



**The United States Army's
Concept Capability Plan
(CCP)**

**Intelligence, Surveillance, and
Reconnaissance**

2015-2024

Version 1.0

12 August 2008



This page intentionally left blank.

Foreword

From the Director U.S. Army Capabilities Integration Center

The U.S. Army Concept Capability Plan for Intelligence, Surveillance, and Reconnaissance identifies the capabilities required to execute Army full spectrum operations in the 2015-2024 timeframe. The capabilities identified in this concept capability plan (CCP) provide a coherent starting point for the further examination of potential gaps in intelligence, surveillance, and reconnaissance (ISR) doctrine, organization, training, materiel, leadership and education, personnel and facilities. As such, this CCP will serve as a starting point for comprehensive capabilities based assessments involving many different proponents.

In examining the Army's future ISR capabilities, this CCP describes the environment in which the future Modular Force will likely operate, the emerging threat from our adversaries, and the joint interdependence of ISR operations. The realization of ISR capabilities is essential to achieving the Army's Capstone Concept objective of becoming a strategically responsive, campaign quality force.

The capabilities outlined in this CCP will be refined and updated as new concepts and requirements emerge from research, joint and Army wargaming, interagency exercises, experimentation and combat development. Many of the ISR capabilities introduced in this CCP will be further developed in other proponent capability documents. This CCP crosses many joint and Army functional areas and I strongly encourage its use in our interaction with other proponents, Services, and joint, interagency and coalition organizations.



Michael A. Vane
Lieutenant General, U.S. Army
Director, Army Capabilities
Integration Center

This page intentionally left blank.

Executive Summary

Introduction

a. This concept capability plan (CCP) identifies required intelligence, surveillance, and reconnaissance (ISR) capabilities to enable Army forces to conduct full spectrum operations during the 2015-2024 timeframe. The CCP process provides a basis for the systematic, integrated, and prioritized development of ISR-related capabilities to support the Army's future Modular Force.

b. This pamphlet is developed to support the capabilities based assessments (CBA) to identify tasks, capability needs, and doctrine, organization, training, materiel, leadership and education, personnel and facilities DOTMLPF solutions for the ISR capabilities identified in this CCP.

Purpose

This pamphlet provides a review of existing concepts and provides further amplification of required ISR capabilities and limitations. It serves to inform subsequent ISR conceptual development and may, if deemed necessary, serve as the basis for subsequent CBA efforts.

Scope

a. National agencies, the U.S. Army Intelligence and Security Command, Army Service component command, corps, division, and brigade combat team forces require a fully integrated ISR enterprise, designed around a common and agreed upon focus and purpose to meet the challenges presented by future adversaries and civil support (CS) situations. Effective ISR operations require solutions to integrate all Army, joint, interagency intergovernmental and multinational (JIIM) ISR capabilities within the operational environment. Failure to integrate ISR capabilities and provide adaptive solutions to ISR operations in a joint, interagency, and multinational environment is clearly detrimental to the Army's future Modular Force. Future ISR capabilities will allow U.S. forces to counter the full range of hostile threats our adversaries possess or acquire, and to operate in CS situations. The ISR CCP identifies required capabilities in order to improve and reinforce a commander's ability to obtain decision-quality information and intelligence, gain and maintain information superiority, improve force protection, and mitigate risks to Soldiers.

b. Currently the joint and Army community rely on documents such as the Joint Battlespace Awareness Concept and the *See* functional concept to address and suggest ways to leverage ISR capabilities as an information source. However, neither of these documents provides sufficient details as to how the joint or Army force should conduct ISR operations. The Army currently has no unified methodology or overall plan that defines or establishes how it will perform and support ISR operations at all echelons. The Army lacks clarity on how it plans, prepares, and executes ISR operations within or between echelons or non-military mission partners.

c. ISR is a combined arms operation that employs assets and organizations at multiple echelons—internal and external to the military—to answer the commander’s information requirements (IR).

d. The acronym ISR means different things to different people, and is sometimes little more than a loose theme around which to build arguments for or against systems or organizations. ISR must be understood as a function that examines what we need to achieve, how we want to conduct ISR operations, and what capabilities we require across the DOTMLPF domains to provide a more organized approach to the operational environments we anticipate. Currently, the U.S. Army has numerous ISR capabilities that are not fully integrated and do not provide capabilities as suggested by the Army functional concepts (TRADOC Pam 525-2-1, The United States Army Functional Concept for See 2015-2024; TRADOC Pam 525-3-4, The United States Army Functional Concept for Strike 2015-2024; TRADOC Pam 525-3-6, The United States Army Functional Concept for Move 2015-2024; TRADOC Pam 525-4-1, The United States Army Functional Concept for Sustain 2015-2024; TRADOC Pam 525-3-3, The United States Army Functional Concept for Battle Command 2015-2024; TRADOC Pam 525-3-5, The United States Army Functional Concept for Protect 2015-2024).

Solution Synopsis

The integration of ISR capabilities is a critical mission enabler and is key to the commander’s situational understanding. The ISR CCP conceptualizes the integration of ISR capabilities from different proponents in the U.S. Army. These capabilities may be incorporated into joint ISR processes across the land, air, sea, space, and cyberspace domains.

Key Ideas

ISR capability integration, applied through Army echelons to the joint and multinational force, offers a wealth of active resources against a thinking and adaptive adversary. This integration will provide the following information attributes to the ground forces commander: availability, precision, security, reach, timeliness, persistence, and agility.

- The future Modular Force must have the capability to operate in a future characterized by persistent conflict at the local, regional, and global levels. Future adversaries will have greater targeting, ISR, and counter-ISR capabilities, challenging U.S. ISR effectiveness and technological dominance.
- The availability of information and intelligence via the global information grid (GIG) is critical to the success of the future Modular Force. The GIG must be sufficiently robust and redundant to withstand adversary attempts to tamper with, attack, or disrupt it, as well as survive challenges presented by the operational environment. The future Modular Force must retain the capability to conduct ISR operations under degraded conditions.
- Information must be timely, relevant, appropriate, and understandable to facilitate the military decisionmaking process (MDMP). Soldiers will accurately report a massive amount of collected data, making the challenge facing the future Modular Force not a lack of data, but deriving meaning from an abundance of data. Soldiers will have to make sense of it all, and deliver accurate information to the commander.
- The future Modular Force must ensure the information that informs the MDMP is safeguarded from adversary tampering and is available only to those with the appropriate

security clearance(s) and a valid need to know. This includes the ability to seamlessly interact over the GIG with JIIM partners.

- The future Modular Force must be able to project ISR capabilities across the operational environment. Much like persistence, reach does not imply the future Modular Force will be everywhere, always. Reach enables the force to provide knowledge over larger distances, into space and urban environments, during day or night.
- Much like precision, timeliness adds value to information. The future Modular Force requires the delivery of information in time to be of value to the commander and/or the operation. Timely information is especially critical to the prosecution of time sensitive targets, high-payoff targets (HPT) and force protection.
- While it is impractical and unaffordable to have persistence (described by the Battlespace Awareness Joint Functional Concept as having two aspects—survivability and staying power) everywhere all the time, the future Modular Force requires the capability to focus sensors and analysis on a specific area or target of interest through all phases of an operation, in order to deny the adversary the ability to take action undetected.
- ISR capabilities must provide information dexterity and thus contribute to the agility of the future Modular Force. ISR capability must support lethal and non-lethal capabilities. ISR capabilities must facilitate the future Modular Force's ability to quickly redirect a particular capability to another effort. Finally, ISR capabilities must play a role in ensuring that a weapon system's effects are brought to bear only against the intended target.
- The future Modular Force must be able to detect and differentiate signatures/emanations beyond current capabilities. Key to this effort is the capability to baseline adversary behavior (normalcy)—to include human dimension indicators, societal norms, customs, mores, and thought patterns—to enable analysis to be less reactive (history) and more predictive (anticipatory) of an adversary's potential course(s) of action (intent).
- Future analysts must have critical thinking and adaptive decision-making skills, cultural awareness, language ability, and non-traditional approaches to analysis. This includes the development of automated or machine-aided capabilities that free analysts from the mundane and time-consuming data filtering/processing activities so they can focus on analysis, red-teaming, potential threats, and hypothesis testing. Information overload will challenge future analysts. Therefore, the future Modular Force requires the capability to conduct smart, precise data diving.
- The future Modular Force must be able to conduct robust countermeasures to adversary computer network operations (CNO) and electronic warfare (EW).

Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Monroe, Virginia 23651-1047

TRADOC Pamphlet 525-7-9

12 August 2008

Military Operations

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE CONCEPT
CAPABILITY PLAN 2015-2024

FOR THE COMMANDER:

OFFICIAL:

DAVID P. VALCOURT
Lieutenant General, U.S. Army
Deputy Commanding General/
Chief of Staff


RANDALL L. MACKEY
Colonel, GS
Deputy Chief of Staff, G-6

History. This publication is a new United States Army Training and Doctrine Command (TRADOC) pamphlet developed as part of the Army Concept Strategy for the future Modular Force.

Summary. The Army Intelligence, Surveillance, and Reconnaissance (ISR) Concept Capability Plan (CCP) identifies strategic, operational, and tactical level required ISR capabilities across the full spectrum of conflict in the 2015–2024 timeframe. ISR is a major contributor to the achievement of information superiority which, in turn, satisfies commander’s information needs and ultimately enables effective decision making. The focus of this pamphlet is on ISR as an enabling operation in support of commanders and identifying any improvements that need to be implemented across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) domains to enhance ISR operations. ISR requires effective planning, preparation, execution, and assessment to be of value to the supported force. This CCP draws its key ideas and capabilities from national strategy documents, the Capstone Concept for Joint Operations, the family of joint operations concepts, the Army Concept Strategy family of concepts (capstone, operating, and functional concepts), and capabilities identified in wargames and experiments. The ultimate outcome of this effort is the potential initiation of capabilities based assessments (CBA) to further address identified capability gaps through the Joint Capabilities Integration and Development System (JCIDS) process. This CCP may also

serve as a useful departure point for the development of an overarching Army ISR concept and follow-on combined arms ISR doctrine.

Applicability. This pamphlet applies to all U.S. Army Training and Doctrine Command (TRADOC) and Department of the Army (DA) activities that identify and develop DOTMLPF solutions to field required ISR capabilities. Active Army, Army National Guard, Army Reserve operating forces, and the Army Materiel Command may use this pamphlet to identify future ISR trends in the Army. This pamphlet may also serve as a reference document to agencies within the joint and interagency communities that are planning or are concerned with Army ISR operations and initiatives.

Supplementation. Do not supplement this pamphlet without prior approval from Director, Army Capabilities Integration Center (ARCIC) (ATFC-ED), 33 Ingalls Road, Fort Monroe, VA 23651-1061.

Suggested Improvements. The proponent for this pamphlet is the ARCIC. Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Director, ARCIC, 33 Ingalls Road, Fort Monroe, VA 23651-1061. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program Proposal).

Availability. This publication is distributed solely through the TRADOC Homepage at <http://www.tradoc.army.mil/>

Contents

	Page
Foreword	i
Executive Summary	iii
Chapter 1 Introduction.....	5
1-1. Purpose	5
1-2. Imperatives	5
1-3. References	6
1-4. Explanation of Abbreviations and Terms	6
Chapter 2 Scope and Background.....	6
2-1. Introduction	6
2-2. Functional Area	7
2-3. Scope	7
2-4. Relation to the Family of Joint and Army Concepts	7
2-5. Operational Outcome.....	15
2-6. Complementing the Joint Warfighting Force	15
Chapter 3 The Military Problem.....	15
3-1. Operational Environment	15
3-2. Problem Statement.....	19
Chapter 4 Key Ideas, Operational Setting, and Operational Framework	20
4-1. Key Ideas	20
4-2. Operational Setting	22
4-3. Army Operations within a Joint Campaign Framework.....	25
Chapter 5 Required Capabilities.....	34
5-1. Definitions	34
5-2. DOTMLPF Capabilities Guidelines	34
5-3. Future ISR Capabilities	37
Chapter 6 DOTMLPF Implications and Questions.....	67
6-1. Doctrine	67
6-2. Organization	69
6-3. Training	70
6-4. Materiel.....	71
6-5. Leadership and Education	73
6-6. Personnel	73
6-7. Facilities.....	74
Chapter 7 Risks and Mitigation.....	74
7-1. Risks	74
7-2. Mitigation	75
7-3. Past and Future Experimentation and Wargames.....	80

Appendix A. References	82
Glossary	85

Chapter 1 Introduction

1-1. Purpose

a. Why this concept capability plan (CCP) is needed. A review of the Army's current and projected intelligence, surveillance, and reconnaissance (ISR) concepts and doctrine reveals the need for a comprehensive intelligence, surveillance, and reconnaissance (ISR) concept, doctrine, and plan that establishes and facilitates horizontal and vertical battle command structure at tactical, operational, and strategic levels. This CCP describes the Army's cooperative integration of ISR-enabled capabilities and requirements for the Army's future Modular Force. This CCP identifies future capabilities—used by a wide range of proponents—that enable effective ISR operations in an interdependent joint, interagency, intergovernmental, and multinational (JIIM) environment. Current Army ISR capabilities are not fully integrated or networked and do not provide capabilities as mandated by joint and Army concept publications (chapter 2).

b. ISR is a continuous enabling operation that spans the breadth and depth of military operations. ISR operations require thorough planning, preparation, execution, and assessment. ISR operations contribute to the achievement of a timely and accurate common operational picture (COP) and assist commanders in attaining information superiority. This posture leads to an end state composed of effective and timely decision-making based on answered information requirements (IR). The central premise of this ISR CCP is to identify capabilities across doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) that develop or advance ISR operations to support the future Modular Force commander's IR. Effective ISR operations are pivotal to the successful execution of full spectrum operations.

c. The Army's Capstone Concept envisions that: "...advanced command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities will form the backbone of the Future[Modular] Force, introducing potentially the most revolutionary advances in force effectiveness. In particular, forces will rely on a knowledge-based C4ISR *network of networks*, vertically and horizontally integrated from strategic to tactical level. The network will provide the means for forces at all levels to: achieve situational understanding; establish, maintain, and distribute a COP; create the commander-centric command and control (C2) environment described above, and operate within a noncontiguous battlefield framework. At the same time, the C4ISR network will sharply enhance the lethality, survivability, agility, versatility, and sustainability of the force, enabling more effective and timely application of the elements of combat power."

1-2. Imperatives

a. To achieve the vision of the Army's *Capstone Concept*, this CCP establishes four key imperatives that reduce the commander's level of uncertainty and improve the predictive capability that future Modular Force commanders require. These imperatives constitute a set of distinguishing principles applicable to the consolidated ISR analysis effort of this CCP. They also apply to the most comprehensive set of mission, enemy, terrain and weather, troops, time

available, and civilian considerations (METT-TC) conditions at all echelons derived from capabilities described in joint and Army concept publications described in chapter 2.

(1) Provide the commander with information that rapidly answers IR. Persistent, low latency, and high fidelity information flow that creates an operational advantage ultimately leads to information superiority.

(2) Facilitate synchronization and integration of ISR operations and capabilities across the full spectrum of operations at all echelons.

(3) Maximize current ISR capabilities and create linkages to emerging capabilities.

(4) Deliver ISR capabilities that address requirements and priorities by influencing the design of ISR systems and payloads:

(a) Expedite the transformation of information into intelligence.

(b) Prevent adversary surprise of United States (U.S.) and friendly forces.

(c) Support decisive full spectrum operations.

(d) Facilitate the agility and speed required to dominate full spectrum operations.

b. This CCP will likely result in one or more capabilities-based assessments (CBAs) to further address identified DOTMLPF capability gaps through the Joint Capabilities Integration and Development System (JCIDS) process. Over time, this CCP will evolve, and inform the development of ISR doctrine, concepts, and experimentation.

1-3. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-4. Explanation of Abbreviations and Terms

Abbreviations and special terms used in this pamphlet are explained in the glossary.

Chapter 2

Scope and Background

2-1. Introduction

a. This pamphlet provides a brief synopsis of existing concepts and provides further clarification of required ISR capabilities. It provides direction to the way ahead, and it may serve as a departure point for subsequent ISR concepts and follow-on doctrine. Upon approval, it will likely result in multiple CBA addressing requirements across all ISR components. ISR CBA may recommend DOTMLPF solutions for ISR capability gaps in the 2015-2024 time frame. As the Department of Defense (DOD) evolves to a modular, scalable, and tailorable

force, Army and joint ISR capabilities must be integrated and capitalized upon to enable situational understanding by the future Modular Force in full spectrum operations.

2-2. Functional Area

This ISR CCP identifies capabilities required to conduct ISR operations during the 2015-2024 timeframe. It leverages the battlespace awareness, C2, force application, and net-centric operations joint functional areas, as well as the joint C2, net-centric operating environment, and persistent ISR joint integrating concepts. In addition, this CCP complies with the Army Concept Strategy documents. Finally, this CCP draws strategic insights from the 2006 Quadrennial Defense Review and the 2005 National Intelligence Strategy.

2-3. Scope

a. This CCP focuses on the ISR capabilities required by the future Modular Force in the 2015-2024 time frame, as defined in the Army Concept Strategy family of concepts. It is firmly based on and further extends development of ISR themes presented in current joint and Army concepts. It addresses aspects of strategic, operational, and tactical ISR within a JIIM environment.

b. Future U.S. military warfighting concepts are described in a series of joint and Army publications. Justifications for the required capabilities in this CCP are included in this and other approved documents. Joint publications that provide a backdrop for this CCP are the *Capstone Concept for Joint Operations*, joint operating, functional and integrating concepts, and especially the *Battlespace Awareness Functional Concept*. In addition, this CCP supports Army concepts, including the *Army in Joint Operations*, *Operational*, and *Tactical* maneuver, and the Army functional concepts of *Battle Command*, *See, Move, Strike, Protect*, and *Sustain*. Joint and Army concepts are described in the next section.

c. Full spectrum operations seize, retain and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results for offense, defense, and stability or civil support (CS) operations as part of an interdependent joint force (JF). The source document for the joint operational environment used in this CCP is the U.S. Joint Forces Command.

2-4. Relation to the Family of Joint and Army Concepts

a. Capstone Concept for Joint Operations (CCJO). The CCJO addresses three fundamental actions for employment by the JF in any campaign: Establish, expand, and secure reach; acquire, refine, and share knowledge; and identify, create, and exploit effects.

(1) This plan supports two of the three CCJO reach domains: virtual reach and human reach. The third, physical reach, is established through military operations or diplomacy either by creating an environment of cooperation and mutual understanding or by forcibly gaining access in the face of adversary strategies and anti-access capabilities. Expanding and securing physical reach is accomplished through lethal and non-lethal means to facilitate operational flexibility and to enhance security along all lines of communication (LOC). Securing physical reach includes protecting LOC to discourage or prevent adversaries from disrupting operations.

(a) Virtual reach is established through the use of cyberspace (includes all domains through which information flows) to acquire, transmit and monitor information in order to gain knowledge. Expanding virtual reach is accomplished by having adaptive virtual capabilities. Securing virtual reach requires preventing adversaries or other entities from disrupting operations in the virtual domain.

(b) Human reach is established by thoroughly understanding the adversary or other groups through various means—examples include diplomacy, information derived from humans, and cultural studies. Expanding human reach is accomplished by continuously engaging and studying the group of interest to know when it is adapting and conditions are changing. Securing human reach is gained through mutual trust garnered over time that may discourage or prevent potential adversaries from disrupting operations.

(2) ISR will play its most prominent role in the fundamental joint action—acquire, refine and share knowledge. This action describes the ability of the joint force commander (JFC) to work within and across national and international sources to build and sustain the knowledge necessary to identify required actions and assess effects. A better understanding of U.S. and friendly forces' capabilities, the environment, and the adversary, results in better employment and integration of JF actions to create decisive effects. Knowledge must be timely, relevant, and accurate to be of value, and it must be acquired, prioritized, refined, and shared vertically (strategic, operational, and tactical) and horizontally (within the JF and among interagency and multinational partners). Knowledge is built on information from integrated strategic, operational, and tactical sources, both military and civilian. The future JF must have the necessary capabilities to accomplish integration. Knowledge allows the JF to see, understand, and act before an adversary can, or before operational needs go unmet in humanitarian crises.

(3) ISR is also critical in identifying, creating, tracking, and exploiting effects. This action describes the ability of the JF to integrate capabilities with those of other instruments of national power to create a desired change in the operational environment or prompt a desired action by an adversary or others. This may involve influencing diverse audiences or systems in the environment, defeating an adversary, or rebuilding after a crisis. Creating effects depends on acquiring knowledge and establishing reach. Knowledge of the adversary or situation as a system is required in order to identify actions that will have the greatest likelihood of creating desired effects. Reach is required to bring actions to bear. Identifying, creating, and exploiting effects to achieve assigned objectives is a continuing, iterative process across the diplomatic, information, military, or economic instruments of national power. Effects created by one instrument of national power may influence or change an effect created by another—it is essential that effects be considered holistically by the JF prior to action. The JFC considers planned diplomatic, information, and economic tasks that, when integrated with military tasks, will cause the desired effects that in turn supports achievement of objectives. The JFC balances knowledge, reach, and effects to generate joint synergy and also attempts to harmonize military actions with those of the other instruments to maximize overall impact. Since the outcome of actions taken against a complex system cannot be predicted with precision, it is essential that the effects be continually assessed and actions adjusted until the desired effects are created and objectives are achieved.

b. Homeland Defense and Civil Support Joint Operating Concept. A secure homeland is the nation's first priority and is fundamental to the successful execution of its military strategy. While there is significant overlap between DOD's role and that of the Department of Homeland Security, DOD's role extends beyond the scope of the National Strategy for Homeland Security paradigm to the DOD strategy for homeland defense (HD) and CS to address conventional and unconventional attacks on the homeland by any adversary (including, but not strictly limited to terrorists). This joint concept describes how the JF will plan, prepare, deploy, employ, and sustain the force in 2012 and beyond to detect, deter, prevent, and defeat attacks against the homeland, provide military forces in support of civilian authority, and plan for emergencies. This concept serves to guide the development of future capabilities within a specific segment of the range of military operations that includes HD and CS missions, and emergency preparedness planning activities. ISR is critical to identifying and deterring potential threats—both state and non-state—to the U.S. homeland. The integration of Army ISR with other Service, interagency (local, state, and federal), intergovernmental, and multinational ISR capabilities plays a central role in the homeland security (HS) mission. This CCP supports the development of those capabilities.

c. Battlespace Awareness Joint Functional Concept. Battlespace awareness is the situational knowledge whereby the JFC plans operations and exercises C2. It is the result of the processing and presentation of information comprehending the operational environment—the status and dispositions of friendly, adversary, and non-aligned actors; and the impacts of physical, cultural, social, political, and economic factors on military operations. The ISR CCP will work toward these key components of the Battlespace Awareness Joint Functional Concept, which are listed below.

- (1) Enhanced understanding of the operational environment.
- (2) Seamless integration of operations and intelligence.
- (3) Improved intelligence synchronization.
- (4) Networked, autonomous sensors.
- (5) Actionable intelligence.
- (6) A ubiquitous network.

d. Joint Command and Control (JC2) Joint Functional Concept. At the core of the JC2 Joint Functional Concept is the ability to make sound decisions in an operationally relevant time frame—perhaps the most important by-product of information superiority. To that end, this CCP shares many aspects with the JC2 Joint Functional Concept: a collaborative information network; a COP; heightened situational awareness (SA); multi-domain, multiagency, multinational information sharing; synchronization of intelligence and operations; and precision effects. In addition, the JC2 Joint Functional Concept and future Modular Force ISR must have the following basic and collaborative capabilities.

(1) Basic Capabilities

- (a) The ability to monitor and collect data.
- (b) The ability to develop situational understanding.
- (c) The ability to monitor the execution of the plan and adapt as necessary.

(2) Collaborative Capabilities

- (a) The ability to network.
- (b) The ability to share information.
- (c) The ability to interact.
- (d) The ability to develop shared awareness.
- (e) The ability to develop shared understanding.
- (f) The ability to decide in a collaborative environment.
- (g) The ability to synchronize.

e. Net-Centric Environment Joint Functional Concept. “The networking of all joint force elements creates capabilities for unparalleled information sharing and collaboration and a greater unity of effort via synchronization and integration of force elements at the lowest levels.” Net-centricity provides the capability to exploit all human and technical elements of the JF and its mission partners by fully integrating several factors. These factors are collected information, awareness, knowledge, experience, and decision making enabled by secure access and distribution. A high level of agility and effectiveness can be achieved in a dispersed, decentralized, dynamic, and or uncertain operational environment. It also provides a foundation across the full spectrum of joint operations for providing the ability to share electronically data among multiple sensors. The ISR CCP incorporates net-centricity as a central pillar in establishing information superiority.

f. Protection Joint Functional Concept. Three key protection activities identified in this joint functional concept—detect, assess, and warn—are integral to the ISR CCP. Taken together, they enhance the military decisionmaking process (MDMP). Those three activities support information superiority by providing:

- (1) Persistent detection of threats in an integrated, shared, understanding of the operational environment.
- (2) Rapid assessment of accumulated data.

(3) Timely dissemination of accurate decisions, warnings, and taskings to allow the force to plan and conduct operations to address specific attacks and or threats.

g. Global Strike (GS) Joint Integrating Concept (JIC). GS is defined as responsive joint operations that strike high-payoff targets (HPT) as an integral part of JF operations. GS supports JF operations to overcome anti-access capabilities, produce other effects to achieve operational and strategic objectives, and enable follow-on decisive operations to defeat the adversary. Executing this concept requires the capability to find, fix, track, and target moving targets (such as, integrated air defense system), weapons of mass destruction and or effects (weapons of mass destructions (WMD), weapons of mass effect), theater ballistic missiles, leadership, C2 infrastructure and networks. ISR operations, synchronization, and integration are critical to this capability. Central to the GS JIC is the ability to understand an adversary's operational systems, methods, and decision-making processes. To execute GS requires persistent observation, reconnaissance, and information collection from both open and clandestine sources. Collection activities must access remote and denied areas and defeat camouflage, concealment, and deception through sensor positioning and the development of new sensing capabilities.

h. C2 JIC. The C2 JIC is an expansion of the JC2 Joint Functional Concept. The future operating requirement will demand that U.S. forces have greater shared awareness and understanding as well as a higher degree of confidence in the availability and quality of information. ISR operations enable several of the commander's basic C2 functions: monitor and collect data on the situation, develop an understanding of the situation, develop courses of action and enable course selection, and monitor execution of the operational plan and adapt as necessary. The ISR CCP intends to capitalize on one of the central ideas of the C2 JIC—collaboration. In this context, collaboration is more than information sharing—it is the achievement of situational understanding resulting from collaborative analysis and assessment of adversary and friendly forces, neutral elements, and the environment.

i. Persistent ISR JIC. The Persistent ISR JIC is the most applicable to this CCP effort. This JIC does not propose new sensors and platforms, centralized collection management or better ways to process, exploit, analyze and distribute sensor data, information, and finished intelligence. It focuses on improving persistence through integrated, synchronized management in the planning and direction of ISR assets to the benefit of the JFC. This JIC relies on five enabling capabilities: Integrated planning and prioritization of information needs; multi-level tasking of ISR assets; global visibility of information needs and ISR assets; automated interfaces; and training and education of ISR managers, operators, and analysts. The ISR CCP and subsequent CBA will attempt to address these five enabling capabilities. The Persistent ISR JIC highlights the inherent jointness of the ISR enterprise and recognizes that no amount of ISR will provide perfect information to the commander, but will help to reduce risk to an acceptable level.

j. TRADOC Pam 525-3-0, The Army in Joint Operations, The Army's Future Force Capstone Concept 2015-2024. This is the Army's major conceptual contribution to the joint operations concept family, specifically the CCJO. Just as information superiority is critical to achieving full spectrum dominance in the CCJO, it is equally vital to the seven key operational ideas presented in the Army's capstone concept: shaping and entry operations, operational maneuver from strategic distances, intratheater operational maneuver, decisive maneuver, concurrent and subsequent stability operations, distributed support and sustainment, and

network-enabled battle command (NEBC). The intent of this CCP is to provide insight into the ISR capabilities required to enable the ground forces' contribution to full spectrum dominance.

k. TRADOC Pam 525-3-1, The U.S. Army's Operating Concept for Operational Maneuver 2015-2024. Achieving information superiority is critical to the commander's understanding of the operational environment. This CCP seeks capabilities across the DOTMLPF domains that transform data into information, information into intelligence, and intelligence into knowledge and understanding. The future operating environment will require providing commanders at all echelons faster, decision-quality information. This CCP supports several key tenets of operational maneuver.

(1) Conducting simultaneous, distributed operations across the range of military operations.

(2) Higher levels of simultaneity with respect to both maneuver and precision engagement.

(3) Capability to maintain continuous operations and avoid the operational pauses that in the past introduced vulnerability and enabled the enemy to reconstitute and regroup.

(4) Higher levels of situational understanding that permit the force to operate non-linearly and apply combat power more effectively against critical adversary capabilities.

(5) Routine, deliberate employment of a broad variety of joint capabilities at lower levels in support of land operations, in contrast to a former reliance on organic forces and capabilities.

(6) Accelerated, collaborative military decision-making and execution processes, with incremental changes to operations while in progress, through self-synchronization.

(7) More effective execution of full spectrum operations, with forces capable of conducting rapid transitions between offensive, defensive, and stability operations.

l. TRADOC Pam 525-3-2, The U.S. Army's Operating Concept for Tactical Maneuver 2015-2024. This concept relies on information superiority to achieve the objectives of the tactical force. This CCP explores capabilities in support of several key characteristics of the concept.

(1) Ability to conduct simultaneous and continuous operations to overwhelm and defeat the adversary

(2) Conducting decisive precision maneuver through unprecedented use of tactical mobility, flexibility, information, and fires to achieve tactical decision.

(3) Bringing to bear a full complement of JIIM assets to routinely employ joint capabilities at the tactical level.

(4) Leveraging unprecedented levels of knowledge, self-synchronization and cooperative engagement will enable the future Modular Force to improve tactical tempo and speed, lethality and momentum heretofore not possible.

(5) Accelerated decision making and tactically responsive forces that operate well within the adversary's cycle of adaptation.

m. TRADOC Pam 525-3-3, The U.S. Army's Functional Concept for Battle Command 2015-2024. "...battle command is the key element that translates information into decision superiority and remains the most critical function of joint operations" and "is the integrating function between the functional concepts of *See*, *Move*, *Strike*, *Protect*, and *Sustain*." information superiority, supported by robust, agile, and persistent ISR operations, is a key element in helping the commander exercise command. Key ideas of the *Battle Command* concept supported by this CCP include those below.

(1) Collaborative planning and an accelerated MDMP.

(2) Decision (or information) superiority characterized by heightened situational understanding, a frequently updated COP, continuous battle assessment, incremental adjustment to operations during execution, and adaptive C2 processes.

(3) A single, integrated Army battle command system (the network) joint-capable to lower levels, enabling multinational and interagency interoperability and integration.

n. TRADOC Pam 525-2-1, The U.S. Army Functional Concept for *See* 2015-2024. Though this CCP draws from all six Army functional concepts, the *See* concept provides the most insight into desired and required future ISR capabilities. For a commander to achieve information superiority, he must have timely access to intelligence about the enemy, as well as knowledge of friendly and neutral forces and the operational environment. This CCP focuses on improving two components of the commander's situational understanding: intelligence about the enemy and knowledge of the operational environment. To facilitate and expedite the MDMP, the *See* concept focuses on data acquisition, transformation of data into information, intelligence, and knowledge; and providing intelligence, knowledge, information and data to the future Modular Force. While technological advances present numerous opportunities for improving the intelligence warfighting function, human cognition is an indispensable enabler of information superiority. There is a tendency to seek hardware and software solutions to operational challenges, but the ISR CCP, and the *See* concept it supports, envisions future capabilities coming from all of the DOTMLPF domains. Ultimately, the commander should possess information and decision superiority at such a high confidence level that he can be predictive of, rather than reactive to, the operational environment.

o. TRADOC Pam 525-3-4, The U.S. Army Functional Concept for *Strike* 2015-2024. The *Strike* concept provides several key ideas for this CCP: achieve near real time (NRT) SA for fires employment; conduct collaborative and dynamic strike planning; and synchronize and exploit joint interdependencies. To attain these key ideas, the *Strike* concept envisions numerous future ISR-related capabilities. They include a global network to enable seamless execution and

interdependency of fires and effects; fully integrated linkage between joint ISR and fires; a continuously updated collaborative information environment to support NRT situational understanding; fully integrated systems of systems that enable a COP; and complete or near-complete elimination of strike systems' shortcomings that currently result in sensor to shooter lag, limited range, high sustainability problems, and other undesirable outcomes.

p. TRADOC Pam 525-3-5, The U.S. Army Functional Concept for Protect 2015-2024. This CCP supports four enabling tasks listed in the *Protect* concept: detect, assess, decide, and act. (NOTE: these tasks are different than the five protect activities from the Protection Joint Functional Concept (detect-assess-warn-defend-recover.)) The *Protect* concept acknowledges that the future operating environment will require speed, agility, simultaneity, and precision against an increasingly complex adversary in an increasingly complex operating environment. These dynamics challenge the attainment of information and decision superiority. The range of operational settings within the spectrum of conflict will be considerably more complex with the expectation that U.S. military assistance in CS operations will continue to rise. ISR is a critical component of protecting the homeland and requires early, routine, and thorough collaboration and integration with the joint and interagency communities prior to conducting operations.

q. TRADOC Pam 525-4-1, The U.S. Army Functional Concept for Sustain 2015-2024. This concept establishes the overarching framework for logistics support to the future Modular Force. At the strategic and operational level, future Modular Force support is envisioned as a single joint system. This system will sense and interpret the operational environment and respond through networked capabilities from the source of support to the point of effect. Future Modular Force support operations include supply and field services, medical support, maintenance, transportation, force health protection, Soldier services, and aviation logistics support. ISR enables these operations over the ubiquitous, fully integrated global information grid (GIG), capable of providing NRT situational understanding. The requirement to provide timely information from ISR operations to widely distributed forces in non-contiguous areas of operation poses many challenges to the future Modular Force.

r. TRADOC Pam 525-3-6, The U.S. Army Functional Concept for Move 2015-2024. This concept focuses on strategic force projection and operational agility in support of joint campaign objectives. The Army's approach to this requirement for strategic responsiveness is through a prompt and sustained framework. The *Move* concept has the following specified requirements for ISR.

- (1) A fully integrated, ubiquitous GIG to support NRT situational understanding.
- (2) Fully integrated, modular, joint C4ISR from ship and or shore.
- (3) Continued access to space-based C4ISR.
- (4) C4ISR enabling effective battle command, information superiority, comprehensive situational understanding, and a COP.

(5) ISR organizations, fully integrated within the joint contingency force structure for entry operations.

2-5. Operational Outcome

a. In accordance with the National Military Strategy, the national military objectives are to protect the U.S., prevent conflict and surprise attack, and prevail against adversaries. Future ISR capabilities will provide the Army, the joint warfighter, and their non-military partners with the capabilities needed to attain information superiority, prevent adversary surprise of U.S. and friendly forces, engage in decisive full spectrum operations, and facilitate the agility and speed required to dominate full spectrum operations.

2-6. Complementing the Joint Warfighting Force

This CCP complements the joint and Army forces by identifying future ISR capabilities. It covers the full spectrum of conflict and all echelons of the future Modular Force, as identified in joint publications and Army Field Manual 3-0, Operations.

Chapter 3

The Military Problem

3-1. Operational Environment

a. The changing operational environment (see figure 3-1). Three factors have significantly broadened the operational environment for the future Modular Force. They include emerging technologies, the influence of urban and restrictive terrains, and the influence of non-governmental agencies.

(1) New and emerging technologies and their proliferation will transform the existing paradigms of warfare and ISR. The threat will acquire emergent sensor and information technologies, and will attempt to neutralize, equalize, or overmatch existing Army ISR capabilities. The threat's use of information management technologies and space-based sensors from third-party nations and agencies, also represent a threat to the future Modular Force. Potential adversaries will also have access to a vast array of ISR products and services through legitimate and illegitimate venues. Certain threat forces will have varying degrees of potential to deny, disrupt, deceive, degrade, or destroy U.S. access to and employment of ISR capabilities.

(2) In current and future operational environments, threat forces will move into complex and urban terrain to degrade the Army's capability to develop the situation out of contact. The threat will also use tactics to exploit joint and allied rules of engagement (ROE) to degrade or neutralize joint and allied combat capabilities. Threats will also seek refuge and concealment for their support activities in complex and urban terrain to better evade the surveillance activities of the future Modular Force.

(3) During the 2015-2024 timeframe, future Modular Force ISR elements will operate in a geo-strategic environment of considerable instability, driven by noteworthy demographic,

geopolitical, economic, and technological dynamics. These dynamics will create an environment of friction as cultures, religions, governments, economics, access to scarce resources, the effects of globalization, and people collide within a geographical location. Future Modular Force ISR elements will encounter unprecedented complexities and enormous uncertainties while conducting operations in support of tactical and operational maneuver. The allegiances of the populace within the operational environment will create the requirement for intricate interactions of ISR elements. Some encounters may be clearly nonaligned, others will be undetermined, and there will certainly be a segment that opposes U.S. presence. Although the probability of the U.S. facing a near-peer competitor is remote, U.S. operational superiority would quickly compel the enemy to adapt asymmetrical methods. Compounding these challenges will be the presence and influence of nongovernmental organizations (NGO) in the operational environment. The allegiances and objectives of these NGO will potentially conflict with those of the U.S. and its allies, and will make interagency coordination even more critical.

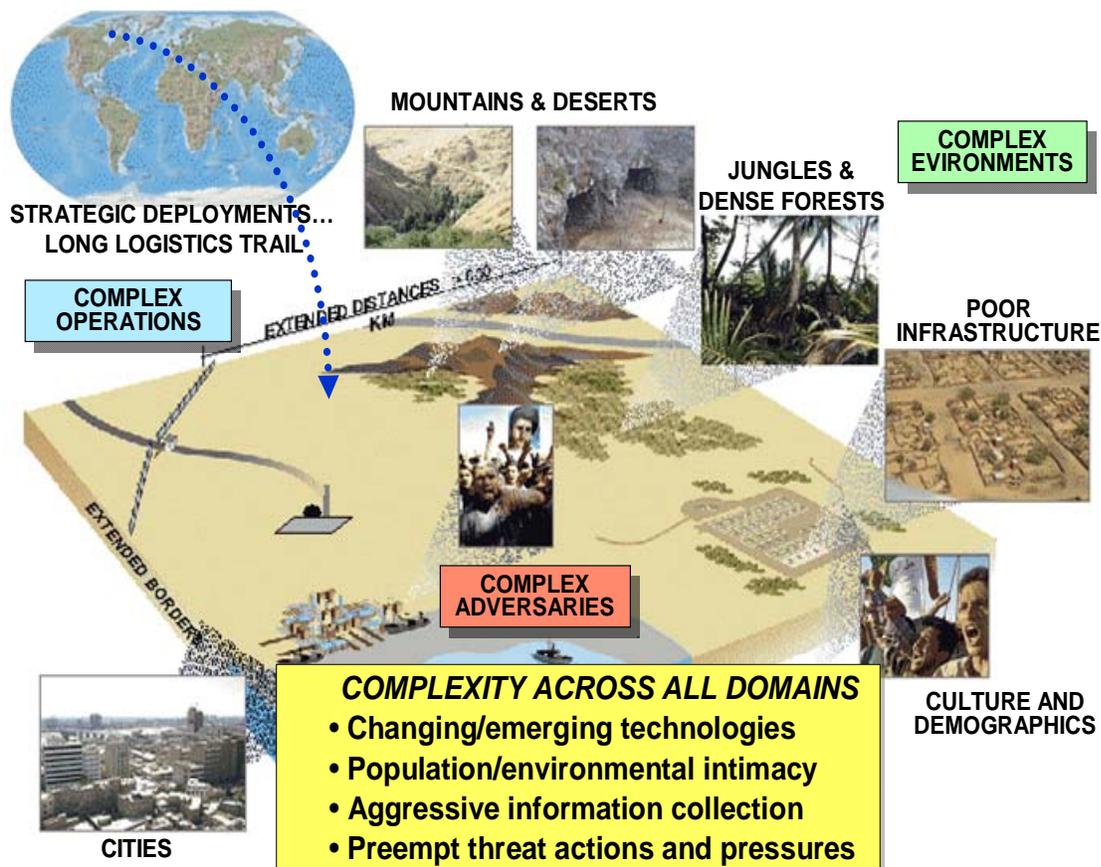


Figure 3-1. Changing Operational Environment

b. ISR Operational Environment and Challenges

(1) An operational environment is defined in joint doctrine as “a composite of conditions, circumstances, and influences that affect the employment of military forces and bear on the decisions of the unit commander.” Information superiority enables the future Modular Force commander to shape the operational environment, but there are significant factors that affect the ability of ISR to support shaping operations. These factors include the integration of

JIIM information and intelligence sources, tailoring ISR capabilities to collect information relevant within urban, restrictive terrain against threat forces using asymmetric tactics, tailoring ISR capabilities to collect relevant information in an environment largely influenced by NGO, and disseminating information with greater speed. These factors challenge the ability of future Modular Force ISR assets to gain and maintain superiority and fidelity of information. However, the end state for ISR operations is not information superiority, it is effective and timely decisionmaking based on answered IR. The future Modular Force will be more vulnerable to direct attack due to the proliferation of communications; sensor, missile, and night vision capabilities; an expanding array of precision munitions; irregular forces; special operations forces (SOF); and a growing threat of WMD. These threats will necessitate greater mobility to avoid detection and targeting. Most adversaries will become more successful in their adaptive use of camouflage, cover, concealment, denial, and deception (C3D2). Combined with dispersion of forces and other adaptive tactics, C3D2 will affect intelligence gathering and targeting.

(2) The operational environment is typically fluid and committed ISR assets will often receive their initial information for an area of interest from JIIM sources (such as, cultural and weather information). Strategic, operational, and tactical ISR elements must collect, fuse, analyze, and distribute intelligence relevant to the operational environment. The ability of Army ISR assets to integrate with JIIM partners will support shaping operations. Cooperative relationships and synchronized information processing procedures will mitigate conflicting efforts and maximize the strengths of all partners.

(3) The future Modular Force will encounter threats that use environmental conditions to support their efforts. Within an operational environment consisting of urban and complex terrain, most military actions will occur at the tactical level, decentralized to battalion, company, platoon, and squad level, and widely distributed throughout the operational environment. To effectively cope with the operational environment, the JFC and staff must consider numerous physical factors associated with operations in the air, land, maritime, and space domains. These factors include, but are not limited to, terrain (including urban settings), weather, topography, hydrology, electromagnetic (EM) spectrum, and environmental conditions in the operational area; distances associated with the deployment to the operational area and employment of forces and other joint capabilities; the location of bases, ports, and other supporting infrastructure; and both friendly and adversary forces and other capabilities in all four dimensions of the operational environment. Combinations of these factors greatly affect the operational design and sustainment of joint operations.

c. Threat. Threat forces will attempt to limit force size and capability to create an opportunity to isolate and defeat early entry forces by employing SOF, long range fires, air, and naval assets to attack points of entry and ports of transfer. Threat forces will work to keep U.S. forces out of areas and facilities key to U.S. operations, and will attempt to force the future Modular Force to areas that present lucrative targets for deep and close fires.

(1) Close combat. Threats will attempt to draw the future Modular Force into close combat situations and attack with a combination of older, but still lethal, technology and state-of-the-art high tech weapons. Threats will use precision munitions, purchased on the open market,

or will often employ locally developed expedients or adaptations, to destroy future Modular Force systems. By attacking future Modular Force systems and degrading their capabilities, they will attempt to create opportunities to mass and attack, and then disperse quickly. Virtually all countries and potential non-traditional adversaries have military capabilities which pose a threat to U.S. forces. In its quest for information superiority, the future Modular Force will face a wide range of conventional and unconventional threats and weapons.

(2) Technological change. The pace of technological change is increasing exponentially. During the 2015-2024 timeframe, the threat will likely be able to gain ground in the technological spectrum or possess selected overmatch when engaged with future Modular Forces. Potential threats have an advantage because their respective military and or paramilitary forces are optimized for their regional environment. Threats will possess advanced communications and signature reduction technologies and implement the full range of C3D2 methods to better coordinate their activities and frustrate future Modular Force target acquisition efforts. Many crises will start regionally, but due to increasing global connectivity, interdependency, and greater access to new, evolutionary, and revolutionary technologies, could rapidly and unexpectedly expand significantly. U.S. forces will face information operations (IO), terrorist attacks, sophisticated ambushes, and adversaries that strike in adaptive, unconventional, and unexpected ways. The operational environment of these conflicts will be complex, intricate, and demanding. This environment could include global information and commercial networks, potential technological revolution, widespread proliferation WMD and selected technologies that will enhance military capabilities, conventionally advanced weapon systems, demographic challenges, and innumerable uncertainties created by complex variables. Information age technologies will provide potential adversaries with capabilities to apply military force with greater precision, lethality, agility, and survivability throughout an expanded environment.

(3) Counter ISR systems. In the past 20 years, adversaries have trained to hide from sophisticated Western sensor capabilities. Threats will employ counter-ISR capabilities to diminish future Modular Forces' situational understanding and awareness. These capabilities will range from advanced technology to unsophisticated, field expedient methods. The prohibitive cost of matching U.S. conventional capability will force most threats to adopt unconventional cost-effective solutions for their military requirements.

(4) Combined traditional, irregular, disruptive, and catastrophic approaches. Threats will combine the widest possible variety of approaches to counter and defeat future Modular Force tactical advantages, including combining conventional, paramilitary, terrorist, and criminal actions, using globally-acquired technologies that counter key U.S. capabilities; and through a catastrophic attack, such as using WMD against the U.S. homeland.

d. Non-combat challenges. U.S. forces will be required to execute a broad range of non-combat operations. These include such missions as stability, support, transition and reconstruction operations, as well as continental U.S. (CONUS) CS. These operations will present human terrain challenges to ISR operations as well as technical challenges created by a focus on primarily non-military targets. The cultural setting will play an important role in these operations. Understanding cultural, ethnic, political, informational, tribal, religious, economic, and ideological factors that govern behavior of the civil populace will be critical. Large

movements of populace are likely to occur or be required, and these will have to be monitored. ISR could face operational "clutter" including medical crises, refugee flows, governmental and NGO, the media, and other factors all contributing to potential multiple dilemmas.

3-2. Problem Statement

a. The Army's ISR capabilities have been traditionally described under tactical and operational doctrine but have never been described as supporting concepts. While the Army's ISR capabilities have been addressed in detail by individual proponents, there is nothing at the unit level (operational or tactical) that specifically describes ISR capabilities and parameters. National agencies, theater Army (such as the Army Service component command (ASCC)), corps, division, brigade combat team (BCT), and supporting forces require integrated ISR capabilities designed around an interdependent and integrated process to meet the challenges encountered in the operational environment. Future Modular Forces operating in joint operational environments will encounter varying degrees of conventional and unconventional threats. These threats will require the collection of information and the integration of intelligence analysis capabilities from lateral and vertical echelons of ISR. Failure to integrate ISR capabilities and provide adaptive solutions to ISR operations in a JIIM environment will result in avoidable risk, resource miscalculation, loss of the initiative, asynchronous battle rhythms, and potentially catastrophic results caused by enemy action. To ensure success, the Army must leverage organic ISR capabilities and facilitate cooperative lateral and vertical ISR capabilities from the other services and JIIM partners through the ISR enterprise. Higher levels of SA and situational understanding will reduce uncertainty, enabling commanders to act more decisively, precisely, and prudently while optimizing the application of all other tactical functions and capabilities.

b. The current role of ISR. Army ISR operations focus on the production of information and intelligence that the commander needs to develop situational understanding and retain the initiative at brigade and below, and timely integration of ISR at division and above. ISR operations enable units to produce the intelligence on the threat, environment, and civil considerations required by force commanders to make critical decisions.

c. Future Role of ISR

(1) The complexity of joint, interagency, and combined arms operations envisioned during the 2015–2024 timeframe will place extreme demands on the future Modular Force commanders and organizations. The purpose of ISR in future operations will not change significantly, but emerging technologies and a more complex human dimension will drive dynamic changes to how the future force conducts ISR operations. In the future Modular Force, ISR seamlessly integrates and synchronizes a critical set of functions with specific tasks supported by capabilities across the DOTMLPF domains. These functions include, but are not limited to collecting, storing, accessing, processing, analyzing, managing, displaying, and disseminating information from a variety of sources. ISR functions support the individual Soldier through the joint task force (JTF) commander for successful execution of operations and retention of the initiative.

(2) ISR capability is retained at all echelons of command. The exponential growth anticipated in both military and commercial information technologies present an opportunity to exploit fully available ISR capabilities throughout all echelons of command and across full spectrum operations. This expansion in ISR technologies highlights the Army's responsibility to influence and shape the design and development of these new technologies to ensure the requirements of the land force are satisfied. Commanders and future Modular Force organizations will depend upon and leverage the power of ISR in order to achieve the Army's seven key operational ideas, as expressed in the Army's capstone. It is within this framework of ISR dependence and risk that the future Modular Force must conduct integrated full spectrum operations.

Chapter 4

Key Ideas, Operational Setting, and Operational Framework

4-1. Key Ideas

a. The integration of ISR capabilities, applied through Army echelons to the JF and interagency partners, offers a wealth of active resources against a thinking and adaptive adversary, and enhances support to civil authorities. This integration will provide the following information attributes to the ground forces commander: availability, precision, security, reach, timeliness, persistence, and agility.

b. The future Modular Force must have the capability to operate in a future characterized by persistent conflict at the local, regional, and global levels. Future adversaries will have greater targeting, ISR, and counter-ISR capabilities, challenging U.S. ISR effectiveness and technological dominance.

c. The availability of information and intelligence via the GIG is critical to the success of the future Modular Force. The GIG must be sufficiently robust and redundant to withstand adversary attempts to tamper with, attack, or disrupt it, as well as survive challenges presented by the operational environment. The future Modular Force must retain the capability to conduct ISR operations under degraded conditions.

d. Information must be timely, relevant, appropriate, and understandable to facilitate the MDMP. Soldiers will accurately report a massive amount of collected data, making the challenge facing the future Modular Force not a lack of data, but deriving meaning from an abundance of data. Soldiers will have to make sense of it all, and deliver accurate information to the commander.

e. The future Modular Force must ensure the information that informs the MDMP is safeguarded from adversary tampering and is available only to those with the appropriate security clearance(s) and a valid need to know. This includes the ability to seamlessly interact over the GIG with JIIM partners.

f. The future Modular Force must be able to project ISR capabilities across the operational environment. Much like persistence, reach does not imply the future Modular Force will be everywhere, always. Reach enables the force to provide knowledge over larger distances, into space and urban environments, during day or night.

g. Much like precision, timeliness adds value to information. The future Modular Force requires the delivery of information in time to be of value to the commander and or the operation. Timely information is especially critical to the prosecution of time sensitive targets, HPT and force protection.

h. While it is impractical and unaffordable to have persistence (described in the Battlespace Awareness Joint Functional Concept as having two aspects—survivability and staying power) everywhere all the time, the future Modular Force requires the capability to focus sensors and analysis on a specific area or target of interest through all phases of an operation, in order to deny the adversary the ability to take action undetected.

i. ISR capabilities must provide information dexterity and thus contribute to the agility of the future Modular Force. ISR capability must support lethal and non-lethal capabilities. ISR capabilities must facilitate the future Modular Force's ability to redirect quickly a particular capability to another effort. Finally, ISR capabilities must play a role in ensuring that a weapon system's effects are brought to bear only against the intended target.

j. The future Modular Force must commit more effort to signatures and emanations detection and differentiation, beyond current or envisioned capabilities. Key to this effort is the capability to baseline adversary behavior (normalcy)—to include human dimension indicators, societal norms, customs, mores, and thought patterns—to enable analysis to be less reactive (history) and more predictive (anticipatory) of an adversary's potential course(s) of action (intent).

k. Develop future analysts with critical thinking and adaptive decision-making skills, cultural awareness, language ability, and non-traditional approaches to analysis. This includes the development of automated or machine-aided capabilities that free analysts from the mundane and time-consuming data filtering and processing activities so they can focus on analysis, red-teaming, potential threats, and hypothesis testing. Information overload will challenge future analysts. Therefore, the future Modular Force requires the capability to conduct smart, precise data diving.

l. The future Modular Force must develop more robust countermeasures to adversary computer network operations (CNO) and electronic warfare (EW). (CNO capabilities will be covered in the CNO CCP; counter-EW capabilities are covered in the EW CCP).

m. It is imperative that the nation develop the capability to implement policy, plans and procedures for conducting ISR operations on American soil. Interoperability across DOTMLPF domains is critical to the HS mission.

4-2. Operational Setting

a. The integration of ISR capabilities into tactical, operational, and strategic plans is a critical combat enabler and is key to the commander's situational understanding. The ISR CCP conceptualizes the integration of ISR capabilities from different proponents in the U.S. Army. These capabilities may be incorporated into joint and interagency ISR processes across the land, air, sea, space, and cyberspace domains.

b. ISR is an inherently joint enterprise, and joint interdependence is essential for the conduct of all ISR operations. Even at the lower tactical levels, where there may be few or no joint assets physically present, the results of joint ISR operations will often provide direct benefit. The synchronized employment of land, air, sea, space, and SOF provides the commander with the widest range of strategic, operational, and tactical options. Joint interdependence is achieved through the deliberate reliance of each Service on its own strengths while protecting or covering the weaknesses or deficiencies of the other Services. In addition to ISR, key joint interdependencies include joint battle command; JF projection; joint air and missile defense; joint sustainment; and joint fires and effects. The Army's capstone, operating, and functional concepts recognize and address each of these dependencies.

c. Reliance on interdependent capabilities could deprive future warfighters of necessary capabilities for success in combat if taken too far. Therefore, force development and employment decisions must emphasize effectiveness over efficiency. However, conducting integrated and interdependent actions is a necessary adaptation to the complexity of the operational environment. It is intended to fully leverage JF capabilities to realize the synergy necessary to effectively counter multiple threats and challenges across the spectrum of operations conducted simultaneously around the world. This idea explicitly recognizes there may be "capability shortages" within any one domain that can be offset through the integrated and interdependent application of capabilities resident in other domains. Applying this idea will enhance JF agility and speed of action, and enhance JF capacity to deter, prevent, and defeat the challenges anticipated in the future operational environment.

d. The array of individuals, specialties, and organizations that influence ISR is considerable and range in sophistication from individual Soldiers on patrol to National Security Agency capabilities. Each increment and specialization fulfills different types of IR according to relevant organizational requirements. Since no single ISR capability is capable of providing a comprehensive COP, Service ISR assets must be able to integrate with joint and interagency capabilities. ISR links and synchronizes multi-echelon ISR capabilities. Army integration will include the following.

(1) Soldier. Soldiers collect and report information through observation as they interact with the terrain and weather, local populations and with threats. Individual Soldiers provide information that can fulfill IR that relate to tactical, operational and strategic information regarding the threat and operational environment. Every Soldier plays a critical role on the battlefield when it comes to SA and reporting. Soldiers have the opportunity to collect information in their operational environment, thus becoming a critical element of their unit's ability to achieve situational understanding of the operational environment.

(2) Through training, all Soldiers are instilled with the mindset that every Soldier is a sensor. Soldiers must seek out knowledge and fight for information in order to gain and maintain greater SA and not wait for intelligence from a higher echelon to filter down to them. Leaders and Soldiers contribute to SA and facilitate information collection by engaging diverse audiences through tactical questioning, liaison activities or operations, debriefing activities and operations, detainee handling, and handling captured enemy documents and captured enemy materiel. Soldiers report information obtained during execution of their assigned mission to answer specified and implied IR. They are able to provide limited instant analysis of anything they observe, which no other information gathering device can do. Every Soldier is a Sensor (ES2) is an Army program to identify information and personnel of immediate intelligence value, but is neither an intelligence program nor part of Army counterintelligence (CI) or human intelligence (HUMINT). However, ES2 is not useful unless each Soldier understands the IR for their unit and how to report that information should they come upon information of value.

(3) Reconnaissance. Dedicated reconnaissance elements primarily function to deliberately collect information on threat composition, disposition, strengths and weaknesses, equipment, capabilities, current course of action, intentions, terrain (to include, for example, bridges, roads, minefields, and tunnels), and environmental conditions. As largely dedicated information collection organizations, reconnaissance elements provide information that fulfills tactical, operational, strategic, and joint IR and commander's critical information requirements (CCIR). Because information collection is the specialized competency of reconnaissance elements, their ISR contributions are focused and their physical capabilities to collect information are specialized to enable extreme degrees of persistence under nearly every conceivable condition. Additionally, reconnaissance elements are assigned or task organized to a variety of organizations from tactical combat units to operationally and strategically focused units.

(a) Ground. Ground reconnaissance capabilities, to include dismounted reconnaissance Soldiers and platform-based assets, will be vital in conditions when stand-off reconnaissance and surveillance systems such as unmanned aircraft systems (UAS) and space-based capabilities cannot operate or are diminished in capability (such as, weather, camouflage). The threat will discover vulnerabilities and limitations of such systems, and exploit them to his benefit. Ground reconnaissance will be able to exploit threat vulnerabilities through persistent contact and interaction with the populations within which the threat conceals itself. Ground reconnaissance will provide the operational commander persistent and immediately available information regarding threat activities and intentions and environmental conditions. This will be particularly vital in complex terrain and in urban areas where reconnaissance must seek out threats that conceal themselves within the population. Within this environment ground reconnaissance elements will frequently be directly engaged and targeted by the enemy. To continue to provide crucial information they must be capable and prepared to survive and fight. Ground reconnaissance confirms or denies reconnaissance by other means.

(b) Aviation. Aviation forces will be a significant contributor to the development of SA and understanding. Acquiring information consists of actions to gather, collect, and fuse data. Aviation assets must fight for collection by conducting operations against the enemy in the

physical realm (such as, surveillance and reconnaissance missions). Gathering information is uncontested by the enemy, and primarily involves readily available data. Data, information, and knowledge resulting from collection involve very little certainty and considerably more human analysis and estimation. Aviation will conduct reconnaissance and surveillance in order to collect information about the activities and resources of an enemy or to secure data concerning meteorological, hydrographic, or geographic characteristics. Future Modular aviation force contributions to the gather function consist of the ability to gather and present the location, status, and missions of all elements of the aviation force through blue force tracking and awareness, and through acquisition of flight, systems, parts data, and information through the aircraft data exploitation capability concept. Blue force tracking is essential for the application of precise future Modular Force and joint strike capabilities. Given distributed and simultaneous operations, asymmetric threats, and complex physical environments, aviation cannot depend on today's painstaking and sometimes inaccurate process for identifying and clearing friendly units and non-combatant locations. The exploitation of available data from aircraft can improve readiness, training, safety, and operations.

(c) Reconnaissance. Aerial reconnaissance provides advanced capabilities to collect data on the enemy that is relevant to joint and future Modular Force requirements. Future Modular Force aviation units must be capable of conducting aerial reconnaissance to produce combat information. Combat information is a by-product of all operations, acquired as they are in progress. Reconnaissance, however, is a focused collection effort that produces combat information. It is performed before and during other combat operations to fight for and provide information used by the commander to confirm or modify his concept. The operational outcome of the reconnaissance mission allows the follow-on forces to maneuver more freely and rapidly to its objectives. Reconnaissance allows the higher commander to keep other forces free from contact as long as possible and concentrated for the decisive engagement. Future Modular Force aviation units employing manned reconnaissance will allow the maneuver commander to 'see first' and facilitate proactive decision-making, and permit friendly maneuver to positions of advantage. Manned and unmanned (MUM) teaming increases operational effectiveness, allowing UAS to assume the dangerous, routine aviation roles while forward decision-makers integrate and fuse information on-scene, and synchronize the combat actions of the combined arms air-ground team. MUM synergy allows manned platforms to focus on battlefield requirements while UAS add sensors, fires, and protection to the effort.

(d) Surveillance. Surveillance is performed by both manned and unmanned aviation in the course of mission execution. Long dwell, persistent surveillance in support of the commander's priority intelligence requirements (PIR) is conducted primarily by UAS operating either autonomously or teamed with manned aircraft. UAS assigned to future modular aviation forces must be capable of systematically observing geographic areas, facilities, and mobile forces with the ability to observe specific named areas of interest (NAI) and target areas of interest (TAI) continuously or with persistent stare. These systems must be capable of ranging any point within the division area of operations (AO) and provide minimum 24-hour continuous observation over complex terrain. Level of interoperability (LOI) 4 control is required for MUM teaming, and UAS should also be capable of ground-air teaming. Sensor systems must be responsive and capable of being dynamically re-tasked in real time. They must provide a capability to perform wide area search to cue other sensors, conduct emitter mapping, electronic

attack (EA), meteorological survey, long endurance wide area surveillance, and wide band communications relay.

4-3. Army Operations within a Joint Campaign Framework

a. An examination of the Army Capstone Concept will outline the plan for the current employment and future development of the Army’s ISR assets. The JF will conduct a phased campaign to achieve assigned objectives. The phases, as elements of the joint campaign, can be inferred from the current CCJO and the Major Combat Operations Joint Operating Concept. These phases often overlap and are described as prepare and posture, shape and enter, conduct decisive operations, and transition (see fig 4-1). The Army future Modular Force will conduct operations fully integrated within the joint operational or campaign framework across the spectrum of conflict. Army operations will enable the JFC to seize the initiative early, transition rapidly to decisive operations, and sustain operations to achieve strategic objectives and maintain stability thereafter. Within the context of the joint campaign framework, the future Modular Force will apply adaptive combinations of seven key operational ideas: shaping and entry operations, operational maneuver from strategic distances, intratheater operational maneuver, decisive maneuver, concurrent and subsequent stability operations, distributed support and sustainment, and NEBC. To facilitate the description of Army ISR operations in support of the future Modular Force, this CCP will concentrate on four phases of the joint campaign as described in TRADOC Pam 525-3-0.

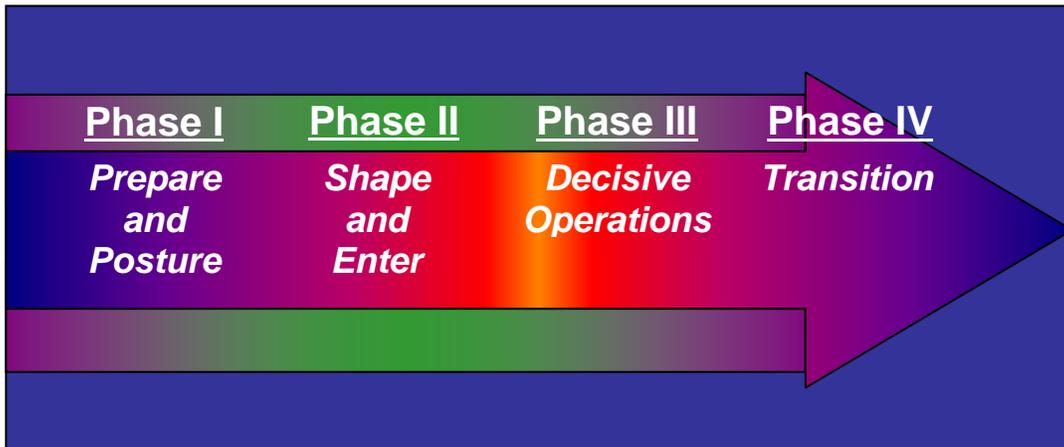


Figure 4-1. Joint Operational Framework

b. Operational Setting. In the future Modular Force, Army ISR will continue to fight for information, synchronize multi-discipline collection, integrate sensing, processing and reporting across all warfighting functions, and improve access, multi-level security, and fusion of data from all available sources. The future Modular Force will be network-enabled, day-night, all-environment capable with access to JIIM capabilities. ISR capabilities will be tailorable, knowledge-based, and manned with expert personnel harnessing the power of modern technology to support commanders and other decision makers, regardless of echelon, Service, or agency. The projected differences between the Army’s ISR capabilities today and in 2015 are as follows.

- (1) There will be an increased capability to collaborate and synchronize between the intelligence and operations processes, as well as all warfighting functions.
- (2) There will be a capability to provide timely and accurate information with fidelity relevant to the COP.
- (3) There will be a capability to access information via the GIG.
- (4) There will be a capability to tailor multi-discipline intelligence for the commander.
- (5) There will be a capability to access expert knowledge, collaboration, and analysis via reach and reachback.
- (6) There will be a capability to enhance multi-echelon sensor integration and synchronize use of all reconnaissance and surveillance capabilities.
- (7) There will be a Capability to operate interdependently with JIIM partners.
- (8) There will be a capability to dynamically task and re-task ISR capabilities across the JF, responsive to fast paced, fluid situations.
- (9) There will be a capability to establish and maintain persistent acquisition and surveillance overmatch in all operational environments.
- (10) There will be a capability to data mine and employ fusion tools to increase SA while reducing processing time.

c. Phase 0/I¹. Prepare and posture. Geographic combatant commanders use a variety of multi-echeloned joint, interagency, and Service component capabilities to develop situational understanding. JIIM training exercises, military exchanges, counterpart visits, partnership events, and other activities are used to build trust and confidence and establish the operational and technical linkages needed for multinational cooperation and interoperability. Joint, combined, and interagency ISR operations, as well as diplomatic exchange, coalition sources, SOF to include civil affairs and psychological operations, police intelligence operations (PIO) and police engagement activities, etc., are used to develop knowledge and refine data repositories that form the foundation for effective information exchange and planning and execution of contingency operations. ISR activities conducted during this phase are initiated and are in progress prior to the deployment of ground forces. The combatant command develops detailed information of the theater, objective areas, and potential adversaries through joint, allied, and coalition coordination, and deliberate ISR preparation. In the homeland, this phase includes integrated interagency exercises, training, planning, cooperative technology sharing, and information sharing before an event occurs.

¹ While this CCP used the four-phase format from the Army Capstone Concept, it acknowledges the normal, routine military and interagency shaping activities (of which ISR is a key component) that occur prior to conflict. See Glossary 2 for the description of Phase 0.

(1) SA. Beyond the information developed through JIIM exchange, ISR provides intelligence on regional stability and potential threats as part of the commander's SA. In peacetime, Army ISR forces, as part of the theater and national intelligence communities, are deployed worldwide and engaged in the collection, analysis, and production of information to support the commander's intelligence needs and the National Military and National homeland security strategies. The ISR enterprise provides the future Modular Force access to national, joint, theater, and coalition ISR data and products. This information forms the foundation against which additional intelligence collection, analysis and reporting are compared to provide indications and warning (I&W) of hostile actions against the U.S. and its interests. Significantly, general military intelligence (GMI) forms the contextual foundation for shared SA. GMI includes pertinent information concerning the political, economic, and social aspects of foreign countries as well as all information on the organization, operations, and capabilities of selected foreign military forces, state actors, non-state actors, and transnational and terrorist organizations. In addition to GMI information, ongoing preparations taking place during the prepare and posture phase require an examination and evaluation of the host nation's civil authority triad—its penal system, judicial system, and law enforcement capabilities. This reflects, in large measure, the adherence to the rule-of-law which lends further military consideration to the propensity of the host nation's indigenous population to affiliate with illicit power structures. These power structures include terrorist organizations, the presence of organized crime, the efficacy of the host nation's penal system, the effectiveness and reputation of the host nation's judicial system (corruption, inhuman treatment, and other). Specific types of information are discussed below.

(a) Threats. Examples of threat data include organized, symmetrical forces and asymmetric threats, such as organized crime elements, illicit power structures, corrupt officials, opposing coalitions, insurgents, terrorists, chemical, biological, radiological, and nuclear (CBRN) hazards (to include WMD and toxic industrial chemical and toxic industrial material). Threats also include drug traffickers, belligerents in peace keeping or peace enforcing operations, and threats to and status of inter- and intratheater transportation infrastructures and ports of debarkation (PODs) and ports of embarkation that could affect planning and execution of strategic airlift, sealift and land movement.

(b) Area of responsibility (AOR) considerations. ISR characterization of the operational environment includes significant political, economic, industrial, geospatial (such as, aeronautical, hydrographic, geodetic, topographic, geologic, botanical), and demographic, medical, climatic, meteorological, and cultural as well as psychological factors of resident populations.

(c) Leadership and C2. Leadership and C2 data includes an assessment of the adversary's will and ability to direct combatant or hostile forces to accomplish a designated mission. It includes information on C2 nodes, lines of authority, reporting chains, and biographical data on key personnel. This collection and analysis effort focuses on establishing the center of gravity at several levels and the links and nodes that provide the resources for maintaining power.

(d) Order of battle. Order of battle data identifies force components and assesses the strengths, vulnerabilities, threat operational doctrine, structures, and dispositions of the personnel and equipment of relevant hostile entities to include WMD.

(e) Technical intelligence (TECHINT). TECHINT assesses the technical sophistication of threat forces, units, weapon systems, and their capabilities, constraints, vulnerabilities, and countermeasures. It will also attempt to determine who is providing certain materials, in particular chemical or nuclear precursor items, or technology to the threat forces.

(f) Force readiness and mission. This data assesses the adversary's readiness, doctrine, and the strategy and tactics it would employ to achieve its objectives.

(g) Force sustainability. Force sustainability assesses the adversary's ability to maintain the level and duration of combat activity (for example, industrial, transportation, and military infrastructure, supply status, attrition rates, and the adversary's morale) necessary to achieve objectives.

(2) I&W

(a) I&W is a continuous effort intended to ensure U.S. forces are not caught unaware. Its purpose is to provide decision-makers early and unambiguous warning of hostile intent against the U.S., its national interests, and its friends and allies. This warning allows national decision-makers to take actions to deter or preempt hostile actions, and sets the conditions for sustained action should deterrence or preemption fail. As a potential crisis develops, commanders begin to concentrate on the situation and prepare for military operations by reviewing existing operational plans. During the planning process, the commander develops more detailed questions and refines his understanding of the current situation through focused intelligence collection and analysis. Warning orders are issued to establish the force structure and command relationships of potentially deploying forces. If the crisis is slow to develop, this process may take months, allowing forces time to conduct deliberate planning, extensive analysis, and mission rehearsals prior to the operation.

(b) If the crisis develops quickly and U.S. interests are immediately in jeopardy, then the planning cycle is compressed and a military unit will be ordered into battle with less time for preparation. All units that receive a warning order for potential participation in a given operation will begin to update existing plans based on the specific mission through METT-TC analysis, and to closely monitor the associated I&W problem and any resulting intelligence reporting. Commanders at all levels are focused on achieving situational understanding. This places increased emphasis on dynamic updates of the situation to support contingency planning and development of force packages. Commanders will task and focus the ISR collection and analysis efforts to obtain the required information and intelligence. The resulting information and intelligence will then be used in planning and rehearsals to develop, modify, and validate operational plans, branches, and sequels.

(c) Commanders of the future Modular Force will have access to all available ISR resources. The intelligence officer, in coordination with the commander's staff, develops the

collection and processing strategies to satisfy the commander's IR and recommends the employment of assets. This function extends to include coordination and integration of these strategies within a larger JIIM framework. Network-enabled reconnaissance and surveillance capabilities provide increased fidelity to conduct activities such as intelligence preparation of the operational environment and running estimate. Data from all sources, military and non-military, is fused to provide a complete intelligence picture, which will reduce timelines for collection, analysis, and reporting. Cross-domain collaboration between ISR elements of the JIIM communities enhances the COP at all echelons. NEBC, of which the ISR enterprise is a key component, accelerates the MDMP. Within the tactical force, the intelligence community (IC), knowledge centers, theater fixed sites, and data repositories are a critical link to fused and tailored products which satisfy IR. From an ISR perspective, the IC remains fully engaged in support of operations throughout all phases of the campaign by matching the battle rhythm of the employed force.

(3) Prior to entering Phase II, the commander evaluates his situational understanding and adjusts his ISR plan to answer IR. Access to national, joint, theater, and coalition data from the ISR enterprise will also assist in answering unit IR. If IRs are not answered, then the commander will have to adjust his course of action or develop a different one.

d. Phase II. Shape and enter. The execution order marks the transition from Phase I to Phase II. Prior to issuing the execution order, divisions, corps, and JIIM ISR assets support shaping operations in the objective area to gain and maintain sensor contact with the adversary and to assist in developing the situation. Upon receipt of the execute order, the geographic combatant commander expands the size and scope of shaping operations. Information and intelligence collected during operational shaping operations is immediately available to initial entry forces, multi-functional and functional brigades, and or BCTs through NEBC and serves to continuously update the COP and running estimate, and inform detailed planning. Commanders at all echelons must employ ISR assets to acquire sufficient situational understanding to employ effectively combat power. ISR assets from echelons above brigade (EAB) continue to provide information to all brigades. Brigades will also employ their ground and air reconnaissance capabilities to provide tactical information and perform security operations. Brigade and below tactical intelligence will be available to all echelons through the ISR enterprise enhancing SA. The commander's ISR assets collaborate with external ISR assets to satisfy IR and provide context and focus to the information and intelligence gathered.

(1) Force packaging and force flow. The organization and flow of the designated force package will depend upon type and relative security/sanctuary of the selected POD. Under most circumstances entry into the AO will be via a combination of sea POD (SPOD) and air POD (APOD). The preferred SPOD is normally located in a friendly, host country where force build-up may occur in relative sanctuary. However, there will be limited scenarios that may require a forced entry into an SPOD. Initial entry using APOD may be a combination of both secure and insecure ports.

(2) Deployment and early entry. Once forces begin deploying into the AO, commanders at all echelons need en route access to intelligence and information to support mission planning and rehearsal and to refine operational plans. IR is fulfilled through the synergistic efforts of all

available ISR assets: Army, joint, theater, interagency, and coalition—from the unit's organic reconnaissance capabilities to space-based surveillance capabilities. Commanders must prioritize their required intelligence support during deployment and early entry operations due to potential transport layer bandwidth constraints. The intelligence officer will manage ISR data through profiles, filters, and other management techniques to answer the commander's IR, and within potential bandwidth constraints.

(3) Commanders must maintain SA of multiple entry points within the AO. The ASCC, division, corps, and JIIM ISR entities provide deploying forces current updates via the COP. The focus of this concentrated effort is to monitor the situation in the AO and determine if any changes to current plans are required, and answers an ongoing question as the commander transitions into theater, “Did a change in the situation on the ground dictate a change to the planned entry operation?”

(4) This portion focuses on supporting commander decisions while en route. Access to the planned APOD is at risk. Once the force is on the ground, it is ready for decisive operations since shaping has occurred simultaneously with deployment through the combined efforts of external ISR capabilities and organic reconnaissance capabilities. Commanders will initiate tactical shaping at this time. Brigades deploy into theater. While the force is building combat power, intelligence support to the commander through ground, air, and space-based reconnaissance assets continues to refine the COP. NEBC provides the commander and the force with continuous updates on the adversary, terrain, weather, civil considerations to include non-combatant organizations, and coalition forces to enable the commander to make timely force employment decisions. When force flow is through a secure SPOD or APOD, the JF land component commander may choose a balanced combination of multifunctional capability including but not limited to: essential ISR capability in order to maintain shaping operations, adequate maneuver and fires forces to initiate immediate action, and necessary mobility and sustainment capability to sustain the force.

(5) When the POD is only partially secured or not secured at all, the initial force package will include the necessary combat power to seize and secure the entry point. This scenario is normally associated with an APOD, but the concept also applies to an unsecured SPOD. Seizing an APOD may include a combination of airborne and airlanded forces. Depending upon the size of the POD, the force may be a BCT or multiple BCT operating under the C2 of a division headquarters (HQ). As the initial combat force seizes the APOD and establishes local security, follow-on forces, early in the deployment sequencing, will include brigade and division level ISR capabilities. The reconnaissance squadron and the military intelligence (MI) company enable the BCT to expand beyond the immediate perimeter of the APOD and establish security and surveillance beyond direct fire weapons capability of the threat force. During entry operations, the combined joint task force (CJTF) has significant ISR assets deployed in the AOR and may have control and/or tasking authority over national assets to detect, identify, and track adversary decisive points and centers of gravity. En route brigades actively collaborate with the CJTF. ISR will provide the threat, non-aligned, and environmental portions of the COP. While brigades are en route, the CJTF employs strike capabilities to shape the operational environment, enabled by information and intelligence collected and developed by supporting ISR assets.

(5) Combat assessments of lethal and nonlethal effects will support decisions regarding the entry locations and unit actions on arrival. To satisfy IR, the CJTF staff will dynamically task, re-task or cue reconnaissance and surveillance assets to provide timely, accurate, and relevant en route and arrival assessments, and to establish the environmental baseline. Until brigades have sufficient combat power and organic collection capability employed, they rely on national, theater, division, or corps ISR assets as they enter the operational environment for maintenance of the COP. Once deployed, brigade reconnaissance assets conduct specific information collection tasks to enable the tactical and operational commanders to develop the AO. The BCT MI element continues to provide context and focus for information and intelligence gathered by echelons-above-brigade. For the future Modular Force, the AO is significantly increased. Upon a brigade's deployment, ISR assets assigned to EAB will complement organic ISR assets. As organic sensor coverage expands, the brigade improves not only its SA, but refines target selection development based on previously determined engagement criteria. Managed by profile and filters, sensor data is available simultaneously to shooters, decision-makers, and analysts, both internal and external to the organization. The NRT access to information enables situational understanding for the commander and empowers him to model future events and the effects of tactical shaping operations.

(6) All brigades have organic, layered ISR capabilities enabling them to cover the assigned AO, with access to augmentation based on METT-TC. As the brigade completes its deployment, ISR elements will transition from a security focus to a reconnaissance focus. A security focus does not mean the brigade's ISR elements are not conducting reconnaissance and surveillance. A security focus simply means that mission orientation is on the position or movement of the friendly main body to provide early warning and time to continue force build-up. The doctrinal necessity to perform continuous reconnaissance for purposes of security does not change. A reconnaissance focus means that mission orientation is on the reconnaissance objective.

e. Phase III. Decisive Operations

(1) In Phase III, objectives are selected and assigned based on ability to see first and conduct shaping operations. ISR operations have depicted the enemy force in sufficient detail to allow the application of combat power at a time and place of the commander's choosing. However, TRADOC Pam 525-3-2 acknowledges situations in which the enemy situation is not adequately developed or is sufficiently vague, requiring commanders to fight for information. The advantages of a fighting force that has information dominance over its adversaries cannot be overemphasized. Thus, the need for future tactical commanders, staffs, and unit personnel to understand the complex tactical environment is critical.

(2) Higher levels of situational understanding and the reduction of uncertainty in future battle will enable commanders to act more decisively, precisely, and prudently while optimizing the application of all other tactical functions and capabilities. The critical role of and need for improvements in ISR capabilities and processes to achieve this goal are self-evident. The ability to maintain such an advantage cannot be taken for granted. Future Modular Force tactical commanders will also need to fight for information in many situations as a prerequisite to informed decisions. Moreover, future commanders must also have the capability to adjust their

ability to see and act first as conditions, missions, and environments change over time, particularly when transitioning between offensive, defensive, and stability operations. This capability is paramount because the information required may radically change during such transitions.

(3) Situational understanding may be even more significant for stability operations to overcome the advantage that an indigenous enemy will undoubtedly possess with respect to knowledge of the conflict environment. The commander's situational understanding (see first) enables the force to maneuver to positions of advantage (act first) and accomplish its mission (finish decisively). Brigades rely on and are interdependent with other ISR formations and capabilities that affect the same AO. There is continuous collaboration with external ISR assets to ensure sensor coverage and create depth. Brigades employ their reconnaissance and surveillance assets to maintain SA and situational understanding within the operational environment. Division and corps ISR assets provide additional SA and context of non-contiguous operational environments. ISR provides the S2 visibility of joint, theater, higher and adjacent unit ISR synchronization plans. Simultaneous information collection and data fusion facilitates military operations and synchronization of organizational echelons. Brigades through organic ISR sensor data and access to external ISR sensor data continuously refine SA and target development. ISR capabilities must also assist in the identification and management of noncombatants and displaced civilians. Special requirements will involve the identification and verification of high-value targets (HVT) and detainees—the necessity for expediency requires this process to occur in near instant fashion to serve the immediate tactical, operational and, at times, strategic commanders' CCIR. There is a strong likelihood that terrorists and HVT will persist in the effort at blending into the local indigenous population to escape detection.

f. Phase IV. Transition

(1) During this phase, theater and National assets and knowledge centers provide I&W as the division and or corps transitions away from combat operations. The combatant commander and all subordinate echelons will transition to stability operations and redefine adversary centers of gravity and focus ISR on political, social, economic and criminal activities that pose a threat to friendly forces and the stability of the AO. Collaboration and interaction with JIIM organizations is essential. Predictive assessments for the remaining threat military forces or illicit power structures contribute to future operational planning and force disposition. It is highly likely that stability operations will be required to at times incorporate tactics, techniques, and procedures (TTP) and ISR assets appropriate for symmetrical warfare and combat depending on the intensity of resistance. Typical centers of gravity for threat forces will be in population centers, which will require more Soldier-civilian interaction supported by stand-off forms of reconnaissance and surveillance. Brigades will continue to employ organic ISR assets, but there will be an increased need for HUMINT to develop SA. Organic sensors support force protection and sustainment operations as theater and national assets continue to conduct overwatch of the AOR to enable full spectrum operations. Access to national, joint, theater, and coalition data bases, as well as collaboration with knowledge centers assists the brigade in developing SA and HVT for transnational threats in the AO.

(2) Timely presentation of relevant information and intelligence continues to be available to the commander via the COP and the running estimate. Collection and analysis for this phase will focus more on the diplomatic, information, and economic domains than previous phases. Throughout the operational phases, returning the governance of the area of conflict to civil authority following hostilities is part of the planning process. ISR assets continue to identify pockets of resistance and monitor environmental conditions. As necessary, forces engage and eliminate these pockets of resistance. EAB will focus on political, social, and economic variables, enable indigenous civil authorities, and provide support for U.S. diplomatic, United Nations and host nation organization's continuing efforts.

g. Army ISR is involved in the planning and execution of military operations across all phases of a campaign. During peacetime, Army ISR supports efforts to both deter conflict and prepare for conflict. One of the underlying principles of America's military strategy is to avoid conflict through deterrence. Deterrence is in part based upon our ability to maintain a global awareness during peacetime that will ensure that evolving crises are identified early enough to prevent them from occurring through some means short of full combat. Army ISR plays an important part in developing that global picture and focusing on potential problem areas when required. Should deterrence fail and U.S. forces be called to respond. Army ISR must ensure that commanders at all echelons have the knowledge needed to be successful at whatever mission they are given. ISR is not additive, but integral, to battle command. Commanders use intelligence preparation of the battlefield to coordinate and synchronize ISR efforts through the GIG as a critical staff process that facilitates and expedites the MDMP. The overarching characteristics of future Modular Force ISR are shown in figure 4-2.

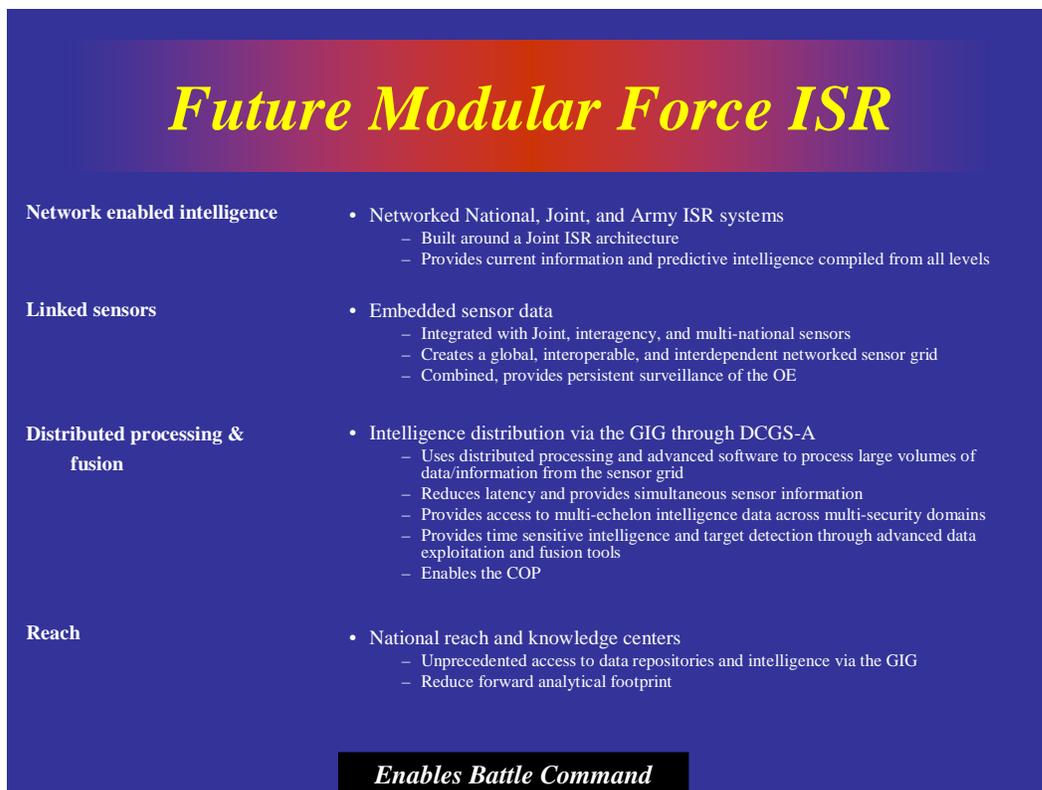


Figure 4-2. Characteristics of the Future ISR Force

Chapter 5 Required Capabilities

5-1. Definitions

a. While each component of ISR, and ISR as a whole, is defined in joint and Army publications, the term “ISR” is subject to much interpretation by individuals, proponents, centers, the individual Services, and the joint and interagency communities. Joint and Army definitions are provided in this chapter as a baseline to ensure required capabilities meet the future Soldier’s needs.

b. ISR

(1) Joint definition. An 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. This is an integrated intelligence and operations function.

(2) Army definition. An enabling operation that integrates and synchronizes all battlefield operating systems to collect and produce relevant information to facilitate the commander’s decision-making.

c. Intelligence, joint and Army definition. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

d. Reconnaissance, joint and Army definition. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

e. Surveillance, joint and Army definition. The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.

5-2. DOTMLPF Capabilities Guidelines

a. Overview

(1) Though the risk inherent in warfare can never be completely eliminated, it can be mitigated by reducing the commander’s uncertainty about the operational environment. To reduce uncertainty the commander requires information superiority, such as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same. This CCP identifies required ISR capabilities, and the need to integrate them to gain and maintain

information superiority. These capabilities must ensure the commander has acquisitions overmatch over threat capabilities; be precise, agile, persistent, secure, and timely; and ensure that ISR information is properly integrated and fused to create a holistic picture of the operating environment.

(2) Future Modular Force joint ISR interdependence is underpinned by a conceptual framework of DOTMLPF. No single DOTMLPF domain will produce a complete or reasonably useful picture of the operational environment. The future Modular Force will create and exploit the synergy of ISR. ISR capabilities supporting each echelon of command must be tailored to provide reliable, focused, persistent, and dedicated support to future Modular Force commanders.

(a) Doctrine. Doctrine provides the structural foundation of our Army. It provides principles and terminology that guide Army forces in joint and Army operations. Joint and Army ISR doctrine will integrate at the strategic, operational, and tactical levels to provide the basic principles of ISR across the future Modular Force. Doctrine forms the basis for training and must be updated to be useful in current operations. Lessons learned integration, once vetted through the Center for Army Lessons Learned or proponent offices, can be used as the basis for updating doctrine and training when doctrine is obsolete. A higher degree of synergy is required in this crucial area to best prepare for both conventional and unconventional threats, and to exploit future ISR capabilities.

(b) Organization. The ability to access information collected or derived from ISR capabilities will exist at all echelons of command. At the strategic level, the Army must access the capabilities of non-Army ISR elements to gain and maintain SA and information superiority. Interdependence among JIIM partners is essential for successful achievement of the commander's intent and addresses his IR. Ground reconnaissance, security, and surveillance assets are a uniquely capable source of tactical information on threat activity within the operational and tactical environment. Ground reconnaissance assets must be survivable to provide persistent, low latency and high fidelity information. When combined with persistent ground and aerial sensor assets, they create a network-enabled architecture which allows for dynamic defense design and task force reorganizations as conditions on the battlefield change, without interrupting ongoing tactical operations.

(c) Training. Training systems must maintain pace with changes that occur in doctrine, organization, and equipment. Training ensures that the future Modular Force is able to conduct full spectrum operations envisioned in joint and Army concepts and codified in doctrine. By embedding ISR capabilities and effects into future Modular Force training, commanders and leaders will begin to expand and capitalize the impact ISR has on warfighting success. Additionally, it is imperative to train ISR professionals to effectively leverage and manage the entire gamut of ISR capabilities. As important as training the ISR force is, ensuring future commanders and leaders at all echelons are well-versed on the ISR capabilities (and limitations) at their disposal is critical. Training devices, simulations and simulators must provide ISR personnel sufficient fidelity to replicate actual conditions encountered across the full range of military operations. Army training must be flexible enough to train and incorporate new technologies (such as embedded system training) at the current and anticipated technology

readiness level. State of the art training must be provided to Soldiers and leaders so they can optimize the ISR capabilities available and develop a joint and expeditionary perspective. Advanced training on currently established TTP integrated with a more realistic training environment that combines specialties and levels of knowledge must also be attained. Different training environments that allow for the training of entirely different warfighting scenarios should also be utilized to enable better knowledge of full spectrum operations. Training must include Army and JIIM capabilities to which the force may have access. It must also include basic reconnaissance skills of individual Soldiers through the newest technology. This includes the ES2 concept.

(d) Materiel. State of the art materiel capabilities should be prevalent in all ISR domains to ensure the future Modular Force commander has a decisive advantage when conducting military operations. ISR elements are usually the first to conduct information collection on threat strengths, weaknesses, location, organization, and dispositions within the operational environment. ISR assets serve as the future Modular Force commander's eyes, ears, nose, and more. As such, they gather and assemble a holistic intelligence picture. This is accomplished through employment of both sophisticated sensor suites such as measurement and signature intelligence (MASINT), signals intelligence (SIGINT), electro-optical infrared, weather systems, as well as ground- and aerial-based air and missile defense sensors and weapons systems that have the capability to detect, locate, track, classify, and identify enemy targets as well as direct observations from Soldiers conducting separate operations. Additionally tactical, theater, joint, National, and multinational ISR sensors linked through an enterprise provide dynamic sensor re-tasking and rapid SA. This requires a dramatic shift from current stovepiped systems to an integrated net-centric system-of-systems that improves current performance and provides the flexibility required to meet the dynamics of the joint operational environment.

(e) Leadership and education. One of the keys in enabling effective full spectrum operations will be the development of leaders and staffs who can perform effectively across the spectrum of conflict in a complex, uncertain, and dynamic operational environment. Leaders must be educated, trained, and developed to be self-aware, innovative, and adaptive throughout training and operations. The interdependence of ISR operations enables Soldiers and leaders to fuse exploitable strategic, operational, and tactical capabilities to ensure warfighting success. Leaders must be educated and experienced with JIIM capabilities early in their careers. Combined with foundations in doctrine, ISR educational opportunities within the institutional training base are required to prepare leaders to be as competent in ISR operational functions as they are with traditional maneuver operations. Leaders will require education on how to manage the ISR system through the 'flat' network which, while maintaining unity of command, enables Soldiers "with access to all sources of information at all classification levels as well as advanced software tools needed to rapidly search, visualize and analyze large quantities of data."²

(f) Personnel. Joint and Army personnel with unique skills in relevant ISR mission areas, including management of the intelligence enterprise, should be assigned to optimize the ISR capability of their organizations. These organizational positions should be considered critical and maintained at authorized capacity. Additionally, as all Soldiers contribute to ISR it is essential that all Soldiers and leaders be capable information collectors (such as, ES2). Soldiers

² Torchbearer National Security Report on Army Intelligence Transformation, Association of the United States Army, Jul 2007, page 7.

should be assigned for the maximum time and certain non-traditional positions should be coded as branch qualifying. This will ensure continuity of effort and trained analysts are kept in strategic positions while staying competitive for promotions.

(g) Facilities. Facilities in the CONUS and in theater must be accessible and exportable to provide the necessary support to operational and tactical warfighters. Facilities must be able to replicate capabilities such as onboard processing, direct down-link, and dynamic retasking. Fixed facilities must be able to support reach-back operations to enhance the SA of deployed tactical units. Surge capabilities using fixed and mobile stations should be an examined option during times of conflict. Mobile facilities may be virtually or physically linked to operational and tactical commanders and the role of these facilities will expand to include both inter- and intra-theater space operations support. Fixed and mobile facilities, in CONUS and in theater, are vulnerable to a wide range of threats and should be provided the levels of security available under the appropriate force protection measures. All related facilities with unique contributions to the ISR efforts must be integrated into the preparation phase as appropriate.

(3) This networked layering and integration of facilities, people, organizations, and materiel is needed to provide the strategic, operational and tactical infrastructure required to advance future Modular Force full spectrum operations. Future Modular Force commanders require reliable, persistent, and dedicated ISR support to achieve the capabilities outlined in joint and Army concepts.

b. The Army's functional concepts provide both explicit and implicit descriptions of the ISR functions necessary to achieve the objective state of the future Modular Force. These capabilities are not ends unto themselves but integral components of a larger capability goal. The influence of a single ISR capability is not confined to a single functional concept but often enables or affects one or more of the functional concepts and multiple proponent areas of responsibility. Because of this, when ISR capabilities are applied simultaneously, they have the potential of creating a synergy no commander or military force has ever enjoyed.

c. Corps, division, BCT, and supporting forces will require a fully integrated ISR system that provides ISR to meet the challenges of future adversaries. This ISR requirement demands new solutions that integrate all joint, Army (operational and tactical), and interagency intelligence capabilities within the operational environment. The required capabilities have been analyzed and presented by intelligence discipline, surveillance capabilities, and reconnaissance capabilities. The areas of surveillance and reconnaissance have been presented by mounted, dismounted, mounted and unmounted airborne, space-based, and sensors capabilities.

d. This listing of required capabilities should be interpreted as objective capabilities for 2015-2024. It is not all inclusive and will be further refined and developed as joint and Army ISR concepts and doctrine emerge, and as JCIDS analyses are executed. Technological and adversary advances may also drive changes to the listed ISR capability requirements.

5-3. Future ISR Capabilities

a. Intelligence Capabilities

(1) All-source intelligence capability statement. The future Modular Force requires the capability to incorporate all sources of information and intelligence, including open-source information, to fuse and produce intelligence in the context of the joint operational environment in order to provide an overall picture of the adversary and the operational environment while supporting the full spectrum of conflict at all echelons.

(a) All-source intelligence encompasses an ever-growing volume of data and information derived from numerous sources, including biometrics, within the operational environment and incorporates intelligence from multiple sources into a single fused intelligence picture. The data and intelligence activities include all single-source disciplines as well as JIIM capabilities. It provides an overall picture of the adversary and the operational environment and reduces the possibility of error, bias, and misinformation through the use of multiple sources of information and intelligence. The ultimate all-source capability is the fusion of information and intelligence across strategic, operational, and tactical environments. Information, when fused by the all-source analyst, enables the commander and his staff to achieve situational understanding to make decisions in order to influence the outcome of operations; prioritize and allocate resources; assess and take risks; and understand the needs of higher, adjacent, and subordinate commanders.

- Fusion is a critical enabler for supporting current and future joint and Army concepts and is defined as a series of processes that transforms observational data into more detailed and refined information, intelligence, knowledge, and understanding (see table 5-1). This definition fails to fully capture a key nuance of fusion, which is that these processes, by their very nature, involve both automation and human cognition.
- The application of fusion impacts several operational imperatives and spans all echelons. Fusion must enable analysis to more rapidly and accurately answer the commander’s PIR and support the creation of the COP and the intelligence running estimate. Additionally it must support battle command, targeting, effects, and combat assessments. Finally, it must provide support to force protection and assist the analyst with ISR integration, synchronization, collection, analysis, and presentation.
- Collection capabilities currently outstrip the ability to rapidly and automatically process and fuse all of the collected information. This results in a requirement for substantial human interaction to produce intelligence. Growth in collectors, both in capability and numbers, will continue at a rapid pace. Should automated processing (fusion) capabilities not make significant progress by 2015, more stress will be placed on humans for analysis, synthesis, and dissemination of intelligence.

**Table 5-1
Fusion Levels**

Characteristics	Levels
Organize the use of discrete pieces of data	Level 0
Identify what is physically out there (searching)	Level 0/1
Resolve data and information conflicts	Level 1/2/3
Correlate like information conflicts	Level 1
Aggregate discrete entities into larger objects	Level 2
Determine what the entities are doing	Level 2
Interpret events and actions	Level 2

Table 5-1
Fusion Levels, cont.

Determine how entities are working together	Level 2
Hypothesize what the enemy or neutral elements will do next	Level 2
Consider how friendly plans will be affected (tied to MDMP)	Level 3
Assess how to improve information fidelity	Level 4
Visualize the information	Level 5

(b) The following capabilities are required to support the all-source intelligence effort.

- The capability to manage theater strategic intelligence activities that include Army and JIIM activities executing Level 0 fusion.
- The capability to collect, receive, or retrieve theater strategic information will enable Level 0/1 fusion.
- The capability to process and exploit collected theater strategic information into useable all-source intelligence enables Level 2 fusion.
- The capability to analyze and produce theater strategic intelligence is the primary capability requirement tied to the intelligence running estimate or Level 2/3 fusion.
- The capability to disseminate and integrate theater strategic intelligence into the COP to enable higher, adjacent, and subordinate levels to conduct their missions (at fusion levels from previous four bullets).
- The capability to evaluate intelligence activities in theater to allow for refinement of all intelligence and operational capabilities at Level 5 fusion.
- The capability to retrieve, search, and disseminate graphically and textually intelligence information within Army and JIIM databases and automation tools.
- The capability to direct operational intelligence activities across the corps and above echelons utilizing organic communications (Army and joint).
- The capability to collect and share operational information across organic corps and above units and populate the COP.
- The capability to process and exploit operational information into the corps and above intelligence running estimate and COP.
- The capability to produce operational intelligence and prepare intelligence products for the corps and above warfighter while enabling the division and below warfighter to react in a timely and responsive manner to meet operational objectives
- The capability to access Army and JIIM information from unclassified to Top Secret and higher (to include caveats) in accordance with applicable security protocols. This includes the ability to retrieve, search, and disseminate intelligence information to civilian, coalition, and partner elements.
- The capability to direct tactical intelligence activities at division and below units that may require integration of coalition and/or JIIM capabilities.
- The capability to collect and share operational information across division and below units.
- The capability to process and exploit operational information into the running estimate and COP at division and below.

- The capability to produce tactical intelligence and prepare intelligence products for combat and support battalion-size units in order to ensure they react in a timely and responsive manner to meet tactical objectives.
- The capability to collect and analyze on-scene information (for example, from improvised explosive device (IED) sites) to determine an adversary's origin, TTP, weapons capabilities, logistics, and others. This could include, but is not limited to, document and media exploitation and collection and analysis of forensic evidence. A current capability exists with the weapons intelligence teams, but it is limited to exploitation of IED sites.
- The capability (architecturally and systematically) for military police (MP) to support all-source intelligence in the application of PIO, which is the integrating function that occurs during the conduct of the other four basic MP functions—law and order operations, internment and resettlement operations, area security operations, and maneuver and mobility support operations.
- The capability to analyze, fuse, collate, archive, disseminate police information collected/retrieved during the application of the five MP functions in a singular system or architecture or process.
- The capability to collect, access, process, and exploit biometrics data to include fingerprint, hand print, iris, deoxyribonucleic acid (DNA), and facial recognition.
- The capability to remotely determine/detect biometric variables/ parameters in all environments
- The capability to protect joint maneuvering forces from reconnaissance, surveillance and target acquisition (RSTA), as well as the full spectrum of potential aerial threats, including cruise missile; ballistic missile; and rockets, artillery (cannon), and mortar threats
- The capability to detect and interpret behavior of a neutral entity or adversary based on cultural indicators (for example, social, religious, tribal, and ethnic).
- The capability to integrate effectively and efficiently JIIM ground and aerial based sensors and weapons system capabilities.

(2) HUMINT capability statement. The future Modular Force requires the capability to conduct military source operations, document and media exploitation operations, screening and debriefings, and interrogations in all environments in order to provide visualization and understanding of the operational environment, provide a shared picture of the situation, precisely locate and track targets, conduct simultaneous operations, operate with joint, combined, coalition and multinational forces, and track and protect friendly forces in support of the ground commander's mission.

(a) As the Army transforms into the future Modular Force through 2015-2024, great emphasis will remain on identification of adversarial forces, their intentions, strengths, weaknesses, capabilities and intent as well as on force protection, technology protection and critical infrastructure protection. Consequently, Army leadership will continue to rely on HUMINT.

(b) Future Modular Force HUMINT must possess the following capabilities.

- The capability to perform HUMINT missions and functions in any environment and at every level of war. This requires HUMINT capabilities to fight for information and be modular, scalable, interoperable, and rapidly deployable.
- The capability to integrate HUMINT collection elements and organizations with other elements (for example, Scouts) and services of the future Modular Force as well as coalition partners to meet future challenges and threats.
- The capability to perform scalable, full spectrum collection at every level of conflict and within every echelon of the force Army HUMINT.
- The capability to facilitate and accommodate input for all forms of data, intelligence, and information under all environmental conditions and safe from enemy exploitation and disruption. This capability will provide effective information reachback, data retrieval, and dissemination and will be available at the lowest tactical level and link with the theater level and beyond.
- The capability to support strategic operations by providing trained HUMINT collectors to satisfy DOD, joint, and National requirements and long-range strategic planning; the capability to execute the full range of its Title 10 functions and missions at the strategic level and provide Title 50 support as required; the capability for strategic HUMINT to support SOF and special mission units within the scope of applicable National, DOD and Department of the Army (DA) security policies and regulations; the capability for all HUMINT echelons to access and interface with joint/National HUMINT databases and products.
- The capability to collect, analyze, produce and exploit documents, electronic media and open source information.
- The capability for HUMINT elements to quickly transition from a peacetime mission to crisis operations in support of the combatant commander's requirements.
- The capability for theater HUMINT elements to conduct unilateral and multinational operations in designated theaters.
- The capability for theater HUMINT to execute the full spectrum of HUMINT missions to collect information in response to the commander's IR.
- The capability to collect, collate, retrieve, disseminate, archive, and secure information and data from across all command echelons extending from squad level through ASCC.
- The capability to maintain a system that harnesses a dynamic informational and intelligence utility that is impervious to disruptions emanating from climate, atmospheric, or enemy interference and activities
- The capability to identify and verify the identification of detainees from the point of capture
- The capability to cross-reference detainees' identity against watch lists and other informational repositories in a timely manner
- The capability to input, retrieve, and selectively disseminate information under all possible conditions
- The capability to exercise unrestricted access in retrieving and communicating information under all situations in NRT.

- The capability to communicate a COP across all echelons from ASCC through squad level in NRT.
- The capability to identify suspicious persons or those intending violence from greater, safer distances.
- The capability to detect and identify suspicious persons among a crowd or gathering of people from safe distances.
- The capability to detect and interpret behavior of a neutral entity or adversary based on cultural indicators (for example, social, religious, tribal, and ethnic).
- The capability (architecturally and systematically) to advance MP support to HUMINT in the combined application of the five basic MP functions—law and order operations, internment and resettlement operations, area security operations, maneuver and mobility support operations, and PIO.
- The capability to fuse, collate, archive, and disseminate HUMINT information, and others, collected and retrieved in the application of the five basic MP functions in a singular system or architecture or process.
- The capability to remotely determine/detect biometric variables/ parameters in all environments, including large gatherings.

(3) Geospatial intelligence (GEOINT) capability statement. The future Modular Force requires the capability to conduct GEOINT activities in the context of JIIM environments in all areas and at all levels/echelons in order to provide early and sustained SA to enhance IO, planning and execution in all operational environments and conditions.

(a) GEOINT is inclusive of imagery, imagery analysis, geospatial engineering, imagery intelligence (IMINT) and geospatial information. GEOINT within the U.S. Army will continue to provide intelligence to the warfighter. However, throughout the next decade, more emphasis will be placed on reducing the end-to-end processing time of the tasking, processing, exploitation, and dissemination process, directly inputting analysis into the COP (perhaps to the point of semi-automation), establishing data repositories of GEOINT related data, and providing better and more abundant GEOINT to the warfighter to the point of establishing a nearly simultaneous, real-time sensor-to-analyst, sensor-to-shooter, and sensor-to-decider situation. Access to network transport and services will be required for this to become a reality.

(b) The future Modular Force will require the following GEOINT capabilities.

- Capability to access national, operational and tactical imagery data (to include full motion video) at brigade level, and GEOINT products at all levels.
- Capability to provide GEOINT between non-contiguous forces whether stationary or on the move in all operational environments and conditions, given a robust distributed communications and information system (all levels).
- Capability to share, push, pull and update information from a wide variety of collection platforms and knowledge bases, access that information simultaneously from multiple distributed, non-contiguous locations in order to provide timely, relevant information in support of the planning, execution and assessment operations of all commanders (all levels).

- Capability to establish early and sustained SA through GEOINT to enhance IO, planning, and execution in all operational environments and conditions (all levels).
- Capability to effectively position, track, cue, cross-cue, task, dynamically re-task, (and delegate the authority to do so) netted layers of redundant space, air, and surface collection assets by the owner of the asset and to task, dynamically re-task, track, and obtain the ability for full control from an asset of another owner, given set rules or priorities established by that owner (all levels).
- Capability to reach back to all knowledge centers and national agencies to rapidly obtain all intelligence related information in all operational environments and conditions, and to establish redundant and distributed GEOINT Knowledge Centers and have the ability to fully control GEOINT Knowledge Centers regardless of the operating environment (all levels).
- Capability to provide high-resolution GEOINT, available in real time, in order to visualize and describe the operational environment under all conditions (all levels and echelons)
- GEOINT systems will have the capability to perform multi-person, multi-station and multi-echelon collaboration using DOD-approved collaboration tools. This includes the capability to simultaneously collaborate and share data and information horizontally at any echelon and vertically between other echelons to include joint and national agencies.
- The capability to input directly GEOINT reports and products into the common reference database to facilitate incorporation of the data into the COP.
- The capability for maneuver, maneuver support, and maneuver sustainment units to display, enhance, start, stop, pause, and annotate GEOINT reports and products.
- Capability to provide persistent imagery surveillance; capability to enable the rapid collection and dissemination of GEOINT; capability to enable the rapid reallocation and re-tasking of surveillance assets; capability to cross-link information and cue other collection assets (all levels).
- Capability to enable autonomous control and information transfer, over the horizon and beyond line of sight (BLOS), with UAS ISR missions (all levels).
- Capability to identify rapidly the locations of friendly and enemy forces.
- Capability to rapidly assess effects to friendly systems and determine if it is the result of friendly or enemy action.
- Capability to identify enemy application of asymmetric weapons or efforts.
- Capability to exploit national, strategic, and operational systems for tactical needs and vice versa
- Capability to conduct long-loiter surveillance (all levels).
- Capability to protect intelligence communications from deliberate or accidental interference.
- Capability to protect the integrity of data while in transit in all operational environments and conditions (all levels).
- GEOINT systems shall have the capability to directly receive and process organic GEOINT data at the BCT level. GEOINT systems shall have the capability to indirectly receive and use non-organic GEOINT data from all sources.

- GEOINT systems shall perform auto-parsing and extraction of selected messages into appropriate databases and fields.
- GEOINT systems and analysts shall have the capability to task all organic and non-organic sensors. GEOINT systems and analysts shall have the capability to tasking, processing, exploitation, and dissemination task-post-process-use all organic GEOINT sensors.
- GEOINT analysts and systems shall have the capability to exploit all GEOINT data from all sources.
- GEOINT systems shall have automated requirements management, mission management, and asset management capabilities to develop ISR synchronization matrices.
- GEOINT sensors on UAS shall have the capability of remotely over-watching key terrain, avenues of approach and danger areas in open and restrictive terrain, and urban areas.
- GEOINT UAS sensors must provide the capability to detect Soldiers and vehicles (moving and stationary) through foliage and in urban terrain.
- GEOINT sensors shall have the capability to conduct long endurance, tactical persistent surveillance across the BCT area of influence.
- Capability to obtain routine and unlimited access to dedicated, persistent GEOINT collection assets at all levels of command in support of strike.
- Capability to access improved real-time, or NRT space-based ISR, on-board sensor processing and direct down link to supported ground systems. This capability should include the ability to dynamically task and re-task space and high altitude long-loiter assets in support of mission objectives (BCT and above).
- Capability to conduct extended range aviation operations with secure over the horizon and BLOS communications, ISR and control data links that provide weather forecasting, terrain and infrastructure updates to include imagery support for en route mission planning and rehearsal, and enemy situation updates in the presence of jamming and counter measures (all levels).
- GEOINT systems shall be capable of automated (assisted or aided) target cueing, recognition, identification, and characterization with or without a human in the loop
- Capability to exploit hyper-spectral imagery (HSI) and multi-spectral imagery (MSI), both space-based and aerial, in a rapid manner for automated and semi-automated land cover classification, to detect and defeat improved camouflage and obscurants, the presence of biological or chemical agents, and other signs of tampering, sabotage, or enemy presence. Provide detection of IED, unexploded ordnance (UXO), and non-explosive obstacles with change detection capability. Provide urban environment detection capabilities to identify threats based on civil activities (all levels).
- Capability to provide dedicated and persistent GEOINT for the protect functions of detect, assess, decide, act, and recover (all levels).
- The future Modular Force will have the capability to harden GEOINT systems against the effects of CBRN, contaminants, decontaminants and electromagnetic pulses.
- Capability to reduce analysis and production time (increased timeliness) is required. GEOINT support to area security operations, maneuver, mobility support operations, law & order operations, and PIO need comprehensive solutions and analysis tools that

enable professionals to manage and mitigate risk, improve accuracy, and dramatically decrease analysis and production time for critical IO.

- At the theater level the future Modular Force requires the capability to obtain high resolution (less than one meter) geospatial data and comprehensive environmental information, including NRT collection in order to visualize, describe, and assess the impact of terrain and weather in all operational environments and conditions.

(4) SIGINT capability statement. The future Modular Force requires the capability to conduct SIGINT activities to gain access to information in denied areas when not deployed, and to provide unique access to information when deployed, for the purpose of developing intelligence in the context of JIIM environments in order to provide warning of adversaries intentions, strengths, weaknesses, and vulnerabilities and to enhance IO, planning and execution in all operational environments and conditions.

(a) SIGINT is intelligence-gathering by interception of signals, whether between people (for example, communications intelligence) or between machines (for example, electronic intelligence), or mixtures of the two. SIGINT consists of several categories: communications intelligence is directed at the analysis of the source and content of message traffic; electronic intelligence is devoted analysis of non-communications electronic transmissions. This would include telemetry intelligence from missile tests, or radar transmitters.

(b) The future Modular Force will require the following SIGINT capabilities.

- Capability to use, process and exploit SIGINT data, information and products to garner intelligence data and geo-locate an adversary.
- Capability to continually exploit and even vector SIGINT satellite products and services.
- Capability to place intercept, direction finding sensors relatively close to friendly forces to facilitate the detection of multi-spectral radio frequency (RF) communications.
- Capability to place intercept, direction finding sensors deep in enemy territory and allowing them to broadcast outside the network via satellite communications to a local/regional hub for exploitation.
- Capability to have UAS with intercept, direction finding capability at all echelons.
- Capability to tap into the local and regional communications system (voice and data), both covertly and overtly, to intercept intelligence data.
- Cryptologic support team capability must be developed down to the squad level.
- Capability to generate, maintain, and define signature databases as required by future SIGINT mission requirements.
- Capability to develop and utilize airborne capabilities to conduct SIGINT operations in dense co-channel signal environments.
- Capability to access national and theater SIGINT data and products.
- Capability to develop SIGINT tools to exploit and analyze data.
- Capability to conduct SIGINT emitter mapping.
- Capability to increase timeliness of data from SIGINT sensors.

- The capability to detect and interpret behavior from a neutral entity or adversary based on cultural indicators (such as, social, religious, tribal, ethnic).
- Capability to support precision targeting.

(5) MASINT capability statement. The future Modular Force requires the capability to conduct MASINT operations, to process and exploit data, information and products from numerous sensors and other intelligence disciplines in the context of JIIM environments in order to provide prompt and sustained enemy SA, preclude enemy success and ensure effective monitoring of the operational environment at all operational levels and in all conditions.

(a) MASINT is technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. MASINT capabilities include radar, laser, optical, infrared, acoustic, nuclear radiation, RF, spectroradiometric, and seismic sensing systems as well as gas, liquid, and solid materials sampling and analysis.

(b) MASINT observables discern distinctive marks, characteristics, sounds or movements. MASINT signatures are limited only by technical means to detect and measure critical enemy and environmental characteristics. Observables include, but are not limited to RF signatures, optical or infrared signatures, spectral signatures, acoustic signatures, seismic signatures, and chemical signatures. Supplemental to MASINT capabilities are products derived from HUMINT, GEOINT (to include IMINT), open- source intelligence (OSINT), SIGINT, and other sources. This additional intelligence information can provide an additional level of fidelity to discriminate similar targets from each other and to provide critical data needed to de-clutter the operational environment. Current MASINT capabilities fall within the following major categories: electro-optical, (spectral, infrared, and laser), radar (LOS, over-the-horizon, and synthetic aperture), geophysical (seismic, acoustic, and magnetic), RF (unintentional radiation and electromagnetic pulse detection), materials (nuclear, biological, and chemical) and nuclear radiation (gamma ray and neutron detection). The future Modular Force requires the following MASINT capabilities.

- Capability to collect, access, and exploit data, information, and products from throughout the ISR system within the joint environment.
- Capability to provide MASINT data and information between non-contiguous forces whether stationary or on the move in all operational environments and conditions, given a robust distributed communications and information system.
- Capability to place sensor fields close enough to friendly forces to facilitate the detection of enemy activities in time to develop a viable defeat plan.
- Capability to place sensor fields deep in enemy territory and enable them to broadcast, via satellite communications or similar capability, to a local and regional hub for exploitation.
- Capability to determine what is happening on a nation's borders (among the first steps towards establishing a nation's sovereignty) in order to interdict illicit activity and contraband in a counterinsurgency setting.
- Capability to detect and locate targets within the parameters of the target selection process, based on the ROE and the target's environment.

- Capability to provide state-of-the-art sensor support for all MP operations.
- Capability to provide the correct number of appropriately trained personnel to effectively field, operate, and maintain sensors at all echelons.
- Capability to extend the range of sensing modalities throughout the commander's area of interest via improved power management and power supplies allowing longer periods of operation and loiter time within and around the operational environment.
- Capability of providing enhanced SA through tactical persistent surveillance via sensing modalities and economy of force measures (for example, by not placing Soldiers in unlikely avenues of approach or placing them in extreme danger while collecting intelligence).
- Capability to operate MASINT sensing modalities in a peer to peer network between sensor nodes and complete compatibility with all future Modular Forces.
- Capability to provide dedicated and persistent MASINT sensing modalities for the protect functions of detect, assess, decide, act, and recover (all levels).
- Capability for all sensing modalities to operate within any and all environments (urban or open terrain, bad weather, underground or under water) with remotely reprogrammable sensing suites and with extended operational life.
- Capability to incorporate ground-based radar.
- Capability to characterize objects within a theater's AOR. This would include the capability to collect detailed surface characterizations of objects to high accuracy, high resolution, and in challenging conditions (such as, darkness or bad weather).
- Capability to access MASINT data and the ability to exploit this information in a timely manner.
- Capability to generate, maintain, and define signature databases as mandated by future MASINT mission requirements.
- Capability to conduct automatic target recognition without a human in the loop based solely on the quality of the signatures database in use.
- Capability for all MASINT sensors to cue automatically other, more objective sensors to establish positive identification for automatic target recognition purposes.
- Capability to conduct long duration, persistent surveillance across the commander's area of influence and interest.
- Capability to access MASINT data and the ability to exploit this data in a timely fashion. Consider the development of ground-based MSI, HSI, and ultra-spectral data. Exploiting this data could help to detect and defeat improved camouflage and obscurants, determine the presence of biological or chemical agents, and identify any signs of tampering, sabotage or the presence of the enemy.
- Capability to provide detection and notification of IED, UXO, and non-explosive obstacles.
- Capability to process collected data within the sensor field (or within the sensor itself) without human involvement.
- Capability to synchronize national MASINT systems and deployable MASINT sensors to characterize the operational environment.
- Capability to collect, access, process, and exploit biometrics data to include fingerprint, hand print, iris, DNA, and facial recognition

- Capability to remotely determine and detect biometric variables and parameters in all environments.
- The capability to detect and interpret behavior from a neutral entity or adversary based on cultural indicators (for example, social, religious, tribal, and ethnic).
- Capability to baseline human behavior in a large population, in order to distinguish abnormal from normal behavior. This includes the ability to detect heart rate, body temperature, anatomical, and other human indicators, enabling the future Modular Force to determine potential adversary intent.

(6) TECHINT capability statement. The future Modular Force requires the capability to generate, exploit, and maintain TECHINT operations and functions in the context of the JIIM environment in order to provide tailored, timely, and accurate intelligence information and training on foreign weapons systems in support of all operations and echelons.

(a) TECHINT is intelligence derived from the collection and analysis of threat and foreign military equipment and associated materiel. The goals of TECHINT are to ensure the U.S. armed forces maintain technological advantage against any adversary, and to provide tailored, timely, and accurate TECHINT support to the warfighter throughout full spectrum operations. This includes providing U.S. forces intelligence, information, and training on foreign weapons systems to an extent that allows their use of captured enemy equipment.

(b) The future Modular Force will require the following TECHINT capabilities.

- Capability to establish linkage with maneuver cells and tactical HQ enabling real time reachback and information management. For example, information and identification obtained from a detainee could be instantly corroborated in establishing whether the person is on a watch list or is suspected as a high-value detainee.
- Capability to enable and facilitate the exchange of data, intelligence, and information into a holistic system of systems that would permit ubiquitous input and collection—impervious to environmental conditions and disruptions caused by the enemy at all echelons and levels.
- Capability to provide a full dimensional application system that would fast-track police intelligence efforts by populating a single source portal that would provide real time corroborative or reachback utility to the user while assuring unfettered access and dissemination.

(7) CI capability statement. The future Modular Force requires the capability to conduct CI investigations, operations, collection, processing, analysis, and technical services in the context of joint, coalition and multinational operations in order to provide force protection, technology protection, and critical infrastructure protection in support of all levels and echelons and in all environments.

(a) As the Army transforms into the future Modular Force through the year 2024, great emphasis will remain on force protection, technology protection and critical infrastructure protection. Consequently, the Army leadership will continue to place a high reliance on CI investigations, operations, collection, processing, analysis, and technical services.

(b) Future Modular Force Army CI must possess the following capabilities.

- Capability to seamlessly integrate with other elements and services of the future Modular Force as well as coalition partners to meet future challenges and threats.
- Capability to visualize and understand their battle space, provide a shared picture of the situation, precisely locate and track critical targets, conduct simultaneous operations, operate with joint, combined, coalition, and multinational forces, and track and protect their own forces.
- Capability to identify, exploit, and neutralize the foreign and adversarial intelligence threats targeting U.S. and friendly forces. This intelligence threat will focus on U.S. intentions, capabilities, strengths, weaknesses and infrastructure.
- Capability to perform CI missions and functions in any environment and in full spectrum operations. This requires CI capabilities to be modular, scalable, interoperable, and rapidly deployable.
- Capability to rapidly deploy to any operational environment.
- Capability to field equipment that is lightweight and reliable, and that has a reduced footprint.
- Capability to field equipment that is interoperable with all intelligence information processing equipment and with other military services to ensure immediate reporting, dissemination and database sharing.
- Capability to tailor operational, management and analysis elements for any military operation.
- Capability to locate CI elements at echelons above their supported unit with plug-in packages, capable of quickly linking up, assimilating, and providing CI support to the unit commander.
- Capability to conduct split-based or decentralized operations, capitalizing on technological advances in collection, analysis, processing, operate on the move, and reporting to respond in NRT to the commander's requirements.
- Capability to respond quickly to regional conflicts, crisis response, power projection, and joint, coalition, and interagency operations, in all environments.
- The capability to detect and interpret behavior from a neutral entity or adversary based on cultural indicators (such as, social, religious, tribal, ethnic).
- Capability to remotely determine and detect biometric variables and parameters in all environments.

(8) OSINT capability statement. The future Modular Force requires the capability to exploit OSINT, in all environments and echelons, in the context of a joint operational environment to satisfy the commander's IR.

(a) Publicly available information forms the basis of all intelligence operations and intelligence products. The availability, depth, and range of publicly available information enable intelligence organizations to satisfy many intelligence requirements without the use of specialized human or technical means of collection. OSINT operations support all ISR efforts by providing information that enhances collection and production. As part of a multidiscipline intelligence effort, the use and integration of OSINT ensures decision-makers have the benefit of

all available information. Though always available, the exponential growth in computer technology and the Internet over the past two decades has placed more public information and processing power at the finger tips of Soldiers than at any time in our past. This combination of technology and information enables the intelligence effort to access large bodies of information required to answer a variety of unclassified intelligence requirements.

(b) Future Modular Force OSINT requires the following capabilities.

- Capability to provide analysts access to OSINT information along with exploitation tools through the ISR enterprise at all echelons and throughout the entire spectrum of conflict.
- Capability to access and exploit reliable, ubiquitous, and timely processing and transmission hardware and software.
- Capability to protect intelligence communications from deliberate or accidental interference while ensuring that needed data is freely transmitted and available to analysts.
- Capability to establish automatic push/pull data ingest features on this common network.
- Capability to incorporate and fuse OSINT into reliable and sanctioned intelligence information.
- Capability to collect and analyze local, regional, and international media information available to different audiences that can affect the operational environment.

b. Intelligence Areas of Interest Capabilities

(1) Intelligence support to EW capability statement. The future Modular Force requires the capability to conduct intelligence support to EW in the context of joint, coalition, and multinational operations in order to provide support to EW and its three major subdivisions (EA, electronic protection, and EW support) for all levels and echelons and in all environments.

(a) EW refers to any military action involving the use of electromagnetic and directed energy to control the EM spectrum or to attack the enemy.

- EA. That division of EW involving the use of EM energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes actions taken to prevent or reduce an enemy's effective use of the EM spectrum, such as jamming and EM deception, and employment of weapons that use either EM or directed energy as their primary destructive mechanism (lasers, RF weapons, particle beams).
- Electronic protection. That division of EW involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability.
- EW support. That division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or

localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, EW support provides information required for decisions involving EW operations and other tactical actions such as threat avoidance, targeting, and homing. EW support data can be used to produce SIGINT, provide targeting for electronic or destructive attack, and produce MASINT. Most EW operations require the support of SIGINT. EW, in turn, can also be used to support and increase SIGINT collection. EW is another tool by which the commander can achieve effects on the enemy while protecting his own force, through control and use of the EM spectrum.

(b) For a complete list of future EW capabilities, refer to TP 525-7-6, the EW CCP.

(2) Intelligence support to CNO capability statement. The future Modular Force requires the capability to conduct intelligence focused CNO in the realms of defense, exploitation, and attack in peacetime and in all phases of conflict, at tactical, operational, and strategic levels in a JIIM environment. This provides commanders down to the battalion level with information dominance, immediate SA, and timely and relevant intelligence such that environmental variables, patterns of life, and human interactions in the cyber domain are accurately depicted and that threats are identified, tracked, given attribution, mitigated, and when authorized exploited or attacked in order to protect the force and to achieve military and national objectives.

(a) CNO is “comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.”

- Computer network attack. “Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.”
- Computer network defense. “Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the DOD information systems and computer networks.”
- Computer network exploitation. “Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.”

(b) A comprehensive list of CNO capabilities will be published in the CNO CCP.

(3) Intelligence support to HS capability statement. The future Modular Force requires the capability to provide assistance, in accordance with law and national policy, to homeland security in the context of National operations in order to support detainee operations, law and order operations, and administrative support to operations (military working dog and protective services) to other government agencies, services, and nations.

(a) MP support to HS is rooted in its Title X responsibilities (detainee operations, law and order operations, and others), and the administrative support (military working dogs, (customs, narcotics, explosives, and others), and protective services), it provides to other

services—many of these tasks could be greatly enabled by advancing various ISR capabilities that would support MPs across the continuum of full spectrum operations.

(b) Future Modular Force Army HS requires the following capabilities.

- Capability to conduct early planning, collaboration, integration, interoperability and information sharing. In HS operations, the Army may be required to operate with JFs, but also with federal, state, local, tribal, and private agencies.
- Capability to improve intelligence interoperability and planning, training, and C2 requirements for HS operations. This might be accomplished through collaborative venues such as exercises, development of systems with mutually beneficial capabilities, conferences and workshops that build integration and interoperability, and providing access to military intelligence training courses.
- The capability, concepts, doctrine, systems, and infrastructure to defeat effectively the full spectrum of potential attacks on the U.S. homeland.
- The capabilities, concepts, doctrine, systems, and infrastructure to respond effectively to HS requirements may resemble some of those required for stability operations overseas.

(4) Army weather capability statement. The future Modular Force requires the capability to conduct weather forecasting and observing operations at the tactical level in all environments to provide prompt, sustained and timely tactical weather observations, tactical forecast and weather effects decision aids in order to update the COP and provide environmental support to all Army activities at all levels, in all environments and at all echelons.

(a) Although Air Force Weather provides most of the Army's weather support, numerous Army-unique weather capabilities exist. Air Force weather support emphasizes providing reachback weather forecast and observation products down to the tactical level. In addition to the Air Force's sustained efforts, Army weather systems continue to evolve their own independent weather support capabilities.

(b) The future Modular Force requires the following weather capabilities to better depict and forecast the operational environment.

- Capability to interface with HQ U.S. Air Force Weather (A3O-W) to establish and refine Air Force support requirements and to provide and define weather support for all levels of support to full spectrum operations.
- Capability to provide timely, accurate, and ubiquitous weather forecasting and observing support at all times and for all echelons using common C2, fully-networked, automatically-updated capabilities. Renewed emphasis will be placed at lower echelons with effective weather information management and visualization capabilities (observed, forecast and decision aid weather information) and cooperative, rapid employment of JIIM integration.
- Capability to transmit/distribute weather data/information up, vertically and laterally within Army future Modular Force units and within the joint operational environment.

- Capability to provide improved weather sensors throughout the operational environment (emphasis on the tactical level), fused and available for input to DOD computer forecasting efforts and to provide timely (NRT) battlefield weather awareness. This will be accomplished through a wide variety of sources and sensors; onboard, remote, in-place, ground-based, space-based, UAS sensor platform, artillery meteorological capabilities, DOD, non-DOD and host nation (gathered) observations, and additional weather observing capabilities yet to be developed. This capability will include a tailorable, layered array of weather sensors in a persistent and semi-persistent weather surveillance mode. As part of this requirement, units will provide this weather intelligence using their own in-house weather resources.
- Capability to provide timely lower-echelon sensor data to upper-echelon (DOD) weather forecast support agencies (such as, Air Force Weather and subordinate functional organizations).
- Capability to employ less-detectable, remotely programmable unmanned sensors.
- Capability to support seamlessly the information needs of any element of the force based on operational opportunities/requirements.
- Capability to develop weather sensor strategy for each AO and all operating conditions.
- Capability to provide continuous access to ever-increasing space-based weather support capabilities, including weather imagery of all types, space-based weather sounding data and surface temperature/soil moisture characteristics.
- Capability to model weather, embedded at appropriate operational and tactical, echelons. This includes utilizing a running estimate capability to provide near-term, timely, and frequently updated (high refresh rate) weather forecasts to the COP.
- Capability to provide weather information (observations, forecasts and decision aids), processed, disseminated and displayed for operations and support.
- Capability to provide weather information (observations, forecasts, and decision aids) for CBRN hazard prediction models and sensors (pre- and post-employment of CBRN capability).

(5) Intelligence process—collection management, ISR synchronization capability statement. The future Modular Force requires the capability to conduct three-dimensional intelligence process collection, management ISR synchronization at all levels in all environments, including the JIIM environments, to provide the prompt, sustained and timely operation and orchestration of sensors, assets, processing, exploitation, and dissemination systems in direct support of current and future ISR operations at all echelons.

(a) ISR synchronization represents the integrated intelligence and operations function described in Joint Publication 1-02. For Army forces, this activity is a combined arms operation that focuses on PIR while answering the IR. Through ISR, commanders and staffs continuously plan, task, and employ collection assets and forces. ISR assets and forces collect, process, and disseminate timely and accurate information, combat information, and intelligence to satisfy the IR and other intelligence requirements. When necessary, ISR assets may focus on special requirements, such as personnel recovery.

- Army doctrine recognizes the joint ISR definition; Army ISR operations complement joint ISR activities. However, Army ISR operations are unique. Because of the complex interaction of Army forces within the civilian population, terrain and time, the Army focuses ISR operations for maximum collection by limited assets to produce the best intelligence and COP possible. Army units contend with complex terrain considerations requiring a fully concerted effort between all ISR assets to included coordinated exploitation of joint and national ISR capabilities. ISR must be extremely flexible, allowing for re-tasking as current operations warrant. Every unit has unique requirements and contributions in the conduct of surveillance or reconnaissance. Many of the personnel and units that provide information for ISR have a primary mission other than ISR.
- ISR synchronization is the task that accomplishes the following: analyzes IR and intelligence gaps; evaluates available assets internal and external to the organization; determines gaps in the use of those assets; recommends ISR assets controlled by the organization to collect on the commander's IR; and submits requests for information for adjacent and higher collection support. This task ensures that ISR and requests for information result in successful reporting, production, and dissemination of information, combat information, and intelligence to support decisionmaking.
- ISR synchronization ensures the commander's requirements drive ISR operations and that ISR reporting responds in time to influence decisions and operations. The intelligence officer, in coordination with the operations officer, and with staff participation, synchronizes the entire ISR effort to include all assets the commander controls, assets of lateral and higher echelon units and organizations, and intelligence reach to support intelligence production and dissemination which helps answer IR and other requirements. The Army division remains the lowest echelon that conducts long-term analysis functions, and is often the lowest echelon at which representatives of national agencies may be present. ISR assets are resident in some form at all warfighting levels. Each echelon requests support from higher and adjacent organizations and directs requirements to subordinates. Coordination between tactical, operational, and strategic levels follow established IC protocols and utilize Army, joint, and DOD programs.

(b) Future Modular Force ISR synchronization requires the following capabilities.

- Capability to develop, implement, and leverage multi-discipline collection strategies.
- Capability to manage, orchestrate, task, synchronize, and integrate JIIM and Army (MI and non-MI) ISR sensors in all operational phases across the spectrum of conflict.
- Capability to provide fusion and other analytical capabilities to support situational understanding of ISR assets.
- Capability to graphically and textually display all ISR assets within a given theater or operational environment and share with higher, adjacent and subordinate echelons.
- Capability to graphically and textually create and display NAI, TAI, and commander's decision points, and share with higher, adjacent, and subordinate echelons or organizations.

- Capability to apply privileges to the ISR synchronization matrix for those authorized to modify and those authorized to read.
- Capability to associate incidents within a given area to IR with associated ISR asset at or in the vicinity.
- Capability to archive the ISR synchronization matrix to compare performance and utilization of each ISR asset over time
- Capability to orchestrate, task, synchronize, and integrate all tactically deployed ISR sensors or collection capabilities. Includes ES2, JIIM entities, and civilians.
- Capability to provide timely and relevant tactical ISR reporting through operational to strategic ISR and operations units, organizations, and agencies.
- Capability to deconflict like information from like ISR sensors or platforms.
- Capability to track collection requirements through the operations and intelligence cycles.
- Automated capability to predict environmental effects on ISR sensors.
- Capability to develop plug-and-play sensors dependent on the theater and the unique requirements of the operational environment, in order to facilitate the incorporation of emerging sensor capabilities.
- Capability to conduct a multi-discipline signature survey of the operational environment. This includes the ability to network sensors to ensure optimized sensor coverage to meet mission requirements.
- Capability to evaluate sensor effectiveness; improve or replace deployed sensors, and or develop new ones; and make the sensor network more robust (types, placement, numbers) based on evolving operational requirements.

(6) Integrated Broadcast System (IBS) capability statement. The future Modular Force requires the capability to leverage IBS at the tactical and operational levels in all environments, including the JIIM environments, to provide the prompt, sustained, and timely dissemination of multi-source and combat information that contributes to SA, survivability, and targeting in direct support of full spectrum operations in all environments.

(a) The mission of the IBS is to provide time-critical survival information and intelligence data broadcast via the GIG to tactical forces. Examples of time critical survival information and intelligence include threat detection, threat warning, and SA. In other words, the information sent is so time-sensitive it needs to be broadcasted to forces within the broadcast footprint and allows commanders to take immediate actions to defeat or counter the threat, and order a protective posture. IBS provides commanders the ability to access a multi-source, integrated network of threat data that is automatically pushed to forces deployed worldwide. Commanders may also query the IBS network in order to pull specific data.

(b) Future Modular Force IBS capabilities include the following.

- Capability to broadcast meteorological targeting data (as backup) to firing units and disseminate potential severe weather conditions.
- Capability to provide global positioning system accuracy guidance updates (based on space weather conditions).

- Capability to provide back-up and dissemination capabilities announcing global positioning system outages.
- Capability to conduct semi-automated target development.
- Capability to alert analysts that newly processed data contains information concerning HVT or NAI TAI.
- Capability to develop semi-automated tools to assist in conducting combat assessment and supporting battle damage assessment (BDA).
- Automated capability to integrate HVT and HPT lists into the ISR synchronization plan.

(7) Intelligence Support to Targeting. The following are required to support targeting.

- (a) Capability to conduct semi-automated target development.
- (b) Capability to alert analysts that newly processed data contains information concerning HVT, HPT or NAI TAI.
- (c) Capability to develop semi-automated tools to assist in conducting combat assessment and supporting BDA.
- (d) Automated capability to integrate HVT HPT lists into the ISR synchronization plan.
- (e) Capability to fuse target location error (TLE) data from multiple sources to provide refined TLE in support of precision engagements.
- (f) Capability to provide TLE, indicating sensor location accuracy.

c. Reconnaissance and Surveillance Capabilities

(1) Mounted reconnaissance and surveillance capability statement. The future Modular Force requires the capability to conduct mounted reconnaissance and surveillance at the tactical and operational levels in all environments, including the JIIM environments, to ensure the success of early entry, forced entry (opposed, unopposed), shaping, decisive offense/defense, and stability operations, and to monitor meteorological, hydrographic, and geographic characteristics at all echelons.

(a) Mounted reconnaissance and surveillance assets capture NRT information. The lack of latency provides a more recent and relevant COP to the commander, which increases the value of the contribution of the mounted reconnaissance and surveillance assets. To support the decision-making cycles of most tactical commanders latency must be minimized and fidelity must be sufficient to address IR and appropriate information according to echelon. Mounted reconnaissance and surveillance allows commanders to harness a balance of organic direct fires, line of sight (LOS) and BLOS, and joint and Army fire support capabilities.

(b) As a minimum, mounted reconnaissance and surveillance will have the following capabilities:

- Capability to provide acquisitions overmatch to the commander in worldwide conditions, available 24 hours a day, day or night, in all terrain, and under all environmental conditions.
- Capability to detect, identify, locate and track, with precision, friendly and enemy forces, neutrals, and other groups in close proximity and at stand-off distances including individual leadership figures and HVT, in a complex and chaotic urban environment.
- Capability to provide immediate, intermittent three-dimensional sensor capability to overcome restrictive terrain.
- Capability to display and record in the COP the successive positions of a moving contact.
- Capability to find, fix, track, target, and assess IEDs, weapons, munitions, and full spectrum CBRN at safe distances.
- Capability to observe and classify all facilities, fixed and mobile.
- Capabilities to collect on, observe, classify, and monitor independent events, of either human or natural sources (riots, explosions, CBRN contamination, etc.).
- Capability to detect and image activity within urban structures.
- Capability to detect sub-surface munitions, weapon systems, structures, and personnel.
- Capability to observe, collect and characterize relevant geographic, meteorological, and physical (infrastructure, natural resources) information within the AO.
- Capability to dismount for local security adjacent to the platforms, as well as reconnaissance in restricted terrain or urban environments and the occupation of dismounted observation posts, and to provide security to assigned or attached personnel.
- Capability to provide connectivity to future force elements compatible with battle command construct requirements to transmit tactical information wirelessly to the designated shooters, the battle command network, and the GIG.
- Capability to wirelessly access available tactical information from adjacent sensors across echelons, and available intelligence from the battle command network and the GIG.
- Capability of assured real time connectivity at extended ranges and non-LOS conditions while overcoming the restrictive nature of terrain and urban environments.
- Capability to access network transport services unhindered by the presence of jamming, countermeasures and adverse environmental interference.
- Capability to defeat threat counter-reconnaissance efforts with comprehensive lethality overmatch and to survive and operate in the same battlefield conditions as the supported force in all environmental conditions.
- Capability to detect, identify, and determine target location with sufficient accuracy for targeting, along with other pertinent battlefield information, and process and report the data through the network in a timely manner.
- Capability to provide target identification, rapid fusion of sensor inputs, fire control, distribution, clearance of fires and BDA procedures with minimal latency.
- Capability to provide detection, fire support, and assessment, in NRT, with every platform having the ability to be a sensor.

- Capability to produce targetable and protected target data.
- Capability to provide targetable data to joint, Army, and allied munitions to include non-precision (area), precision, precision guided and precision smart munitions.
- Capability to support virtual teaming, mutual support, and the ability to rapidly mass effects when required, and the routing and rerouting of targeting data to sensors.
- Capability to collect, collate, retrieve, disseminate, archive, and secure information and data from across all command echelons extending from MP squad level through the ASCC.
- Capability to operate in real time (minimization or elimination of latency).
- Capability to provide tactical persistent surveillance.
- Capability to provide overlapping sensor detection capability.
- Capability to provide all-weather, climate, and terrain operations, from open desert to dense vegetation, mountainous and urban locales.
- Capability to detect threat forces at stand-off distances (such as, distances beyond an adversary's engagement envelope).
- Capability to be undetectable or unrecognizable by adversary systems and capabilities.
- Capability to deploy rapidly intra-theater.
- Capability to operate with high mobility permitting access to distant, restricted, inaccessible terrains and environments.
- Capability to provide complementary assessment capability.
- Capability to horizontally and vertically fuse specific strategic, operational, and tactical sensor inputs.
- Capability to obtain early developmental situational information.
- Capability to be flexible and persistent under all environmental conditions and for extended operational periods of time.
- Capability to interact, interdict, and fight for information, allowing immediate action by the operational commander.
- Capability to detect IR that pertains directly to the operational commander.
- Capability to interact with local indigenous populations according to ROE.
- Capability to operate in close proximity, as well as from extended range, to enemy and threat forces with high fidelity and low latency.
- Capability to detect, recognize, and identify targets through a variety of spectra with high fidelity.
- Capability to produce information for the commander and analysts at an operational tempo that exceeds other intelligence-producing assets' capabilities.
- Capability to provide the tactical commander NRT information to confirm or deny the situation template and facilitate the MDMP.
- Capability to operate with assured redundancy when aerial and space-based assets are unable to achieve required fidelity.
- Capability to simulate information for the friendly strategic, operational, or tactical commander.
- Capability to maintain a system that harnesses a dynamic informational and intelligence utility that is impervious to disruptions emanating from climate, atmospheric, or enemy interference and activities.

- Capability to cross reference detainees' identity against watch lists and other informational repositories—the capability to instantly communicate findings.
- Capability to input, retrieve, and selectively disseminate information under all possible conditions.
- Capability to exercise unfettered access in retrieving and communicating information—greatly minimizing the timeline from collection to interpretation, to description.
- Capability to communicate a COP across all echelons from ASCC through squad level in NRT.
- Capability to identify suspicious persons or those intending violence from safe distances.
- Capability to identify suspicious persons from among a crowd or gathering of people from safe distances. This will enable the future Modular Force to baseline human behavior in a large population, in order to distinguish abnormal from normal behavior. This includes the capability to detect heart rate, body temperature, anatomical and other human indicators, enabling the future Modular Force to determine adversary intent.
- Capability to obtain unfettered access to relevant information portals linked with the COP under all situations in NRT.
- Capability (architecturally and systematically) to advance MP support to HUMINT in the combined application of the five basic MP functions.
- Capability to use, collate, archive, and disseminate HUMINT information, and others, collected and retrieved in the application of the five basic MP functions in a singular system or architecture or process.
- Capability to detect, identify, warn, and react to explosive hazards from safe distances while traveling at various rates of speed to ensure adequate protection of the force and to preserve combat power, momentum, and LOC needed for sustainment.
- Capabilities to detect, identify, collect, and analyze CBRN hazards from distances sufficient to avoid contamination or exposure to ensure protection of the force and to preserve combat effectiveness.
- Capability to identify detainees from the moment of capture, which, within the context of an asymmetrical threat, can occur at any location within the AOR—to safeguard and expedite the hasty evacuation and transfer of detainees linked to strategic interests (high value, and others).
- Capability to identify internally displaced persons to contrast instantly their known identity with intelligence repositories extrapolating the JIIM domains.
- Capability to battle track movement of all assigned vehicles and personnel under all types of conditions and under any threat.

(2) Dismounted reconnaissance and surveillance capability statement. The future Modular Force requires the capability to conduct dismounted reconnaissance and surveillance at the tactical and operational levels in all environments, including the JIIM environments, to ensure the success of early entry, forced entry (opposed/unopposed), shaping, decisive offense, defense, and stability operations at all echelons.

(a) Dismounted reconnaissance and surveillance capabilities are characterized and defined by personnel requirements, personnel carry capabilities, and man-portable equipment capabilities. Dismounted reconnaissance and surveillance also have the capability to fight for information and conduct counter-reconnaissance operations. Dismounted reconnaissance and surveillance personnel are capable of conducting missions in close proximity to threat and enemy forces with minimal risk of detection and a high probability of survival. Additionally, on various types of dismounted missions, reconnaissance and surveillance may be impossible due to terrain and terrain restrictions such as foliage and complex terrain may inhibit the fidelity of aerial and space-based surveillance assets. In these cases, dismounted reconnaissance and surveillance personnel are required and able to access these areas and provide information with a high degree of fidelity. Dismounted reconnaissance and surveillance capabilities are highly effective in stability operations where multi-disciplinary skill sets are used to provide the commander the most complete picture possible.

(b) As a minimum, dismounted reconnaissance and surveillance will have the following capabilities.

- Capability to deploy rapidly intratheater.
- Capability to operate in real time (minimization or elimination of latency).
- Capability to be used selectively when other strategically-oriented surveillance assets are unable to provide sufficient fidelity.
- Capability to be responsive to strategic requirements in specific IR that require the highest and most intimate degree of fidelity with the lowest degree of latency.
- Capability to provide operational commanders with IR in locations and with fidelity and timeliness that cannot be achieved by mounted ground reconnaissance/surveillance or strategic assets.
- Capability to provide exceptional fidelity and minimal latency to the operational commander.
- Capability to operate in close proximity to enemy and threat forces, as well as from extended range (beyond an adversary's engagement envelope), allowing high fidelity and low latency hindered only by the limitations of the network.
- Capability to interact with local indigenous populations according to ROE.
- Capability to possess high degrees of stealth.
- Capability to possess low signature emissions.
- Capability to observe threats and enemy forces from relatively close proximities.
- Capability to achieve mobility over terrain that is impassable by any vehicles and ensure high measures of fidelity of information not achievable by aerial and space reconnaissance/surveillance assets.
- Capability to provide the tactical commander the necessary C2 over high-fidelity and low-latency reconnaissance/surveillance capabilities that can satisfy IR.
- Capability to provide acquisitions overmatch over threat formations within restrictive, urban and "no-go" terrain, available 24 hours a day, in all terrain, and under all weather conditions. This also includes acquisitions overmatch of individual leadership figures and HVT.
- Capability to provide intermittent three-dimensional sensor capability to support fighting in urban environments.

- Capability to detect, image, and characterize activity within urban structures .
- Capability to detect, image, and characterize activity in sub-surface locations and structures.
- Capability to observe and classify all facilities, fixed and mobile (including those sub-surface and in urban areas), with special emphasis on the precursor chemicals or material used in the production of WMD. This would include surface and sub-surface toxic plumes released by the production or storage practices.
- Capabilities to observe, classify, and monitor independent events, of either human or natural source (riots, explosions, CBRN contamination, and others).
- Capabilities to observe, collect and characterize relevant geographic and physical (infrastructure, natural resources, meteorological) information within the AO.
- Capabilities to observe, collect and characterize socio-cultural and institutional data and indicators including religious, ethnic, political, economic, and physical (infrastructure, natural resources) to predictably assess the impact these spheres will/can have on planned or on-going military operations and how these links will impact other nodes and ultimately impact the identified centers of gravity at the different levels.
- Capability to employ designated sensors of adjacent, supporting platforms while remaining undetected and masked to threat forces.
- Capability to defeat threat counter-reconnaissance efforts with comprehensive lethality overmatch, to include the use of weapons from designated adjacent, supporting platforms while remaining undetected and masked to threat forces.
- Capability to see through walls and hardened surfaces to detect weapons, ammunition and explosive devices at ranges of lethality overmatch.
- Capability to detect nuclear, biological, and radiological contamination at safe distances from protected platforms or by using remotely operated sensors.
- Capability to display and record in the COP the successive positions of a moving contact.
- Capability to find, fix, track, target, and assess (engagements) IEDs and the full range of CBRN hazards at safe distances.
- Capability to provide connectivity to future force elements compatible with battle command construct requirements to transmit tactical information wirelessly to the designated shooters, the battle command network, and the GIG through supporting, adjacent platforms.
- Capability to detect, identify, mark and designate targets; establish network affiliation; determine pertinent battlefield information; and process/report the data through the network in a timely manner.
- Capability to provide target identification, fire control, distribution, clearance, and BDA procedures with minimal latency and to provide information for rapid fusion of sensor inputs through adjacent supporting platforms.
- Capability to provide fire support to joint, Army, and allied munitions to include precision engagements, brilliant and precision munitions, improved lethal and nonlethal effects, scalable munitions, and munitions utilizing in-flight corrections.

(3) MUM airborne reconnaissance and surveillance capability statement. Future Army aviation forces require the capability to conduct aerial armed reconnaissance and surveillance operations to produce actionable combat information to provide essential combat information before, during, and after combat.

(a) Army aviation core competencies are reconnaissance, attack, security, vertical maneuver, air movement, and battle command. Army aviation makes its primary contribution to the Army's ISR effort by conducting reconnaissance and surveillance. The bulk of Army Aviation reconnaissance and surveillance operations are conducted by the combat aviation brigade (CAB) with manned reconnaissance and attack helicopters and UAS. Aerial armed reconnaissance must be able to find and fix threat units, to build and share the COP tailored to air-ground team task and purpose, and to focus combat power at the decisive point at the right time. The aviation unit may conduct reconnaissance with air assets alone, (MUM or teamed) or integrated with ground maneuver units. Future Modular Force aviation units employing manned armed reconnaissance helicopters allow the maneuver commander to 'see first' with a man-in-the-loop decision maker well forward to provide proactive versus reactive decision making capability and fight for combat information regarding dispositions of enemy forces and relevant terrain to permit friendly maneuver to positions of advantage. MUM teaming increases operational effectiveness, allowing UAS to assume the dangerous, routine aviation roles while the forward decision-maker integrates and fuses information on-scene and synchronizes the combat actions of the combined arms air-ground team. MUM synergy allows manned platforms to focus on battlefield requirements while UAS add sensors, fires, and protection to the effort.

(b) Aviation provides reconnaissance and surveillance to enable the joint commander to extend tactical reach, negate effects of terrain, seize key nodes, attain surprise, and dislocate or isolate enemy forces that are in contact or in imminent contact. Aviation provides reconnaissance to enable exposure of the entire enemy area to direct attack, separate enemy elements, prevent massing, and deny enemy reinforcement. Army aviation conducts reconnaissance and surveillance in order to find and fix threat, assist in building and sharing the COP tailored to the air-ground team task and purpose, and to focus combat power at the decisive point at the right time. Aviation forces conduct security operations to provide reaction time, maneuver space, and protection to air-ground maneuver. They participate in decisive, integrated air-ground operations, conduct close combat attack in support of ground maneuver elements and provide both direct access to joint and Army fire delivery systems and provide and or integrate close air support on demand.

(c) Army aviation operates aircraft at extended range, conducts Level IV interoperability of UAS from attack and reconnaissance helicopters, provides capability for networked links to other joint and Army fires and ISR assets and conducts interdiction attack and mobile strike operations. Army aviation combines ground based fires to attack aviation, unmanned systems, and joint assets to mass effects, in order to isolate and destroy key enemy forces and capabilities and to shield friendly forces as they maneuver out of contact. Aviation reconnaissance and attack helicopters and UAS with advanced target acquisition sensors provide the capability to identify targets and perform reconnaissance at survivable standoff. CAB UAS provide extended time on station RSTA, persistent stare and wide area surveillance. The CAB's armed reconnaissance, attack helicopters, and UAS provide lethal overmatch against the anticipated

target set by employing extended range weapon systems to enable survivable standoff from threat.

(d) Aerial surveillance conducted by UAS operating either autonomously or teamed with manned aircraft, provide long dwell, tactical persistent surveillance in support of the commander's PIR. UAS assigned to future Modular Force aviation forces must be capable of systematically observing geographic areas, facilities, and mobile forces with the ability to observe specific NAI and TAI continuously or with persistent stare. These systems must be capable of ranging any point within the division AO and provide a minimum of 24-hour continuous observation in complex terrain. LOI 4 is required for MUM teaming, and the systems also require the capability for ground-air teaming. Sensor systems must be responsive and capable of dynamic re-tasking in real time. They must provide a capability to perform wide area search to cue other sensors, conduct emitter mapping, EA, meteorological survey, long endurance wide area surveillance, and wide-band communications relay.

(e) Future MUM teaming aviation reconnaissance and surveillance will have the following capabilities.

- Capability to utilize the COP in performing reconnaissance and surveillance operations and quickly report the information in COP-compatible formats.
- Capability to conduct security operations in a traditional cavalry role with ground maneuver forces to provide reaction time, maneuver space, and protection to the air-ground maneuver team.
- Capability to conduct decisive, integrated air-ground operations, and close combat attack in support of ground maneuver elements as they close with and destroy the enemy.
- Capability to identify, mark, and designate targets and perform reconnaissance at survivable standoff and be capable of providing mutually supporting fires to each other and to supported ground elements.
- Capability to exercise LOI 4 while operating in a teaming arrangement with UAS in order to control and dynamically task UAS and their payloads.
- Capability to network to other joint and Army fires and ISR assets, and be able to provide and integrate close air support on demand.
- Capability to reliably and routinely access a continuously updated collaborative information environment, and be capable of routinely teaming manned with unmanned platforms that can provide intelligence and targeting information as well as BDA.
- Capability to conduct EA from a UAS.

(f) The BCT will have the following capabilities.

- Capability to employ unmanned robotic, remotely operated ground and aerial sensors without degrading onboard sensors and weapons capability while on the move.
- Capability to conduct one-man operation of robotic, unmanned, and remotely operated sensors.
- Capability to launch and recover on the move.

- Capability to be tamper-resistant.

(4) Space-based reconnaissance and surveillance capability statement. The future Modular Force requires the capability to utilize space-based ISR at all levels and in all environments, including the JIIM environments, which provides the ability to detect changes in threat posture, monitor weather conditions, track equipment and monitor facilities at all echelons worldwide.

(a) Space-based reconnaissance and surveillance have long been significant enablers of land force operations and their roles in future force operations will continue to expand. Space-based reconnaissance/surveillance systems supporting the future Modular Force will grow from a predominately strategic infrastructure at the national level, to a layered infrastructure designed to support the strategic, operational, and tactical levels with responsive launch capabilities and high altitude platforms and payloads. Strategic space-based systems will continue to provide GEOINT (to include IMINT), SIGINT, and MASINT on a global basis. Rapid collection, processing, and dissemination systems will provide reconnaissance and surveillance information and intelligence via the GIG in NRT. Operationally responsive launch capabilities with tailorable payloads will provide a theater-focused reconnaissance and surveillance capability. Rapid reallocation and re-tasking will significantly increase a theater commander's ability to see the battlefield. In the past, tactical reconnaissance and surveillance was limited to terrestrial and aerial operations. In the future, a layer of high altitude long endurance platforms with a variety of payloads will bring the power of space to the tactical warfighter. These non-orbiting systems will enable persistent, wide area, and long range reconnaissance and surveillance. The power of space is not limited to friendly forces. Because of the significant increase in foreign military, civil, and commercial space operations, threat forces will also enjoy the power of space-based systems. The future Modular Force requires the capability to reconnoiter and surveil the skies to track and assess the activities of threat and non-aligned space-based assets.

(b) The following space-based and space-enabled capabilities are required to support the reconnaissance and surveillance operations of the future Modular Force.

- Capability to provide the space and high altitude long-endurance platforms, links and processors to enable the fusion, sharing, push, pull and update information from a wide variety of sensors and sources in all domains, access that information simultaneously from multiple non-contiguous locations in order to provide timely, relevant information in support of the planning, execution and assessment operations of the JF and component commanders.
- Capability to rapidly process ISR information and data to be of value to decisionmakers and commanders.
- Capability to provide space-enabled, persistent imagery and SIGINT surveillance.
- Capability to enable the rapid collection and dissemination of intelligence.
- Capability to enable the rapid reallocation and re-tasking of surveillance assets.
- Capability to cross-link information and cue complementary aerial systems.
- Capability to provide improved real time, or NRT space-based ISR, on-board sensor processing and direct downlink to supported ground systems.

- Capability to dynamically task and re-task space and high-altitude long-endurance assets in support of JFC objectives.
- Capability to rapidly obtain the needed data and transfer to the proper location in such a way as to avoid information overload.
- Capability to provide full spectrum dominance of space, to include unrestricted access to space-based communications, ISR, weather, terrain and environmental monitoring, position, navigation and timing, and the ability to deny these options to the enemy at the time and place of our choosing.
- Capability to establish early and sustained control of the space domain to enhance joint-integrated IO in all operational environments and condition.
- Capability to rapidly downlink, process, and analyze national and commercial imagery from archive and databases in theater.
- Capability to rapidly obtain the needed data and transfer to the proper location in such a way as to avoid information overload.
- Capability to cross-link information and cue complementary aerial systems such as UAS.
- Capability to provide high-resolution geospatial data and comprehensive environmental information, including real time collection, in order to visualize and describe the operational environment and then assess the impact of terrain, atmosphere, weather, and space observables in all operational environments and conditions.
- Capability to rapidly identify the locations of friendly and enemy forces.
- Capability to rapidly assess effects to friendly systems and determine if it is the result of friendly or enemy action.
- Capability to identify enemy application of asymmetric weapons or efforts.
- Capability to exploit national and strategic systems for tactical needs.
- Capability to conduct long-loiter reconnaissance.
- Capability to rapidly exploit HSI and MSI to detect and defeat improved camouflage and obscurants, the presence of biological or chemical agents, and other signs of tampering, sabotage, enemy presence, detection of changes in ground reflectance, elevation, industrial emissions, crop types, thermal characteristics of buildings or areas. Provide detection of IED, UXO, and non-explosive obstacles with change detection capability. Provide urban environment detection capabilities to identify threats based on civil activities.
- Capability for strategic space-based systems to provide GEOINT, SIGINT, MASINT, and weather on a global basis.
- Capability to rapidly collect, process, and disseminate reconnaissance information and data intelligence via the GIG in NRT.
- Capability to cue and cross-cue a variety of sensors to enhance the reconnaissance data available to the commander.
- Capability to provide operationally responsive launch with tailorable payloads to provide a theater-focused reconnaissance capability.
- Capability to rapidly reallocate and the ability to re-task will significantly increase a theater commander's ability to understand the activities of the threat, its resources, and the natural environment.

- Capability to employ a layered infrastructure that brings space-based reconnaissance to the tactical level.

(5) Reconnaissance and surveillance sensors capability statement. The future Modular Force requires the capability to conduct sensing operations covering all aspects of battlespace observation including, but not limited to atmospheric (weather) sensing (tactical level), target identification and observing operations using both active and passive means at all levels, in all environments (including the JIIM environment), and at all echelons.

(a) Future Modular Force sensor capabilities will see continual improvements in sensor science along with creative utilization of yet-to-be-applied technologies. Although Army sensor use is currently at an all-time high, increased application of technologies and innovative thinking promise to bring newer and more reliable capabilities into the sensor arsenal. Ideally, new sensor systems will utilize stand-off, remote sensing capabilities designed to detect things never before considered possible. For example, remote sensing of a complete suite of weather conditions at horizontal and vertical ranges well beyond five kilometers. Even more promising is the development of stand-off sensing capabilities to detect human biometric parameters (such as, heart rate and heart rate changes, personnel temperature and temperature fluctuations, perspiration rates, rapid or erratic eye movement, and others) that may preclude individual hostile intent. Continued development of see-through-the-wall technologies are also a vital part of these stand-off sensing capabilities. Development of reliable subsurface void detection capabilities and active digging or use activities will enhance security around secure facilities, to include national borders.

(b) Future Modular Force sensor capabilities include the following.

- Capability to detect and locate targets within parameters of the target selection standards, based on ROE and the target's environment, so the desired effects can be delivered to a precise location at the correct time.
- Capability to employ the appropriate strategies, numbers, and types of weather sensors along with required sensor placement and maintenance for area-specific employment of required weather sensing capabilities.
- Capability to develop and field adequate sensing capabilities at all levels.
- Capability to employ improved unattended ground sensor power-supply capabilities for extended periods of operation especially in deep employment scenarios (extended range and application).
- Capability to determine what is happening on a nation's borders (the first step towards establishing a nation's sovereignty) in order to interdict illicit activity and contraband in a counterinsurgency setting.
- Capability to provide enhanced SA through tactical persistent surveillance via economy of force measures (for example, not having to use Soldiers in unlikely avenues of approach or place them in extreme danger).
- Capability to employ tactical unattended ground sensors in a peer-to-peer network between its nodes, and complete compatibility with all future Modular Forces.

- Capability to operate ground sensors within an urban environment, and CBRN sensors with nested, remotely programmable, and extended operational life and capabilities.
 - Capability to provide state-of-the-art sensor support for all MP operations.
 - Capability to recruit and train the appropriate number of personnel to effectively field, operate and maintain these sensors (at all levels).
 - Capability to develop and field adequate sensing capabilities at the operational and tactical levels (stand-off observation capabilities).
 - Capability to create and maintain an ongoing research and development endeavor with emphasis on an entire spectrum of remote sensing capabilities (i.e., biometrics and weather applications, see-through-the-wall capabilities).
 - Capability to incorporate vital sensed data into NRT COP products.
 - Capability to develop common methodologies and strategies for all sensor emplacement, application and processing.
 - Capability to develop plug-and-play sensors dependent on the theater and the unique requirements of the operational environment, in order to facilitate the incorporation of emerging sensor capabilities.
 - Capability to conduct a multi-discipline signature survey of the operational environment. This includes the ability to network sensors to ensure optimized sensor coverage to meet mission requirements.
 - Capability to evaluate sensor effectiveness; improve or replace deployed sensors, and or develop new ones; and make the sensor network more robust (types, placement, numbers) based on evolving operational requirements.
 - Capability to synchronize and exploit the employment of multi-discipline intelligence sensors against a specific target or target set (individual object, system, or network) in order to maintain sensor contact with the target as environmental constraints or the target's behavior dictate, and gain a greater understanding of all aspects of the target, in all operational environments (to include large gatherings).
-

Chapter 6

DOTMLPF Implications and Questions

6-1. Doctrine

- a. Are space operations adequately addressed in Army doctrine for the theater, corps, and division doctrinal publications that are related to ISR?
- b. Are current TTP adequate to execute ISR related Army space operations?
- c. Do proponent doctrinal publications integrate requisite Army space operations into the ISR construct?
- d. What emerging space technologies, processes and capabilities need to be codified in Army doctrine to ensure everyone who uses space based capabilities in support of ISR operations are able to adapt their own doctrine to assimilate any new processes from the space community?

e. Is current joint and Army doctrine adequate to mandate/regulate common sensing structure, development and application across the JIIM environment?

f. What doctrinal changes are needed to support future force ISR? The Army needs to determine changes needed to ISR synchronization doctrine, determine doctrinal changes needed to support fusion and analysis, and determine doctrinal changes needed to support counter-ISR campaigns.

g. What is the appropriate sensor mix (for example, ground, air, and multidiscipline) at each echelon to collect across the full spectrum of operations? The Army must determine the best methods to conduct cooperative sensor employment, develop doctrine, TTPs, and concepts for cooperative sensor employment, develop network design to allow for efficient, effective cooperative employment, and determine what reliance should be placed on JIIM sensor capabilities at ASCC, corps, division and brigade to exploit coverage gaps.

h. How will disparate forces, based on different doctrines share an applicable and cross-functional COP?

i. What doctrinal compromises or common ground must be developed for current, future, modular, joint and coalition forces to operate reconnaissance assets concurrently?

j. When one organization is optimized for standoff engagements and another is optimized for close combat, and they have to operate together in tandem, how will one's reconnaissance satisfy the IR of both organizations?

k. How will command structures be required to adapt reconnaissance operations, based in individual organizational doctrine, to interoperate tactically, operationally, and strategically? Can and should these adaptations be standardized?

l. Can a ground reconnaissance 100-series field manual be created to provide common reconnaissance understanding to commanders of all types of forces?

m. How will mixed formations of current, modular, and future forces be organized for combat and interoperate over different areas of interest (in terms of IR and area of operation size)?

n. What doctrinal changes are required to support employment of Army ISR assets in CONUS in support of HD and CS operations?

o. What doctrinal changes are required to support Army ISR interoperability with non-DOD Federal agencies and state, local, tribal and private organizations involved in HD and CS operations?

6-2. Organization

a. Are current Army space organizations adequate to meet the space operations requirements of the future Modular Force in the execution of ISR mission and support?

b. Is a new organizational structure required to achieve these required capabilities? Assessments are needed to determine if the organization design can really support the concepts and systems envisioned for the future Modular Force.

c. What Army ISR capabilities should reside in tactical and operational forces in order to ensure all are being applied during the planning, preparation, and execution of ISR operations? The Army must determine the degree to which fully autonomous, semi-autonomous, and computer-assisted operations will support sensed ISR within the future Modular Force, and determine to what level sensor reports will be fused at the platform level.

d. What joint or Army organization is responsible for fusing emerging technologies and processing capabilities to ensure compatibility, commonality, and availability (fusion) of sensed data?

e. What ISR future Modular Force capabilities are needed at each echelon?

f. What concepts, systems, and organization will potential adversaries develop to thwart or adapt to U.S. ISR superiority?

g. What is the best design for future Modular Force ISR fusion architecture? The Army must determine the functions required of the future Modular Force ISR collection architecture to meet emerging threat signatures and technical developments within the collection community.

h. What office is responsible for coordinating ISR fusion efforts for the future Modular Force?

i. Who controls (requirements, assets and mission management) UAS on ISR missions?

j. Identify or create decision-making tools and methods that assist future commanders in determining the best balance between centralization and decentralization based on mission and situation.

k. What proponent(s) or entity(ies) will direct future ISR collaboration, integration, and synchronization?

l. What organizational configurations will sufficiently enhance persistence, lethality, and mobility while satisfying the commander's IR?

m. What organizational configurations will be most capable of intra-theater deployments, joint, and inter-operable modularity?

- n. What information and intelligence latencies will take place between forces and what interoperability challenges will result?
- o. What reconnaissance interoperability challenges will exist between current force, future force, modular force, joint and coalition organizations?
- p. What is the right mix of ISR formations and capabilities at each echelon (battalion through division and echelons above division)?

6-3. Training

- a. How is the integration and application of space power included in current training and leader development?
- b. How can the Army adapt its training to better integrate space and ISR operations?
- c. How will evolving technologies and ongoing consolidation of ISR capabilities and or planned changes in organization affect the ways in which Army units and leaders operate and what are the training implications of these changes to support all Army ISR operations?
- d. How will evolving ISR doctrine impact units and leaders?
- e. What training designs will develop units' and leaders' ability to capitalize on the full range of ISR capabilities?
- f. What are the ISR training requirements for enlisted personnel, non-commissioned officers, warrant officers, officers, contractors, and DA civilians? What are the ISR sustainment training requirements for enlisted personnel, non-commissioned officers, officers, contractors, and DA civilians?
- g. What are the ISR doctrine, tactics, and techniques sustainment training requirements for enlisted personnel, non-commissioned officers, warrant officers, officers, contractors, and DA civilians?
- h. What type, scope, and frequency of Army ISR training must the future Modular Force conduct to enable effective operations?
- i. What ISR test and training ranges are necessary?
- j. What modeling and simulations (M&S) are required to support Army ISR operations at the tactical, operational, and strategic levels?
- k. What cross-force training will be required of Soldiers assigned to modular force units?
- l. What critical institutional training from future forces will need to be integrated into modular and current forces?

m. What training is required to ensure Army ISR supporting HD and CS operations is interoperable with the lead federal agency, other non-DOD federal agencies, and state, local, tribal, and private organizations?

6-4. Materiel

a. What space-based military satellite communications relay systems are needed for the future Modular Force to ensure units conducting ISR operations will be able to communicate with their higher HQ who will most likely be BLOS or over the horizon?

b. What space-based ISR assets are necessary to support future Modular Force full spectrum operations?

c. What is the role of commercial space-based systems in ISR?

d. What ground terminal systems are needed?

e. What space-based early warning detection, assessment, and dissemination systems are needed for the future Modular Force?

f. What space control systems are needed to meet the ISR requirements of the future Modular Force?

g. What high altitude assets are needed and what is the role of these systems in providing dedicated and persistent surveillance support to the warfighter?

h. How will space-based systems and terrestrial nodes enable multi-echelon and multidimensional ISR, fires, and maneuver that are fully networked?

i. What are the space-based systems required to support the expanding role of unmanned systems on the battlefield?

j. What space-enabled sensor-to-shooter linkages are needed to support future Modular Force full spectrum operations?

k. How will space-based systems enable dominant situational understanding?

l. What new sensors/sensor schemes or strategies need to be developed?

m. What sensor design, processing, dissemination capabilities and sensor mix are needed to accomplish integrated ISR efforts allowing the commander to see first?

n. How should the Army fuse ISR sensor data and information into a standardized data base to make the operational picture relevant, timely, and accurate?

- o. What are the capabilities, functionality and components required to enable the commander to see first?
- p. How can collection management tools can be embedded in operational planning tools and which sensors can be multi-purpose platforms?
- q. Which ongoing scientific efforts would, if successful, fundamentally alter future force concepts? The following concerns should be addressed when answering this question: determine which technologies will be able to provide solutions; determine the invention path needed to mature those technologies; build a technology roadmap integrating needed resources; and forecast the impact on ISR operations realized by these advances in technology and capability.
- r. What target development and BDA tools are required at each echelon to meet timeliness, accuracy and relevancy demands?
- s. Can multi-spectral signature reducing technologies effectively enhance persistence of mounted and dismounted ground reconnaissance forces?
- t. Can enhanced lethality capabilities improve ground reconnaissance force fight-for-information abilities?
- u. Will leveraging multi-spectral sensor capabilities enhance ground reconnaissance forces' abilities to answer IR and improve persistence?
- v. Will current, near-term, or future communications capabilities sufficiently minimize or eliminate latency?
- w. How will current forces communicate digitally and compatibly with future forces?
- x. Will current and modular forces be able to conduct digital collaboration with future or coalition forces?
- y. Will current, near-term, or future mounted and dismounted reconnaissance materiel assets be capable of rapid intratheater deployment?
- z. Will current or future mounted and dismounted assets have required terrain access capabilities to answer strategic, operational, and tactical commanders IR with high-fidelity and low-latency?
- aa. What complementary systems can be implemented to ground reconnaissance in urban settings?
- bb. Will future force acquired data be able to be displayed in current and modular force tactical operations center and displays?

cc. What new ISR collection, processing, analysis and reporting systems are required to ensure interoperability with/support to the lead federal agency, other non-DOD federal agencies, and state, local, tribal and private organizations in HD and CS operations?

6-5. Leadership and Education

a. How can we develop more adaptive space savvy leaders in order to ensure that all echelons of command are capable of integrating space based capabilities into the conduct and execution of ISR operations?

b. How do we provide world-class leader development in the area of ISR operations?

c. How do we develop leaders ready to deal with the complexity of ISR, its associated operating environments, and interagency implications in order to ensure that all leaders understand that ISR capabilities are few and their requirements are many?

d. What ISR leader development programs are needed in officer education system, warrant officer education system, and noncommissioned officer education system?

e. Can leaders be trained to employ successful terrain management in all potential scenarios from conventional fights to asymmetric fights to complex web-defenses?

f. Can leaders be trained to synergize all applicable information collection sources successfully?

g. Can leaders be trained to successfully and appropriately leverage required effects to obtain IR and meet commanders' intents?

h. How can leaders, at all operational and tactical echelons of command, develop sound judgment to adapt reconnaissance organizational structure and leverage appropriate assets according to the mission and environment?

i. What leader development programs are required to ensure Army ISR assets used in CONUS in support of HD and CS operations are used effectively, efficiently, and legally?

6-6. Personnel

a. Are there sufficient ISR staff and capabilities in the support brigades?

b. What is the strategy for developing ISR reachback capabilities to reduce forward footprint?

c. Will future Modular Force ISR personnel requirements be met and managed by a consolidated manpower organization?

- d. What skill sets are required to conduct ground reconnaissance in conventional, asymmetric, urban, and complex-terrain operations?
- e. What skill, cognition, and experience sets are required of staff members and commanders who plan reconnaissance?
- f. How will officer career maps accommodate professional development on ISR operations (such as, promotions, rewarding and career-enhancing ISR assignments)?
- g. Will creating a warrant officer military occupational specialty MOS with incentive pay provide the stable career path to maintain technical expertise?
- h. Will filling technical positions with U.S. Army Reserve and Army National Guard Soldiers provide the stability and skill sets to meet the future demands of ISR analysts?

6-7. Facilities

- a. Are there adequate facilities available to Soldiers, leaders, battle staffs, non-uniformed personnel, and units to attain and maintain acceptable levels of ISR training effectiveness?
- b. What infrastructure is required at forts and installations to adequately support ISR in both training and operational constructs consistent with Army, joint and multinational concepts?
- c. What infrastructure is required in theater to support Army ISR operations missions?
- d. What facilities are needed to support ISR special access programs?
- e. What installation infrastructures are needed to support home station space operations functions?
- f. What facilities/infrastructure are required to consolidate ISR capabilities for the future Modular Force?
- g. What range and simulation facilities are required for new aerial and digital reconnaissance capabilities to be used by ground reconnaissance forces?

Chapter 7 Risks and Mitigation

7-1. Risks

- a. Currently, there are no U.S. Army or joint documents that provide a concept for integrated and synchronized Army ISR operations. This CCP is the first Army-specific document that attempts to provide a concept for integrated ISR operations. There are many concepts referenced in the development of this document. The references in Appendix A detail the numerous

capabilities researched and the mission areas that were studied either prior to or during the formulation of this CCP.

b. This CCP discusses ISR support to the full range of military operations. Future adversaries will exploit every conceivable capability to keep the U.S. from achieving its military, economic, diplomatic, and political objectives. It is conceivable, even likely, that adversaries will adopt capabilities and tactics unimagined by the U.S. and its allies. This CCP does not attempt to address every contingency, branch, or sequel. Rather, it strives to identify capabilities across the DOTMLPF domains that are adaptable and tailorable to the broadest possible range of threats the United States and its allies might face in 2015-2024.

c. Chapter 1 identified several imperatives that are germane to the discussion of risk. If unfulfilled, these imperatives will not cripple the future Modular Force, but will impede the commander's ability to achieve information superiority. Timeliness, accuracy, and adequacy of intelligence and combat information enable the future Modular Force's SA.

(1) Provide the commander with information that rapidly answers IR. Persistent, low latency, and high fidelity flow of information ultimately leads to information superiority

(2) Facilitate synchronization and integration of ISR operations and capabilities in full spectrum operations at all echelons

(3) Maximize current ISR capabilities and create functional linkage to emerging capabilities

(4) Deliver ISR capabilities that address requirements and priorities by influencing the design of ISR systems and payloads to expedite the transformation of information into intelligence; prevent adversary surprise of U.S. and friendly forces; support decisive full spectrum operations; and facilitate the agility and speed required to dominate full spectrum operations.

7-2. Mitigation

a. The Army is pursuing the most comprehensive transformation of its forces since the early years of World War II. This transformation is happening while the nation is at war. The urgency of supporting the current fight blurs the usual dichotomy between the current and future Modular Force. The Army must seek to accelerate inculcation of select future Modular Force capabilities into the current force to support today's fight, while simultaneously ensuring that today's lessons learned are applied to future Modular Force developments and timing. This transformation encompasses more than materiel systems. Adaptive and determined leadership, innovative concept development and experimentation (CD&E), and lessons learned from recent operations produce corresponding changes in the DOTMLPF domains. Experimentation, wargames and experience are the methods the Army uses to mitigate risk while considering and improving capabilities for the future Modular Force.

b. Experimentation. Experimentation is the process of exploring innovative methods of operation to access feasibility, evaluate utility, and or determine limitations of the concepts being explored. Experiments conducted in support of JCIDS efforts use the 2015–2024 timeframe. The Army also conducts wargames using futuristic scenarios (15 to 20 years and beyond) to explore concepts in order to better define which of those concepts should be the subject of experimentation. Army experimentation is usually conducted in the form of discovery (usually in a constructive M&S environment), hypothesis (also in an M&S environment but with human in the loop role players) and demonstration (live or simulation) settings.

(1) Discovery experiments are designed to inform a concept. The setting tends to lack the degree of control necessary to infer cause and effect.

(2) Hypothesis testing experiments are the traditional type used by individuals to build, confirm and advance knowledge. This occurs by seeking to falsify specific hypotheses (specifically if...then statements) or discovering their limitations. In order to conduct hypothesis-testing experiments, the experimenter shall create a situation in which one or more factors of interest can be observed systematically under conditions that vary the values of factors thought to cause change in the factors of interest – while other potentially relevant factors are held constant.

(3) Demonstration experiments are used to display knowledge and the settings tend to be somewhat orchestrated. Often times the Army uses this method to display prototypes of emerging technologies that are nearing maturity and are potentially ready for fielding to the force.

c. M&S. M&S is often called upon to make an informed assessment. Scenarios or vignettes are built to look at one or more sets of conditions that will best help to evaluate these hypotheses, but the raw data is often not conclusive or requires reasoned review by seasoned subject matter experts to confirm the reliability of these simulation or modeling efforts.

d. CD&E. CD&E is fundamentally a risk reduction activity; failure to conduct effective CD&E significantly increases developmental risk for the future Modular Force and operational risk to the current force. Specific actions are required to reduce operational risk to the current force and developmental risk for the future Modular Force.

(1) Operational risk to the current force. Increase the capabilities of the current Modular Force through prototype experiments that test the compelling solutions and develop DOTMLPF capability packages to support the spiraling forward of future Modular Force capabilities to satisfy critical current force operational needs

(2) Developmental risk for the future Modular Force. Reduce future Modular Force development risk by developing concepts and capabilities that meet the needs of the future JFC through rigorous CD&E.

(a) Army efforts. Army wargaming and experimentation to support this CCP for Army ISR operations and its impact on DOTMLPF sets will be developed and studied using approved

defense planning scenarios and vignettes. If required, other scenarios and vignettes may be recommended or other methods found to evaluate aspects of ISR operations. Experimentation will help define how the capability requirements, outlined in chapter 5 of the CCP, can best be implemented.

(b) Joint efforts. Joint wargaming and experimentation will also support this CCP. Active participation in other Service as well as joint events is critical to the full assessment of the Army's DOTMLPF solution sets. Army ISR organizations and operations will be tested, evaluated and modified as conditions (for example, scenario, vignette) change during experimentation. Scenarios and vignettes selected for experimentation will provide an illustration of how Army ISR organizations will conduct or support operations throughout the deployment cycle while supporting the full spectrum of conflict.

e. Wargaming. Wargaming is a process of discovery and assessment—discovering insights into Army ISR and assessing the validity of strategic visions and emerging concepts—while looking 20 to 30 years into the future. Wargaming begins by attaining operational research on future warfighting systems and concepts and applying them to simulated military operations in order to prove or disprove visionary ideas and to discover gaps and seams in future ISR operations. Wargaming examines Army functional concepts of *Command, See, Move, Strike, Protect, and Sustain*, the results of which inform experimentation and eventually informs the development of Army ISR concepts, TTPs, architectures, and future systems. Wargaming personnel lead participation in Army and Joint wargames to integrate Army ISR capabilities, concepts, and visions into wargame scenarios, orders of battle, force laydowns, and computer simulations.

f. Studies. Mounted and dismounted ground reconnaissance studies have determined three general misconceptions and a conceptual reality. There is a misconception that reconnaissance is primarily an intelligence operation. This misconception directly supports the misconception that commanders do not plan nor manage mounted and dismounted ground reconnaissance at the operational level. The third general misconception is that reconnaissance is most effective and successful when conducted with stealth to avoid contact. The conceptual reality is that reconnaissance is a tactical combat operation that requires constant adaptation in all possible environments.³

(1) Though generally considered an intelligence operation, ground reconnaissance is most successful when regarded and planned as a tactical combat mission for the purpose of collecting intelligence. The 1987 Rand Study on reconnaissance conducted at the National Training Center (NTC) revealed that 69 percent of task force missions were successful when reconnaissance was successful and only 8 percent of task force missions were successful when reconnaissance failed.⁴ The current high mobility multipurpose wheeled vehicle (HMMWV)-based ground reconnaissance unit, the battalion scout platoon, possesses virtually no firepower or armor protection. This organization may be required to penetrate enemy defensive screens and avoid enemy main body elements and obstacles. Light skinned ground reconnaissance elements

³ Glenn, R.W., Medby, J.J., Gerwehr, S., Gellert, F., & O'Donnell, A. (2003). Honing the keys to the city: Refining the United States Marine Corps reconnaissance for urban ground combat operations. Rand National Defense Research Institute.

⁴ Duncan, S.C. (1994). Seven years after: Has task force ground reconnaissance improved since the Rand Study? Fort Leavenworth, KS: U.S. Army Command and General Staff College.

are at high risk of destruction when operating in areas occupied and defended by the enemy. At NTC rotations since 1987 ground reconnaissance elements lost half or more of their reconnaissance teams in 54 percent of all missions and 58 percent of the destruction and loss was due to enemy direct fire. During Operation Desert Storm only 13 percent of ground combat units used HMMWV-only platoons while 87 percent used either all tracked vehicles or a combination of HMMWVs and tracks because of the HMMWV's limited survivability, lethality, and mobility.⁵ Commanders must plan and conduct reconnaissance as a tactical combat mission in order to mitigate risk and to ensure success.

(2) Operational commanders and their staffs must plan and conduct effective ground reconnaissance in order to achieve success in combat. Doctrinally, reconnaissance is the product of the collaborative efforts of the operations and intelligence staffs. The results of many unsuccessful NTC rotations reflect trends by many units to empower the intelligence officer to plan and conduct reconnaissance operations. However, this tendency to disengage the commander and operations officer from the reconnaissance planning process results in the following negative aspects of reconnaissance operations.

- (a) The reconnaissance and surveillance plan is an intelligence shop only product.
- (b) The reconnaissance and surveillance plan is an afterthought.
- (c) The reconnaissance and surveillance plan is not designed to answer the commanders' PIR.
- (d) Poor infiltration planning of the ground reconnaissance elements.
- (e) Task forces unaware of the brigade's intelligence collection plan.
- (f) Information dissemination within the tactical operations center needs improvement.
- (g) Establishing trigger lines which will move the scouts once contact by the main body has been made.⁶

(3) Ideally, reconnaissance units use stealth and avoid physical contact with the enemy. In this manner, units may gather information by quiet and deliberate techniques without an enemy's knowledge while maintaining surprise. However, exclusive use of stealth is not always practical and historically the best way for reconnaissance units to obtain information requires combat operations. Reconnaissance by fire and reconnaissance in force are examples of such combat operations. Enemy contact and resultant actions can produce vital information concerning an enemy's capabilities, intentions, and structure. Such information development represents the fundamental difference between reconnaissance and surveillance. Commanders must plan reconnaissance operations with stealth and combat in mind. Reconnaissance involves actively collecting data while surveillance depends heavily on the activity of the enemy to collect

⁵ Sanderson, J.R. (1996). Running blind in the desert: How the USU.S. Army can improve its reconnaissance planning and execution at the National Training Center. Fort Leavenworth, KS: USU.S. Army Command and General Staff College.

⁶ Running blind in the desert.

information. If the enemy chooses to remain passive, the effectiveness of surveillance may be degraded. Ground reconnaissance elements must operate in areas occupied and defended by the enemy to develop information about the enemy.⁷ Pure stealth requires ground reconnaissance elements to maneuver in ways that avoid the enemy, requires the enemy to fail in counter-reconnaissance, and it essentially surrenders reconnaissance elements' initiative to the enemy without adequate protection, lethality, or preparation.⁸ While various studies conducted at the NTC empirically suggest that deliberate or reckless ground reconnaissance engagements with the enemy are the cause of high reconnaissance losses and greatly endanger the success of the mission, actual combat experience offers a different perspective. In 1952 the Armor School conducted over 300 interviews with World War II and Korean War reconnaissance veterans. The results indicated that the veterans' training included the use of stealth as the preferred method of reconnaissance but in combat units had to fight for information.⁹ Reconnaissance operations depend upon stealth to achieve surprise and to determine the nature of an enemy force. Stealth therefore causes a desired effect on the enemy. However, pure dependence on stealth for reconnaissance operations may not provide commanders with accurate enemy information which may be obtained through enemy contact and combat operations.¹⁰

(4) The urban environment demands almost constant creative adaptation due to its inherent character, compression of space and related close proximity of participating parties. Less important than finding the optimum tactic, technique, or procedure is the creation of individual, group, or families of TTP that can be molded to meet specific situational needs. Urban operations are manpower-intensive and the character of the environment makes them casualty-intensive. Advantages in stealth that fewer numbers of ground reconnaissance elements and members bring may be offset or compromised by sacrifices in load-carrying capability, security, and the ability to defend the team. Ultimately, the ground reconnaissance teams should be sized and configured according to the mission in urban operations as well as all other reconnaissance operations.¹¹ Additionally, technological advantages that enhance ground reconnaissance capabilities in conventional warfighting are limited by the physical and human terrain. As a consequence, the urban environment requires that reconnaissance be conducted in adaptive "layers" of conventional integrated reconnaissance capabilities, ground reconnaissance capabilities, with both conventional forces and SOF.

(5) Other complex terrains require adaptation of TTPs to retain initiative and to shape operations. Complex terrain such as mountainous, jungle, or urban include threats that are indigenous to the area and do not fight conventionally. SA is complicated because of terrain complexity and threat manipulation of terrain to friendly forces' disadvantage. Predominant reliance on aerial reconnaissance, radio intercept, and agent reconnaissance is not always successful in producing meaningful tactical intelligence in complex terrain as the Soviets discovered during their occupation of Afghanistan from 1978 to 1989.¹² Dismounted

⁷ Running blind in the desert.

⁸ Running blind in the desert.

⁹ Hickey, C.M. (1997). Heavy brigade offensive reconnaissance operations: A systems perspective. Fort Leavenworth, KS: U.S. Army Command and General Staff College.

¹⁰ Running blind in the desert.

¹¹ Glenn, R.W., Medby, J.J., Gerwehr, S., Gellert, F., & O'Donnell, A. (2003). Honing the keys to the city: Refining the United States Marine Corps reconnaissance for urban ground combat operations. Rand National Defense Research Institute.

¹² Nawroz, M.Y., & Grau, L.W. (1995). The Soviet war in Afghanistan: History and harbinger of future war? Military Review, September/October. Retrieved 1 Nov 2007 from [http://www.smallwars.quantico.usmc.mil/search/LessonsLearned/afghanistan/warraf\[1\].asp](http://www.smallwars.quantico.usmc.mil/search/LessonsLearned/afghanistan/warraf[1].asp).

capabilities, to include sensors, are highly useful in such terrains to access difficult locations and collect information.¹³ Mounted capabilities are also useful in dominating terrain and in providing firepower to successfully conduct reconnaissance by fire and shape the operation.¹⁴

7-3. Past and Future Experimentation and Wargames

a. TRADOC and its proponent schools have conducted extensive experimentation that has implications on the ISR CCP. The following is a list of major experiments and wargames conducted over the last two years involving ISR.

- (1) Long-Range Ground Reconnaissance Study 2005.
- (2) Prototyping Rock Drill II February 2005.
- (3) Division ISR Computer-Assisted Map Exercise (Collection Management) April 2005.
- (4) Division ISR Staff Exercise, July 2005.
- (5) Fusion Workshop Phase II, November 2005.
- (6) Unified Quest, 2006.
- (7) Joint Expeditionary Force Experiment, 2006.
- (8) Distributed Common Ground System-Army Excursion, January 2006.
- (9) Requirements Seminar, November 2006.
- (10) Capabilities Seminar, January 2007.
- (11) Joint Interoperability Seminar, March 2007.

b. Future Experimentation. The following experiments and wargames will further assist in defining the Army's future Modular Force ISR capabilities.

- (1) ISR Warfighter Integrated Event I, February 2008.
- (2) Joint Interoperability Seminar, March 2008.
- (3) Complex Web Defense Experiment, March 2008.
- (4) Biometric Summit, March 2008.

¹³ The Soviet war in Afghanistan: History and harbinger of future war?

¹⁴ Dooley, M.A. (1994). Ignoring history: The flawed effort to divorce reconnaissance from security in modern cavalry transformation. Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS

- (5) Company Analysis Team, April 2008.
 - (6) Joint Expeditionary Force Experiment 2008, Collaboration and Connectivity, April 2008.
 - (7) ISR Warfighter Integrated Event II, August 2008.
 - (8) Omni Fusion 2008, September 2008.
 - (9) Unified Quest, 2008 (multiple events).
 - (10) Future Joint ISR Requirements Seminar (to be determined).
 - (12) ISR Warfighter Integrated Event, August 2009.
-

Appendix A References

Section I

Required References

ARs, DA pams, field manuals (FM), and DA forms are available at [Army Publishing Directorate \(APD\) – Home Page http://www.usapa.army.mil](http://www.usapa.army.mil). TRADOC publications and forms are available at [TRADOC Publications at http://www.tradoc.army.mil](http://www.tradoc.army.mil).

Battlespace Awareness Joint Functional Concept.

Capstone Concept for Joint Operations.

Command and Control Joint Integrating Concept.

Field Manual 3-0
Operations.

Joint Command and Control Functional Concept.

Joint Publication 3-0
Joint Operations.

Major Combat Operations Joint Operating Concept.

Persistent Intelligence, Surveillance, and Reconnaissance: Planning and Direction JIC.

TRADOC Pamphlet 525-2-1
The United States Army Functional Concept for See 2015-2024.

TRADOC Pamphlet 525-3-0
The Army in Joint Operations, The Army's Future Force Capstone Concept 2015-2024.

Section II

Related References

A related publication is a source of additional information. The user does not have to read a related reference to understand this publication.

Army Posture Statement, 2007.

Army Strategic Planning Guidance, FY2006-2023.

Army Transformation Roadmap.

CJCSM 3500.04D
Universal Joint Task List.

FM 7-15

The Army Universal Task List.

FM Interim 3-90.9

Future Combat Systems Brigade Combat Team Operations.

Homeland Defense and Civil Support JOC.

Military Support to Stabilization, Security, Transition, and Reconstruction JOC.

National Defense Strategy of the United States.

National Counterintelligence Strategy of the United States.

National Intelligence Strategy of the United States.

National Military Strategy of the United States.

National Security Strategy of the United States.

Net-Centric Environment Joint Functional Concept.

Protection Joint Functional Concept.

Quadrennial Defense Review.

Strategy for Homeland Defense and Civil Support.

TRADOC Pamphlet 525-3-1

The United States Army Operating Concept for Operational Maneuver 2015-2024.

TRADOC Pamphlet 525-3-2

The United States Army Operating Concept for Tactical Maneuver 2015-2024.

TRADOC Pamphlet 525-3-3

The United States Army Functional Concept for Battle Command 2015-2024.

TRADOC Pamphlet 525-3-4

The United States Army Functional Concept for Strike 2015-2024.

TRADOC Pamphlet 525-3-5

The United States Army Functional Concept for Protect 2015-2024.

TRADOC Pamphlet 525-3-6

The United States Army Functional Concept for Move 2015-2024.

TRADOC Pam 525-7-9

TRADOC Pamphlet 525-3-90

The United States Army Future Combat Force Operational and Organizational Plan for the Future Combat Systems Brigade Combat Team.

TRADOC Pamphlet 525-4-1

The United States Army Functional Concept for Sustain 2015-2024.

TRADOC Pamphlet 525-7-4

The United States Army's Concept Capability Plan for Space Operations 2015-2024.

TRADOC Pamphlet 525-7-6

United States Army Concept Capability Plan for Army Electronic Warfare Operations for the Future Modular Force 2015-2024.

TRADOC Pamphlet 525-66

Military Operations Force Operating Capabilities.

Glossary

Section I Abbreviations

AO	area of operations
AOR	area of responsibility
APOD	aerial port of debarkation
ASCC	Army service component command
BCT	brigade combat team
BDA	battle damage assessment
BLOS	beyond line of sight
C2	command and control
C3D2	camouflage, cover, concealment, denial, and deception
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAB	combat aviation brigade
CBA	capabilities based assessment
CBRN	chemical, biological, radiological, and nuclear
CCIR	commander's critical information requirements
CCJO	Capstone Concept for Joint Operations
CCP	concept capability plan
CD&E	concept development and experimentation
CI	counterintelligence
CJTF	commander joint task force or combined joint task force
CNO	computer network operations
CONUS	continental United States
COP	common operational picture
CS	civil support
DA	Department of the Army
DNA	deoxyribonucleic acid
DOD	Department of Defense
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel and facilities
EA	electronic attack
EAB	echelons above brigade
EM	electromagnetic
ES2	every Soldier is a sensor
EW	electronic warfare
GEOINT	geospatial intelligence
GIG	global information grid
GMI	general military intelligence
GS	global strike
HD	homeland defense
HMMWV	high mobility multipurpose wheeled vehicle
HPT	high-payoff target

HQ	headquarters
HS	homeland security
HSI	hyperspectral imagery
HUMINT	human intelligence
HVT	high-value target
I&W	indications and warning
IBS	Integrated Broadcast System
IC	intelligence community
IED	improvised explosive device
IMINT	imagery intelligence
IO	information operations
IR	information requirement
ISR	intelligence, surveillance, and reconnaissance
JC2	joint command and control
JCIDS	Joint Capabilities Integration and Development System
JF	joint force
JFC	joint force commander
JIC	joint integrating concept
JIIM	joint, interagency, intergovernmental, multinational
JTF	joint task force
LOC	line of communications
LOI	level of interoperability
LOS	line of sight
M&S	modeling and simulation
MASINT	measurement and signatures intelligence
MDMP	military decision making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MI	military intelligence
MP	military police
MSI	multi-spectral imagery
MUM	manned and unmanned
NAI	named area of interest
NEBC	network-enabled battle command
NGO	nongovernmental organization
NRT	near real time
NTC	National Training Center
OSINT	open-source intelligence
PIO	police intelligence operations
PIR	priority intelligence requirement
POD	port of debarkation
RF	radio frequency
ROE	rules of engagement
RSTA	reconnaissance, surveillance, and target acquisition
SA	situational awareness
SIGINT	signals intelligence

SOF	special operations forces
SPOD	sea port of debarkation
TAI	target area of interest
TECHINT	technical intelligence
TLE	target location error
TRADOC	Training and Doctrine Command
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system
US	United States
UXO	unexploded ordnance
WMD	weapons of mass destruction

Section II

Terms

acquisition overmatch

Analysis shows that when sensor overmatch is teamed with acquisition standoff, an acquisition overmatch is achieved, which radically degrades threat capabilities. This means scouts dominate at all ranges, even if they are moving. Adding far-target location and target-designation capabilities with point-and-shoot network links provides scout-enabled effects to shape the battlespace, with human control, out of enemy contact. Analysis has shown that scout-enabled fires within acquisition overmatch provides significantly fewer friendly losses, greater decision time and space of the commander, and facilitates decisive maneuver. (Armor Magazine, Mar-Apr 2003).

adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged.

air defense

Defensive measures designed to destroy attacking enemy aircraft or missiles in the atmosphere, or to nullify or reduce the effectiveness of such attack.

all-source intelligence

Intelligence products and or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked.

area of influence

A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control.

area of operations

An operational area defined by the joint force commander for land and maritime forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces.

area of responsibility

The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations.

armed reconnaissance

A mission with the primary purpose of locating and attacking targets of opportunity, such as, enemy materiel, personnel, and facilities, in assigned general areas or along assigned ground communications routes, and not for the purpose of attacking specific briefed targets.

battlespace awareness

Knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and non-combatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply combat power, protect the force, and or complete the mission.

civil support

Department of Defense support to U.S. civil authorities for domestic emergencies, and for designated law enforcement and other activities.

collection

In intelligence usage, the acquisition of information and the provision of this information to processing elements.

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 re-tasking, as required.

collection manager

An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission.

combat information

Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements.

common operational picture

A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 1-02) A single display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command. (FM 3-0).

counterintelligence (

Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

cyberspace

The notional environment in which digitized information is communicated over computer networks.

data

The lowest class of information on the cognitive hierarchy. Data consist of raw signals communicated by any nodes in an information system, or sensings from the environment detected by a collector of any kind (human, mechanical, or electronic). (TRADOC Pam 525-2-1). Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (JP 1-02)

document and media exploitation

The processing, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under the U.S. government's physical control and are not publicly available. This definition excludes: handling of documents and media during the collection, initial review, and inventory process; and, documents and media withheld from the IC document and media exploitation dissemination system in accordance with Director of National Intelligence-sanctioned agreements and policies to protect sources and methods. (Intelligence Community Directive Number 302, 6 JUL 2007).

effect

1. The physical or behavioral state of a system that results from an action, a set of actions, or another effect. 2. The result, outcome, or consequence of an action. 3. A change to a condition, behavior, or degree of freedom.

electronic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support full spectrum operations. The Army's operational concept: Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent JF to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and

informed by a thorough understanding of all variables of the operational environment. Mission command that conveys intent and an appreciation of all aspects of the situation guides the adaptive use of Army forces.

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. (JP 2-03).

global information grid

The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems.

homeland defense

The protection of U.S. sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President.

homeland security

Homeland security, as defined in the National Strategy for Homeland Security, is a concerted national effort to prevent terrorist attacks within the U.S. reduces vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. The Department of Defense contributes to homeland security through its military missions overseas, homeland defense, and support to civil authorities.

human intelligence

The collection by a trained HUMINT collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities. (FM 2-0).

imagery intelligence

Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media.

indications and warning

Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the U.S. or allied and or coalition military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear and non-nuclear attack on the U.S., its overseas forces, or allied and or coalition nations; hostile reactions to U.S. reconnaissance activities; terrorists' attacks; and other similar events.

information

Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation.

information operations

The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

information requirements

Those items of information regarding the adversary and the environment that need to be collected and processed in order to meet the intelligence requirements of a commander.

information superiority

The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

intelligence

The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

intelligence, surveillance

An activity that synchronizes and integrates the planning and reconnaissance and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. For Army forces, this activity is a combined arms operation that focuses on priority intelligence requirements while answering the commander's critical information requirements.

joint concept

Links strategic guidance to the development and employment of future JF capabilities and serve as "engines for transformation" that may ultimately lead to DOTMLPF and policy changes.

joint force commander

A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a JF.

joint task force

A JF that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander.

knowledge

In the context of the cognitive hierarchy, information analyzed to provide meaning and value or evaluated as to implications for the operation. (See Functional Concept).

lead federal agency

The federal agency that leads and coordinates the overall federal response to an emergency. Designation and responsibilities of a lead federal agency vary according to the type of emergency and the agency's statutory authority.

measurement and signature intelligence

Technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. MASINT capabilities include radar, laser, optical, infrared, acoustic, nuclear radiation, radio frequency, spectroradiometric, and seismic sensing systems as well as gas, liquid, and solid materials sampling and analysis.

near real time

Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays.

nongovernmental organization

A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and or encouraging the establishment of democratic institutions and civil society.

open-source intelligence

Information of potential intelligence value that is available to the general public.

operational environment

A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.

persistent surveillance

A collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in near or real-time. Persistent surveillance facilitates the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action.

Phase 0

From Joint Publication 3-0, this phase is defined as "Joint and multinational operations — inclusive of normal and routine military activities — and various interagency activities are performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies. They are executed continuously with the intent to enhance international legitimacy and gain multinational cooperation in support of defined military and national

strategic objectives. They are designed to assure success by shaping perceptions and influencing the behavior of both adversaries and allies, developing allied and friendly military capabilities for self-defense and coalition operations, improving information exchange and intelligence sharing, and providing U.S. forces with peacetime and contingency access. Shape phase activities must adapt to a particular theater environment and may be executed in one theater in order to create effects and/or achieve objectives in another.”

police intelligence operations

A military police function that supports, enhances, and contributes to the commander’s force protection program, common operational picture, and situational understanding. The police intelligence operations function ensures that information collected during the conduct of other military police functions is provided as input to the intelligence collection effort and turned into action or reports. (FM 3-19.50)

reachback

The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed.

real time

Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays.

reconnaissance

A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

request for information

Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command’s procedures. The National Security Agency and Central Security Service uses this term to state ad hoc signals intelligence requirements.

signals intelligence

A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. Intelligence derived from communications, electronic, and foreign instrumentation signals.

situational awareness

Immediate knowledge of the conditions of the operation, constrained geographically and in time.

situational understanding

The product of applying analysis and judgment to relevant information to determine the relationships among the mission variables to facilitate decisionmaking.

surveillance

The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.

synchronization

1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In the intelligence context, application of intelligence sources and methods in concert with the operation plan.

tactical persistent

The synchronization and integration of available, surveillance networked sensors and analysts across warfighting functions and operational environments, to provide commanders with combat information, actionable intelligence, and situational understanding. In response to the tactical commander's requirements (the CCIRs), TPS missions detect, characterize, locate, track, target, and assess specific objects or areas, in real or near real time despite target countermeasures or natural obstacles. (USAIC&FH White Paper, 25 SEP 07).

technical intelligence

Intelligence derived from exploitation of foreign material, produced for strategic, operational, and tactical level commanders. Technical intelligence begins when an individual service member finds something new on the battlefield and takes the proper steps to report it. The item is then exploited at successively higher levels until a countermeasure is produced to neutralize the adversary's technological advantage.

