and signature intelligence
MCN-AE	modular communications node-advanced enclave
MDMP	military decision making process
MDO	multi-domain operations
MDSS	multi-domain sensing system

MDTF	multi-domain task force
MI	military intelligence
MIB (T)	MI brigade (theater)
MICO	military intelligence company
MIEW	military intelligence electronic warfare
MIMCA	multi-intelligence modernization combined action
MIMFO	multi-intelligence modernization supporting multi-function operations
MIRAGE	multi-threat IR/RF advanced generic effects
MITS	MI training strategy
ML	machine learning
MOS	military occupational specialty
MTI	moving target indicator
NIFC-CA	Naval integrated fire control-counter air
NIFE	Naval integrated fires element
NIPRNet	non-secure internet protocol router network
NRTIO	near real time identity operations
NSANet	National Security Agency network
NXGBCC	next generation biometrics collection capability
OCO	offensive cyberspace operations
OE	operational environment
OGS	operational intelligence ground station
OSINT	open source intelligence
PAI	publicly available information
PED	processing, exploitation, and dissemination
PLA	People's Liberation Army
POR	program of record
PNT	positioning, navigation, and timing
RAPTR	reconfigurable aperture for precision targeting radar
RC	required capabilities
RDF	Rainmaker data fabric
RF	radio frequency
S&T	science and technology
SAR	synthetic aperture radar
SCARS	simultaneous countermeasures for active reconnaissance and surveillance
SFAB	security force assistance brigade
SHOT	synchronizing high OPTEMPO targeting
SIGINT	signals intelligence
SIPRNet	secure internet protocol router network
SMART	scalable multi-function adaptive RF technologies
SPECTER	stand-in passive collection, targeting and exploitation radar
SSF	Strategic Support Force
STARE	stand-in advanced radio frequency effects
STITCHES	SoS (system of systems) technology integration tool chain for heterogeneous electronic systems
SURF	social understanding and reasoning framework
TAA	total Army analysis

TCPED	tasking, collection, processing, exploitation, and dissemination
TECHINT	technical intelligence
TGS	tactical intelligence ground station
TITAN	tactical intelligence targeting access node
TLIS	terrestrial layer intelligence support
TLS	terrestrial layer system
TNG	theater net-centric geolocation
TRADOC	U.S. Army Training and Doctrine Command
TRL	technology readiness level
TSB	theater support battalion
TSOC	theater special operations command
TS/SCI	top secret/sensitive compartmented information
TTX	table top exercise
UAS	unmanned aerial system
UC	Unified Challenge
UGS	unattended ground sensors
U.S.	United States
USAR	U.S. Army Reserve
USAREUR	U.S. Army Europe
USARPAC	U.S. Army Pacific
USG	United States government
VIBES	voice identity biometrics exploitation services
WAMI	wide area motion imagery
WI	weather initiative

Section II
Terms

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

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

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

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

Army Service component command

Command responsible for recommendations to the joint force commander on the allocation and employment of Army forces within a combatant command. (JP 3-31)

Army special operations forces
(DOD) Those Active and Reserve Component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. Also called **ARSOF**. (JP 3-05)

battle damage assessment
The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force. Also called BDA. (JP 3-0)

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

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

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

collection management
In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 2-0)

command and control
The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Also called C2. (JP 1)

communications intelligence
Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called COMINT. (JP 2-0)

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

counterintelligence
Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. (JP 2-01.2)

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

denied area
An area under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities. (JP 3-05)

dissemination
In intelligence usage, the delivery of intelligence to users in a suitable form. (JP 2-01)

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

electromagnetic spectrum
The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 3-13.1)

electronic intelligence
Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (JP 3-13.1)

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

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

fires
The use of weapon systems or other actions to create specific lethal or nonlethal effects on a target. (JP 3-09)

force modernization
The process of improving the Army's force effectiveness and operational capabilities through force development and integration. (AR 5-22)

fusion
In intelligence usage, the process of managing information to conduct all-source analysis and derive a complete assessment of activity. (JP 2-0)

geospatial intelligence
The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. Also called GEOINT. (JP 2-03)

human intelligence
A category of intelligence derived from information collected and provided by human sources. Also called HUMINT. (JP 2-0)

imagery intelligence
The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. Also called IMINT. (JP 2-03)

information collection
An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations. (FM 3-55)

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

intelligence
(1) The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. (2) The activities that result in the product. (3) The organizations engaged in such activities. (JP 2-0)

intelligence community
All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. (JP 2-0)

intelligence discipline
A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. See also counterintelligence; human intelligence; imagery intelligence; intelligence; measurement and signature intelligence; open-source intelligence; signals intelligence; technical intelligence. (JP 2-0)

intelligence operations

(Army) The tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements. (ADP 2-0)

intelligence preparation of the battlefield
(Army)The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. (ATP 2-01.3)

intelligence warfighting function
The related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment. (ADP 3-0)

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

interoperability
1. The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (JP 3-0) 2. The condition achieved among communications-electronics systems or items of communications electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (JP 6-0)

joint intelligence operations center
An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. Also called JIOC. (JP 2-0)

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

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

materiel
All items (including ships, tanks, self-propelled weapons, aircraft, and so forth, and related spares, repair parts, and support equipment but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. (AR 5-22)

measurement and signature intelligence
Information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized,

technically derived measurements of physical phenomenon intrinsic to an object or event. Also called MASINT. (JP 2-0)

military decision-making process
An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

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

multi-domain operations
Operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture; employment of multi-domain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives. (TP 525-3-1)

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

open-source intelligence
Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. Also called OSINT. (JP 2-0)

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

organization
A unit or element with varied functions enabled by a structure through which individuals cooperate systematically to accomplish a common mission and directly provide or support warfighting capabilities. Subordinate units/elements coordinate with other units/elements and, as a whole, enable the higher-level unit/element to accomplish its mission. This includes the manpower (military, civilian, and contractor support) required to operate, sustain, and reconstitute warfighting capabilities. (AR 5-22)

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

processing and exploitation

In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (JP 2-01)

reconnaissance
A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (JP 2-0)

signals intelligence
1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called SIGINT. (JP 2-0)

site exploitation
(DOD) A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or materiel found during the conduct of operations. (JP 3-31)

situational understanding
The product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables to facilitate decision making. (ADP 5-0)

space domain
The area above the altitude where atmospheric effects on airborne objects become negligible. (JP 3-14)

special operations forces
Those Active and Reserve Component forces of the Services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations. Also called SOF. (JP 3-05)

stand-off
The physical, cognitive, and informational separation that enables freedom of action in any, some, or all domains, the electromagnetic spectrum, and information environment to achieve strategic and/or operational objectives before an adversary can adequately respond. It is achieved with both political and military capabilities. (TP 525-3-1)

strategic support area
The area of cross-combatant command coordination, strategic sea and air lines of communications, and the homeland. (TP 525-3-1)

surveillance
The systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. (JP 3-0)

targeting
The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

technical intelligence
Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. Also called TECHINT. (JP 2-0)

theater Army
An echelon of command designated as the Army Service component command responsible for recommendations of allocation and employment of Army forces to the geographic combatant commander. Also called TA. (JP 3-31)

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)

warfighting function
A system (people, processes, and tools), other enabling capabilities, and group of tasks united by a common purpose that leaders use to accomplish missions and train objectives. (TP 525-3-3)

warning intelligence
Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. (JP 2-0)

window of superiority
Converging capabilities in time and space in selected domains and environments to enable commanders to gain localized control or physical, virtual, and/or cognitive influence over a specified area to prevent its use by an enemy or to create conditions necessary for successful friendly operations. (TP 525-3-1)

Section III
Special Terms

multi-intelligence
Multi-source intelligence from across the different intelligence disciplines such as HUMINT, SIGINT, OSINT, GEOINT, and MASINT

[1] ADP 2-0, p.2-4.
[2] National Defense Strategy 2018
[3] Blank, S. (1991). The Soviet Military Views Operation Desert Storm: A Preliminary Assessment, Strategic Studies Institute.
[4] Gompert, D, Astrid S., Garafola, C., (2016) War with China: Thinking Through the Unthinkable. Rand.
[5] *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the PLA, Washington, D.C., CNA Corporation*. *2005.*
[6] TRADOC Pamphlet 525-3-1, 2028, The U.S. Army in Multi-Domain Operations
[7] National Defense Strategy 2018
[8] Blank, S. 2018 Moscow's Competitive Strategy American Foreign Policy Council
[9] Connell M., Vogler, S., Russia's Approach to Cyber Warfare, Center for Naval Analyses. 2017.
[10] Streltsov A., Basic Goals of Government Policy in Information Wars and Battles, Military Thought (English), 2011.
[11] Russian Military Power - Building a Military to Support Great Power Aspirations. DIA, 2017
[12] Russian Military Power - Building a Military to Support Great Power Aspirations. DIA, 2017
[13] CSIS Space Threat Assessment, 2018.
[14] Military and Security Developments Involving the People's Republic of China 2019 Office of the Secretary of Defense
[15] Cliff, R., Fei, J., Hagen, J., Hague, E., Heginbotham, E., Stillion, J., (2011) Shaking the Heavens and Splitting the Earth Chinese Air Force Employment Concepts in the 21st Century. Rand.
[16] *Chinese Military Power*, DIA, 2019
[17] Gompert, D, Astrid S., Garafola, C., (2016) War with China: Thinking Through the Unthinkable. Rand.
[18] *Chinese Military Power*, DIA, 2019
[19] National Defense Strategy 2018
[20] The Joint Operating Environment 2035, *The Joint Force in a Contested and Disordered,* **2016.**
[21] ISR TTX, BUR, UC
[22] ISR TTX, BUR, UC
[23] ISR TTX, UC
[24] ISR TTX, BUR, UC
[25] ISR TTX, BUR
[26] ISR TTX, BUR, UC
[27] ISR TTX, BUR
[28] ISR TTX, BUR, UC
[29] UC
[30] ISR TTX, BUR, UC derivative writings
[31] ISR TTX, BUR, UC derivative writings
[32] AISR White Paper p. 12
[33] TLS ICD p 5
[34] Tactical Intelligence Targeting Access Node Ground Station Concept of Employment, January 2020 (TITAN CONEMP) p.10 - 11
[35] MDSS ICD p. ii
[36] AISR White Paper p. 17
[37] TLS ICD p iii
[38] DCGS-A CD2, June 19 p.2
[39] DCGS-A CD2, June 19 p.2
[40] Data Science DOTMLPF Assessment, 4 June 2019 p 36
[41] DCGS-A CD2 p. 8
[42] Reach PED refers to PED capabilities at centralized locations where sensor data is disseminated for intelligence PED support. (ADP 2-0)
[43] AISR paper p.3
[44] MIEW CONOPS p 6, 25
[45] DCGS-A CD2
[46] Multi-Functional Intelligence and Electronic Warfare (MIEW) Concept of Operations (CONOPS) p. 9
[47] TITAN CONEMP p. 22
[48] AISR White Paper, p5
[49] AISR White Paper, p12
[50] High Altitude White Paper, p.6
[51] TLS ICD 22 Feb 2018 p. iii
[52] TLS ICD 22 Feb 2018 p. 4
[53] The SOJTF is the equivalent of an Army Echelon above Brigade formation for SOF operational level mission command. It directs ARSOF's indigenous approach that supports Army and joint force regional engagement by developing resilient, capable, and interoperable partners. Networked with cyberspace, space and other joint force capabilities, it shapes friendly, neutral, and hostile perceptions to levy strategic costs, disrupt threat influence activities, influence threat behavior, and disrupt threat information-related capabilities. (Special Operations Supporting Concept) When a GCC establishes and employs subordinate JTFs and task forces, the GCC or commander, theater special operations command, may establish and employ a special operations joint task force, joint force special operations component, special operations command-forward, or joint special operations air component to control SOF assets and accommodate special operations requirements. Accordingly, the GCC establishes command relationships between SOF commanders and other JTF/task force commanders.
[54] STP 34-35D-OFS
[55] STP 34-35D-OFS p. 1-2
[56] TC 2-19.400 p iii
[57] TC 2-19.400 p 1-1
[58] Intelligence Center of Excellence FMD Strategy (2018)
[59] US Army Intelligence and Security Command (INSCOM) 2018 Science and Technology (S&T) RFI Priority
[60] PEO IEW&S S&T Roadmap Item

[61] Army Warfighting Challenge #17 – Employ Cross Domain Fires
[62] Intelligence Center of Excellence FMD Strategy. Intelligence Center of Excellence Problem for Intelligence Force Modernization (2018). US Army Modernization Priority #1.
[63] Army Science Board Study, The Military Benefit and Risks of the Internet of Things
[64] INSCOM Cloud Initiative Concept of Operations
[65] Intelligence Center of Excellence Problem for Intelligence Force Modernization (2018). Army, Navy, and Marine Corps Shared Intelligence S&T Priority. Army Warfighting Challenge #1 – Develop Situational Understanding.
[66] Army Warfighting Challenge #16 – Set the Theater
[67] https://www.defense.gov/explore/story/Article/1747501/clear-skies-for-dod-cloud-initiative/
Intelligence Community Commercial Cloud Enterprise Industry Day Slides, 22 March 2019.
[68] Emerging Science and Technology Trends: 2017-2047, A Synthesis of Leading Forecasts November 2017
[69] Initial Capabilities Document (ICD) for Multi-Domain Sensing Systems (MDSS), Date Submitted: 14 August 2019
[70] TLS ICD 22 Feb 2018 p. 1
[71] TLS ICD 22 Feb 2018 pp. 4-5
[72] TITAN CONEMP pp 4-5
[73] TITAN CONEMP pp 23-29
[74] TITAN CDD
[75] CIHEP-A CDD April 2019
[75] HQDA EXORD 204-17 Identification of gaps in capability between Trojan Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) Lightweight Integrated Telecommunications Equipment (LITE) (V) 3 and the Modular Communication Node-Advanced Enclave (MCN-AE) that require mitigation.
[75] HQDA EXORD 204-17, Transport Convergence
[76] DCGS-A Distributed Common Ground System – Army IS-CDD INC 2 v1.11 20 April 2015. DCGS-A INC 2 RDP v1.3 30 October 2015. DCGS-A INC 2 RDP CD#1 Bn Solution v1.9 12 December 2017. DCGS-A INC 2 RDP CD#2 Fixed Site v1.10 10 October 2018. DCGS-A INC 2 RDP CD#3 Information Collection v1.1 8 December 2017.
[77] Intelligence Collection Exploitation Toolkit CDD (Army Site Exploitation Increment 0) v0.3 2 October 2018
[78] HQDA EXORD 204-17 Identification of gaps in capability between Trojan Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) Lightweight Integrated Telecommunications Equipment (LITE) (V) 3 and the Modular Communication Node-Advanced Enclave (MCN-AE) that require mitigation. HQDA EXORD 204-17, Transport Convergence.
[79] MDSS ICD pp. 4-5
[80] Biometrics Enabling Capability – Intelligence System CDD v1 4 March 2020
[81] Terrestrial Layer System CDD v1.0 16 August 2018. Terrestrial Layer Intelligence Support to MDB, Joint Combined Arms Maneuver ICD v5.0 25 April 2017.
[82] TITAN CONEMP