

# Intelligence

February 2017

**This page intentionally left blank**

## Foreword

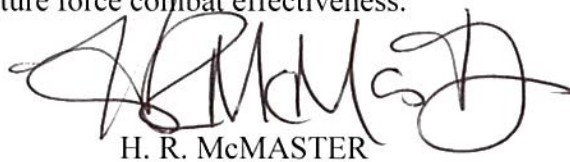
### *From the Director United States (U.S.) Army Capabilities Integration Center*

The U.S. Army is the Nation's principal land force organized, trained, and equipped for prompt and sustained cross-domain combat. Army organizations provide foundational intelligence capabilities to the Joint Force. Joint and Army commanders rely on data, information, and intelligence during operations to develop situational understanding against determined and adaptive enemies. Knowledge of the threats, enemies, adversaries, and operating environment is critical to Army and Joint Force success. Army forces must process, exploit, and analyze information from multiple disciplines and domains and push intelligence to the point of need to maintain advantages over the enemy. However, because of limitations associated with human cognition, and because much of the information obtained in war is contradictory or false, more information will not equate to better understanding. Commanders and units must be prepared to integrate intelligence and operations to develop situational understanding in close contact with the enemy, partners, and civilian populations.

TRADOC Pam 525-2-1, *The U.S. Army Functional Concept for Intelligence (AFC-I)*, expands on the idea of developing situational understanding presented in TRADOC Pam 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World (AOC)* and TRADOC Pam 525-3-6, *The Army Functional Concept for Movement and Maneuver (AFC-MM)*. The AFC-I describes extending the intelligence enterprise from national to tactical echelons, organizing the force to support the regionally aligned expeditionary Army forces, leveraging technology to enable Soldiers, and developing professionals to deliver information and intelligence to commanders as they execute joint combined arms operations. While technology is a central enabler to this effort, the Army must produce agile, adaptive, culturally aware, and innovative leaders and Soldiers who provide the intelligence commanders and units need to win against adaptive enemies.

Enemies will employ countermeasures to avoid detection and cloud efforts to develop situational understanding; therefore, Army forces must be prepared to employ multi-disciplinary intelligence, simultaneously through multiple domains, and operate under conditions of uncertainty. Because enemies will disrupt information collection, analysis, and dissemination, Army forces must work to develop situational understanding with degraded systems. Since enemies will employ sophisticated collection against U.S. forces, the Army must protect high value intelligence assets and take actions to secure the force and deceive the enemy. Enemies will operate across multiple battlegrounds and multiple domains; U.S. forces must integrate intelligence efforts with multiple partners and develop understanding across all domains, and in other contested spaces such as, political subversion, information, corruption, organized crime, illicit finance, and perceptions. Situational understanding encompasses threats, enemies, and adversaries; the operational environment; and the people among whom wars are fought. Military intelligence must bridge into political, cultural, social, informational, financial, ideological, institutional, criminal, and economic intelligence to enable Army forces to shape security environments, defeat enemy organizations, and consolidate gains.

This concept serves as a foundation for developing future intelligence capabilities and helps Army leaders *think* clearly about future armed conflict, *learn* about the future through the Army's campaign of learning, *analyze* future capability gaps and identify opportunities, and *implement* interim solutions to improve current and future force combat effectiveness.

A handwritten signature in dark ink, appearing to read 'H. R. McMaster', with a stylized, flowing script.

H. R. McMASTER  
Lieutenant General, U.S. Army  
Director, Army Capabilities  
Integration Center

## Preface

***From the Commander  
United States (U.S.) Army Intelligence Center of Excellence***

*TP 525-3-1, The U.S. Army Operating Concept: Win in a Complex World (AOC)* outlines how the future Army will win in a complex world. To do this, the Army must develop a high degree of situational understanding in an environment frequently described as complex, uncertain, and rapidly changing. *TP 525-2-1, The U.S. Army Functional Concept for Intelligence (AFC-I)* identifies future challenges and proposes solutions to support the situational understanding needed to win in a complex world. The intelligence enterprise provides synergistic intelligence capabilities to the commander. The central idea of this concept is the Army will use the intelligence enterprise to support situational understanding. This enhances operations and intelligence integration: the intelligence enterprise delivers intelligence to operations.

The Army operates as part of a joint, interorganizational, and multinational team, and Army intelligence forces support situational understanding of this team using an enterprise approach. The intelligence enterprise includes joint, interagency, intergovernmental, and multinational partners bound by formal agreements, agreements to which many interorganizational partners such as commercial entities and non-governmental organizations would not agree for the sake of their neutrality and access in a given conflict. This distinction is important when discussing the function of the intelligence enterprise but it does not preclude support to interorganizational partners within legal limits in a given operational situation.

The Army identifies four major areas of effort to maximize support to commanders through the intelligence enterprise. The Army must extend and evolve the intelligence enterprise to support the entire force, organize the force to support the regionally aligned expeditionary Army, leverage technology to enable a smaller force as it overcomes future challenges across all domains of war, and develop Soldiers, leaders and Army civilians to thrive in the future operating environment. This concept expands on these four big ideas.

This concept identifies many technological solutions to future problems. Technology is an enabler, not an end in itself. Throughout history, technology allowed fewer Soldiers to work faster, extended access to targets, and provided an advantage over adversaries. In this concept, technological solutions and people are interdependent; neither can succeed alone. However, nothing in this concept will succeed without the right people, Soldiers and Army Civilians with the cognitive, physical, and social skills to thrive in an uncertain world.



SCOTT D. BERRIER  
Major General, US  
Commanding

**This page intentionally left blank**

## Executive Summary

The AFC-I identifies the key challenges, solutions, and supporting capabilities required to enable intelligence support to joint combined arms operations in future environments against increasingly capable opponents. It supports the ideas in joint and Army concepts. This concept is an evolutionary document which builds on current efforts.

Analysis of the future operating environment, strategic guidance, and joint and Army concepts identifies three major challenges for Army intelligence. Army intelligence forces must support a regionally aligned, globally responsive force based primarily in the continental U.S. Army intelligence forces must support an expeditionary, dispersed, and decentralized force operating decentralized in multiple domains that must respond rapidly, often to austere locations. Finally, Army intelligence forces must be effective in complex and urban terrain.

The central idea of this concept is to integrate the national to tactical intelligence enterprise with multi-domain operations to provide a high degree of situational understanding across the range of military operations (ROMO) while operating in complex environments against determined, adaptive enemy organizations. To realize this central idea, Army capability developers must extend the intelligence enterprise from national to tactical echelons, properly organize the force, leverage technology to better enable Soldiers, and develop professionals to deliver timely, relevant information and intelligence to the commander.

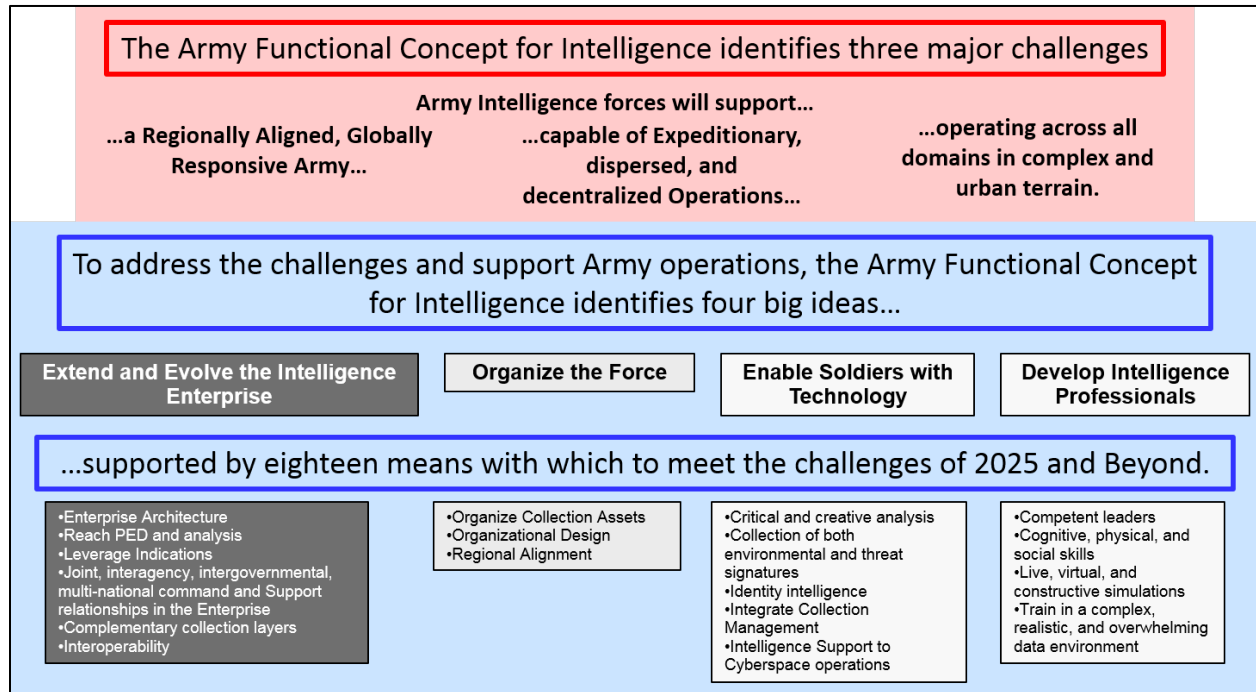
The intelligence enterprise is inherently cross-domain and is the sum total of the intelligence efforts of the entire U.S. intelligence community. It requires architecture, interoperability among partners, unique command and support relationships that ensure support from non-Department of Defense and non-U.S. partners, complementary collection from all domains (land, air, maritime, space, and cyberspace), geographic distribution of processing, exploitation, and dissemination (PED) and analytic capabilities, and timely warning of events that could involve U.S. forces. Efforts largely include maturation, or further development of existing capabilities to ensure support to commanders.

Army intelligence forces must organize to support a regionally engaged, globally responsive, semi-independent, expeditionary Army. Army intelligence forces must align regionally to remain engaged at all times and respond rapidly to support expeditionary operations. This organization includes corps and below forces and capabilities found in the U.S. Army Intelligence and Security Command.

Technology will enable Soldiers to mitigate many complex problems of the future OE. Improved or new analytic processes will use very large data sets to address emerging, unconventional problems. The Army will use a wide array of sensors to capture environmental, individual, and conventional signatures, including open source and the Internet of things. Comprehensive management of information collection resources will require advanced technology. Cyberspace operations and cyberspace enabled intelligence will require constant innovation and investment to enable the overall operation and overcome enemy countermeasures to U.S. operations.

Finally, underpinning all capability development is the human dimension. The Army cannot implement this concept's central idea without the right cognitive, physical, and social skills to succeed and flourish in the uncertainty of the future OE. Warfare will always be a human endeavor characterized by ambiguity, fear, anxiety, and chance. Army intelligence professionals must achieve cognitive dominance through realistic training provided by agile institutions using live, virtual, and constructive simulations.

Figure 1 summarizes the AFC-I. It identifies the major challenges this concept addresses, articulates the four major areas of effort and nineteen subordinate means laid out in this concept.



**Figure 1. Army functional concept for intelligence (AFC-I) summary**



Department of the Army  
Headquarters, United States Army  
Training and Doctrine Command  
Fort Eustis, VA 23604

TRADOC Pamphlet 525-2-1\*

25 January 2017

**Military Operations**

**THE U.S. ARMY FUNCTIONAL CONCEPT FOR INTELLIGENCE 2020-2040**

---

FOR THE COMMANDER:

OFFICIAL:

KEVIN W. MANGUM  
Lieutenant General, U.S. Army  
Deputy Commanding General/  
Chief of Staff



RICHARD A. DAVIS

Senior Executive  
Deputy Chief of Staff, G-6

**History.** This pamphlet is a major revision of U.S. Army Training and Doctrine Command (TRADOC) Pam 525-2-1 dated 13 October 2010. Because this publication is revised extensively, not all changed portions have been highlighted in the summary of change.

**Summary.** TP 525-2-1 describes capabilities the Army will require in 2020-2040 to enable the intelligence warfighting function. This concept will lead force modernization efforts by establishing a common framework within which to develop the specific capabilities required to enable intelligence during the conduct of future joint combined arms operations in uncertain, highly competitive, and dynamic operational environments.

**Applicability.** This concept guides future force modernization and supports the Joint Capabilities Integration and Development System process. It also supports Army capabilities development processes described in the Army Capabilities Integration Center (ARCIC) Concepts and Capabilities Guidance, and functions as the conceptual basis for developing affordable options for the future force pertaining to intelligence across doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) and within policy. This concept applies to all TRADOC, Department of the Army (DA), and Army Reserve Component activities that develop DOTMLPF requirements.

---

\*This publication supersedes TRADOC Pamphlet 525-2-1, dated 13 October 2010.

**Proponent and supplementation authority.** The proponent of this pamphlet is the TRADOC Headquarters, Director, ARCIC. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. Do not supplement this pamphlet without prior approval from Director, TRADOC ARCIC (ATFC-ED), 950 Jefferson Avenue, Fort Eustis, VA 23604-5763. Proponent for military intelligence force modernization and the resulting activity of this pamphlet is the Commander, U.S. Army Intelligence Center of Excellence.

**Suggested improvements.** Users are invited to submit comments and suggested improvements via DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Director, TRADOC ARCIC (ATFC-ED), 950 Jefferson Avenue, Fort Eustis, VA 23604-5763. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program Proposal).

**Availability.** This pamphlet is available on the TRADOC homepage at <http://www.tradoc.army.mil/tpubs/>.

---

## Summary of Change

TRADOC Pamphlet 525-2-1

U.S. Army Functional Concept for Intelligence, 2020-2040

This revision dated 25 January 2017-

- o Changes the applicability period to 2020-2040 (title page).
- o Revises the foreword.
- o Updates the background, operational context, and assumptions that provide the basis for the concept's solutions (para 1-4, 1-5, and chap 2).
- o Updates the military problem, central idea, and solutions (chap 3).
- o Revises the summary and the required capabilities statements (chap 4 and appendix B).
- o Adds appendices on science and technology, risks of adopting this concept, intelligence teams, an operational vignette, a force modernization strategy, elaboration on each challenge identified in chapter 2, and crosswalk with Army warfighting challenges (apps C-K).

**Contents**

	<b>Page</b>
<b>Preface.....</b>	<b>v</b>
<b>Executive Summary .....</b>	<b>vii</b>
<b>Chapter 1 Introduction .....</b>	<b>5</b>
1-1. Purpose .....	5
1-2. References .....	5
1-3. Explanation of abbreviations and terms .....	5
1-4. Background.....	5
1-5. Assumptions .....	5
1-6. Linkage to joint and Army concepts .....	6
<b>Chapter 2 Operational Context .....</b>	<b>7</b>
2-1. Challenge context .....	7
2-2. Challenge to Army forces.....	7
2-3. Challenge to Army intelligence forces .....	8
2-4. Summary of intelligence challenges.....	13
<b>Chapter 3 Military Problem and Solutions .....</b>	<b>13</b>
3-1. Military problem.....	13
3-2. Central idea.....	13
3-3. Implementation of the central idea .....	14
3-4. Extend and evolve the intelligence enterprise .....	16
3-5. Organize the force .....	22
3-6. Enable Soldiers with technology .....	24
3-7. Recruit, train, educate, and retain intelligence professionals .....	29
3-8. Network dependency .....	31
3-9. Conclusion.....	32
<b>Chapter 4 Conclusion .....</b>	<b>33</b>
<b>Appendix A References .....</b>	<b>34</b>
<b>Appendix B Required Capabilities (RCs).....</b>	<b>38</b>
<b>Appendix C Science and Technology .....</b>	<b>44</b>
<b>Appendix D Risk and Mitigation.....</b>	<b>47</b>
<b>Appendix E Intelligence Teams: The Army Contribution to the Intelligence Community</b>	<b>48</b>
<b>Appendix F Intelligence Enterprise Support to Engagement and Expeditionary Operations</b>	<b>50</b>
<b>Appendix G Intelligence Force Modernization Strategy .....</b>	<b>58</b>
<b>Appendix H Implications of a Regionally Aligned and Globally Responsive Force to Army Intelligence Forces .....</b>	<b>60</b>
<b>Appendix I Expeditionary implications to Army Intelligence Forces .....</b>	<b>63</b>
<b>Appendix J Complex and Urban Terrain.....</b>	<b>64</b>
<b>Appendix K RC Crosswalk with Army Warfighting Challenges.....</b>	<b>71</b>
<b>Glossary .....</b>	<b>75</b>
<b>Endnotes.....</b>	<b>78</b>

## Figure List

	<b>Page</b>
Figure 1. Army functional concept for intelligence (AFC-I) summary.....	viii
Figure 3-1. Defining partners in information sharing.....	15
Figure 4-1. AFC-I summary .....	33
Figure B-1. Intelligence support relationships.....	43
Figure F-1. Prevent and shape intelligence capabilities.....	55
Figure F-2. Win intelligence capabilities.....	57
Figure J-1. Megacities complexity.....	70

## Table List

Table J-1. Variables that converge to make megacities a complicated operational environment (OE).....	65
Table K-1. AFC-I RCs and warfighting challenges crosswalk.....	74

## **Chapter 1**

### **Introduction**

#### **1-1. Purpose**

a. *United States (U.S.) Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-2-1, The U.S. Army Functional Concept for Intelligence (AFC-I)* drives Army intelligence force modernization activities in 2020 to 2040. It identifies the key challenges, solutions, and supporting capabilities required to enable the intelligence warfighting function to support joint combined arms operations across all phases in complex environments against increasingly capable opponents to accomplish campaign objectives and protect U.S. national interests. While this publication supersedes the previous concept, it does not rescind previous and ongoing capability development work.

b. This concept poses and answers the following questions:

(1) What are the key challenges and conditions of the future mission sets and operating environment that stress intelligence warfighting function Soldiers and units as they support joint combined arms operations?

(2) How might the Army adjust the intelligence warfighting function to support future joint combined arms operations?

(3) What specific capabilities must the Army adjust or develop within the intelligence warfighting function to support future joint combined arms operations?

#### **1-2. References**

Appendix A lists required and related publications.

#### **1-3. Explanation of abbreviations and terms**

The glossary explains abbreviations and special terms used in this pamphlet.

#### **1-4. Background**

Recent strategic guidance reflects a need for more versatility, a shift in U.S. national security focus, and directs the Army to plan for budget and force reductions. Therefore, Army intelligence leaders and capability developers must reconsider future roles and responsibilities necessary to meet joint, Army, defense, and national demands.

#### **1-5. Assumptions**

a. Department of Defense (DOD) information networks will be robust, reliable, and resilient enough to support the demands of the intelligence enterprise. The network will connect every point of the intelligence enterprise. It will support the demands of operations and intelligence integration. This is the most critical assumption and represents the greatest risk.

b. The assumptions of the *TP 525-3-0, The U.S. Army Capstone Concept (ACC)* and *TP 525-3-1, The U.S. Army Operating Concept: Win in a Complex World (AOC)* are valid.

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

d. Future Soldiers will have the skills, knowledge, and attributes to leverage the intelligence enterprise to help solve complex problems under conditions of uncertainty at a rapid pace.

## **1-6. Linkage to joint and Army concepts**

a. The *Capstone Concept for Joint Operations (CCJO)* describes a globally postured Joint Force that combines quickly capabilities and mission partners across domains, echelons, geographic boundaries, and organizational affiliations. Agility, partnering, and cross domain synergy are paramount to success in the CCJO. These networks of forces and partners form, evolve, dissolve, and reform in different arrangements in time and space with significantly greater fluidity than the current Joint Force. The ACC describes what the Army must do to support the Joint Force in the future operational environment (OE). The Army must provide land power to prevent conflict, shape the OE, and win decisively. Operational adaptability, the ability to shape conditions and respond effectively to changing threats and situations with appropriate, flexible, and timely actions, is central to the ACC.

b. The AOC is the implementation of the CCJO and the ACC. The AOC central idea states, “The Army, as part of joint, interorganizational, and multinational teams, protects the homeland and engages regionally to prevent conflict, shape security environments, and create multiple options for responding to and resolving crises.”<sup>1</sup> The AFC for Movement and Maneuver addresses cross-domain maneuver, semi-independent operations, realized mission command, and integrated reconnaissance and security operations. Mission tailored Army units will be regionally engaged across the globe, building partners, deterring adversaries, and overcoming challenges to defeat enemies using multiple, often simultaneous, actions integrated in time, space, and purpose that create multiple, concurrent dilemmas. The diversity of missions and operational locations, often challenging U.S. national security, poses several challenges to developing situational understanding.<sup>2</sup> Increasing complexity coupled with decreasing available time combine with the need to synthesize enormous volumes of information. These conditions demand more depth in understanding of both the world as it is and the possible activities that could threaten U.S. interests.

c. Army forces develop situational understanding through action during peacetime engagement and during heightened tension and combat operations. This includes information from the bottom up and the top down from joint teams and all warfighting functions. Information collection and analysis help improve understanding of the enemy, terrain, weather, and civil considerations. Soldier interaction with the local population provides information on the social, political, and economic factors in the operational area. Soldier interaction with friendly civilians and local authorities builds trust which can translate to early warning of unrest or hostile action. Peacetime engagement develops context which, when combined with other information, provides situational understanding. During stability or combat operations, Soldier interaction with refugees, internally displaced persons, or prisoners provide context unavailable from technical means alone. Enemy

forces often operate among the population and Soldier interaction may be the only method to distinguish friend from foe. Information collection is a continuous process conducted by all Soldiers. The AFC-I proposes how Army intelligence forces conduct intelligence to support the commander's situational understanding.

---

## **Chapter 2**

### **Operational Context**

#### **2-1. Challenge context**

Increasing fidelity, faster answers, and insights into the intent of thinking enemies and adversaries continue to challenge Army forces for the foreseeable future. Addressing these challenges generates enormous amounts of data and complicates efforts to add clarity while not overwhelming decision makers. Fiscal constraints demand near-term solutions that preserve the balance of readiness, force structure, and modernization necessary to meet the demands of the national defense strategy now, while setting the stage to begin evolving the force in the mid-term (2020-2030) and bringing innovative solutions to fruition to meet the challenges of the far-term (2030-2040).<sup>3</sup> Efforts to improve situational understanding must be consistent with the need to support the speed, tempo, scale, and duration of expeditionary maneuver and joint combined arms operations under the most challenging conditions, including failed governance, order, and economy. Analysis of the future operating environment and implications of joint and Army concepts frame the AFC-I military problem.

#### **2-2. Challenge to Army forces**

a. The AOC identifies five future OE characteristics.<sup>4</sup> These characteristics pose challenges to U.S. national decision makers and to U.S. forces.

(1) International conditions will change more rapidly based on the increased velocity and momentum of human interactions and events.

(2) Technologies will become universally available and create a potential to overmatch U.S. capabilities.

(3) Weapons of mass destruction (WMD) proliferation among state and nonstate actors will pose an increased threat to U.S. security interests.

(4) Advanced cyberspace and counter-space capabilities will spread to state and nonstate actors, allowing them to protect their access and disrupt or deny access to others.

(5) Operations will occur among populations in cities and complex terrain.

b. The Army as part of a joint, interorganizational, and multinational force must overcome these challenges from a largely continental U.S. (CONUS)-based posture and with decreasing resources. Army intelligence forces contribute to mitigating or overcoming the effects of these challenges, but also face their own challenges.

## **2-3. Challenge to Army intelligence forces**

a. Army commanders must develop and sustain a high degree of situational understanding while operating in complex environments against determined, adaptive enemy organizations.<sup>5</sup> Commanders and staffs require situational understanding in a rapidly changing world with state and nonstate adversaries equipped with advanced technologies and weapons operating from and in complex, urban environments who have the will and determination to fight.

(1) Challenges to U.S. interests place a heavy emphasis on developing understanding before a crisis erupts. Demographics, including culture, resources, infrastructure, public order, and others, are key to understanding the character of local conflict and drive U.S. response. Rapid urbanization, particularly in the developing world, creates complex environments from which adversaries operate. In the future, the Army must provide intelligence support for a regionally aligned globally responsive force capable of expeditionary, dispersed, and decentralized operations in complex and urban terrain.

(2) Competitors will include near peer and regional hegemon, as well as less conventional state and non-state adversaries. They will employ conventional, unconventional, and hybrid strategies across all domains. The joint force will operate in theaters where the players are clearly understood and operate in the gray zone where there is ambiguity regarding the adversary.

b. Support a regionally aligned globally responsive force.

(1) Army intelligence professionals, as part of the intelligence enterprise, must understand what defines normalcy in areas of interest to the U.S. and rapidly recognize change in conditions that threaten U.S. interests. An Army with global responsibilities must always be ready. The transition from peacetime to crisis may occur rapidly, and as the U.S. military footprint becomes increasingly CONUS-based, it will be more important to build, maintain, and use knowledge to overcome the tyranny of time. Army intelligence forces will not always build this foundation from scratch, but will use any capability already established across all warfighting functions. Traditional foundations of knowledge are not sufficient for future intelligence needs and regional engagements. Flows of information, money, weapons, bad actors, and relationships among the flows—legitimate or illicit—are important.

(2) Geospatial databases support the understanding of existing infrastructure and potential entry points but do not fully address the complexities of large urban centers, such as megacities. Country studies establish an overview, but city studies and transnational studies are lacking. While infrastructure and order of battle information remain valid, understanding networked and transnational enemy organizations, social media, and biometric identity information have equal or greater importance in some missions. Commanders must also understand critical infrastructure, assets, and terrain in the cyberspace domain. Nonstate ideological movements or political competition may drive national and subnational change more rapidly than conventional analysis may indicate. Proliferation of technology and WMD between states and nonstate actors disrupts normalcy faster than country studies can update.



(3) A regionally engaged globally responsive force needs fundamental situational understanding before engagement. Regional engagement improves the knowledge base through focused and specific information collection. Any engagement force is an opportunity for bottom up reporting that improves the knowledge base. Understanding environments<sup>6</sup> and threats during peacetime may allow the U.S. to avoid escalation to conflict, or, if necessary, facilitate operational planning and support rapid transition to crisis planning and execution. Societal, medical, and threat data will help decision makers understand the human terrain and shape the military concept of the operation. Understanding the environmental hazards posed by pollution, industrial facilities, and infectious diseases will provide leaders with knowledge to plan operations and protect Soldiers. Regional engagement requires language and cultural familiarity if not proficiency. This requirement reinforces the need for realistic training and institutional agility to increase unit readiness. Regional engagement requires understanding of interoperability challenges and mission partner capabilities. Detailed intelligence helps prepare the force for engagement and helps develop partners who may support the U.S. in other operations.

(4) Intelligence leaders and forces must help commanders recognize quickly if normalcy is disrupted. Although some crises may surprise the intelligence community, timely recognition of unacceptable change allows the commander to make timely decisions to conduct shaping operations that may influence the perception battleground. Uncertainty and rapid change increase decision-making variables and decrease timeliness of reported information, forcing commanders to constantly review and challenge assumptions and assessments. Uncertainty and rapid change elevate the analytic risk associated with decision-making and further compound the challenges of the environment.<sup>7</sup> Warning intelligence assesses the probability of hostile actions to provide sufficient warning to prevent, preempt, counter, or otherwise moderate their outcome.<sup>8</sup> The *Joint Concept for Entry Operations* (JCEO) calls for timely access to warning intelligence.<sup>9</sup> Commanders need thoughtfully developed indicators to shorten planning cycles and improve the knowledge base of a given area. This reinforces the need for a detailed knowledge base to help analysts predict conflict and improve unit readiness. Analysts must provide uninterrupted awareness to commanders from peace through crises and back to peace. This awareness requires solving a wide range of mission and operational problem sets anywhere and anytime.

(5) For further discussion of implications of a regionally aligned and globally responsive force to Army intelligence forces see appendix H.

c. Support to expeditionary, dispersed, decentralized, and semi-independent operations in multiple domains.

(1) An expeditionary force must be rapidly employable, scalable and tailorable, and globally responsive in sufficient strength, capability, and endurance. Army intelligence leaders and intelligence forces must support an expeditionary, dispersed, and decentralized force without adding unnecessary lift, sustainment, and security requirements. To support a light expeditionary footprint, intelligence forces must enable home station mission command posts with intelligence reach centers that connect across all networks to the forward deployed force. Army intelligence products must continuously inform commanders through all phases of military operations, across the range of military operations (ROMO) whether stationary or during strategic or tactical movement. Intelligence informs operations as operations inform intelligence. Army intelligence

forces must have the core competency capabilities of collection, processing, exploitation and dissemination (PED), analysis, and intelligence synchronization to support the force continuously.<sup>10</sup> Collection assets must have the range, persistence, and overwatch capabilities to support situational awareness for globally dispersed and decentralized forces. PED and analysis must be always alert and timely. The commander must be able to synchronize these capabilities as conditions change.

(2) Expeditionary forces must overcome anti-access (A2) and area denial (AD) challenges.

(a) The CCJO establishes the need to overcome A2 and AD capabilities. The JCEO further states that intelligence organizations in support of entry operations require two specialized categories of capabilities: focused collection on the A2 and AD threats to light weight entry forces and threats to the air and sealift used during the entry operation.<sup>11</sup> The *Joint Operational Access Concept* (JOAC) establishes the need to develop cross domain multi-disciplined intelligence during opposed access and the need to conduct timely and accurate cross domain all source intelligence fusion in an opposed access situation.<sup>12</sup> Current Army tactical intelligence collection systems are not available or optimized until after establishing forces on the ground. The Army designed tactical intelligence collection assets to support close in engagements. The JCEO demands the ability to access national capabilities, such as aerial, space, and cyberspace, at appropriate echelons during entry operations and calls for the ability to deploy and access robust intelligence, surveillance, and reconnaissance capabilities sufficient to meet the needs of the initial entry force, before and during the initial entry phase.<sup>13</sup> This is particularly difficult during forcible entry and must continue through subsequent operational phases.

(b) To be globally responsive, an increasingly CONUS-based Joint Force must deploy rapidly over extended distances, sustain itself, and achieve strategic results. Army forces must have the ability to maintain situational awareness over great distances and between dispersed formations. Army collection assets must improve size, weight and power capabilities, resulting in increased endurance, to be more deployable and sustainable while increasing sensor and platform versatility and while operating from effective, defensible network architectures. Joint and national collection capabilities, primarily from the air and space layers but also from the maritime and cyberspace domains, may be the only available collection assets during entry operations. Army commanders must be able to task and receive collection from assets during strategic movement and tactical maneuver.<sup>14</sup> A force in transit must receive, as well as send information updates that could affect the plan. This supports the Army's ability to prevent conflict, shape the environment, and win the conflict if prevention fails. Additionally, the JOAC identifies the need for operational forces to detect and respond to hostile computer network attack in an opposed access situation.<sup>15</sup>

(3) Expeditionary and semi-independent forces must be prepared to operate under austere conditions, possibly for long periods. Some contingency locations will not be near adequate ports or along sufficient lines of communication. Low density intelligence collection assets must be sustainable. Many current aerial intelligence collection systems must have basing rights. Expeditionary aerial intelligence collection assets must be smaller, more survivable, employable without airfields, or have longer operational ranges. Enemy forces will employ synchronized space, cyberspace, and electronic warfare capabilities to disrupt or degrade Army information networks. Intelligence leaders must balance the need to feed the commander's situational understanding with severely constrained bandwidth limitations. It will be important to operate during times of reduced

or interrupted connectivity or in cases of no connectivity to ensure that intelligence is available at the earliest consumable point. Austere conditions may also include locations where there has been little or no regional engagement, and infrastructure is not well known. Leaders must ensure collectors and analysts are trained to perform duties during austere conditions. Training conditions must include techniques to overcome limited network architecture and infrastructure.

(4) For further discussion of expeditionary, dispersed, decentralized, and semi-independent implications to Army intelligence forces see appendix I.

d. Operating in complex and urban terrain.

(1) The Army must map and understand urban areas and megacities before operations begin. The human dynamic and the physical environment make operations in densely populated urban areas extremely difficult.<sup>16</sup> By 2030, more than 60 percent of the world's population will live in urban areas in the littoral region. By 2035, over 40 cities will have a population of ten million or more. These megacities are important to their nation's stability and the region's economy and security. Threats to U.S. interests abroad and to the homeland emanate from these globally connected and chaotic urban centers, increasing the need for precision information and intelligence to include geo-location and identification capabilities.

(2) Current information collection techniques are not robust enough to understand the rapidly changing urban environment. The speed of human interaction is greatest in a large urban environment. Operations in urban environments are not traditional adversary centric problems – the environment itself offers significant challenges to a conventional force and provides ample concealment to the enemy. Social networking, flows, infrastructure layering, radical variations by neighborhood, multiple authority structures, and others, complicate information collection against populations, infrastructure, and physical environment signatures. Government, religious, economic, and ideological actors use social and traditional public media to influence the population. Understanding the environment requires collecting and exploiting relevant signatures, many of which are either as of yet undiscovered, or lack sufficient technical exploitation to be useful.

(3) Army intelligence collection is historically more effective against mission variables than against operational variables.<sup>17</sup> However, the context of the future fight may place a premium on the operational variables and understanding the cause and effect relationship among them. Population, structural, and signal density in urban environments produce physical and virtual clutter which reduces the effectiveness of intelligence collection and complicates target acquisition. The subterranean environment offers specific challenges to information collection. Market saturation of cell phones and other mobile, web enabled devices produce a signal dense environment which complicates target acquisition and signals intelligence (SIGINT) collection. Further, the multidimensional urban environment presents a departure from the more traditional horizontal target engagement that Army intelligence analysts are accustomed to supporting. Increasing proliferation of personal mobile communications is making connectedness more robust at the personal level adding to the difficulty of identifying relationships, particularly in a population sympathetic to U.S. adversaries. To complicate the environment further, standard communication systems (such as satellite communications and line-of-sight radios) may not work

in (or under) cities. The population volume and language and dialect diversity present in many locations degrade human intelligence (HUMINT) collection capability. Access to existing public and private infrastructures and security systems is another challenge.

(4) Understanding complex and urban environments requires the detailed analysis that defines the unique and multi-domain nature of major urban areas. Intelligence preparation of the operational environment (IPOE) is country-based currently and inadequate for analyzing a large, complex city as a system. Large cities bring new requirements for understanding the population's impact on the OE and drivers of conflict. This will require an understanding and proficiency with new technical capabilities, automated human terrain mapping and modeling obtained through Internet research, capturing and understanding social media movements, engagement, and staff expertise prior to expeditionary action. Neighborhood level knowledge is critical to understanding the complex interactions in cities and requires Soldier interaction at the street level. Public health concerns, resource scarcity, rule of law, communications infrastructure, and wealth disparity all impact the large city and Army intelligence forces must understand those impacts. Complex and urban environments can increase weather condition effects on personnel and equipment as issues, such as poor drainage, wind funneling, and heat island effects become more pronounced. Transportation and distribution infrastructure varies radically, with concentrations of high-tech transportation and globally connected air- and sea- ports intermixed with open landfills, subterranean infrastructure, and makeshift power grids.

(5) Large urban centers have become the native environment for non-nation state, and unaligned individuals and organizations that live and work in the shadows of national rule. In this environment, criminal and ideological networks offer opportunity for the unemployed masses. Threats to U.S. interests abroad and to the homeland will emanate from these globally connected urban centers.

(6) For further discussion of complex urban terrain implications to Army intelligence forces, see appendix J.

e. Operating in the homeland.

(1) Army intelligence forces must prepare to provide detailed intelligence on threats and hazards within the homeland to facilitate mission command over a wide range of military operations. To support these operations, intelligence forces, when granted proper authorities, must be proficient in supporting incident awareness and assessment to inform decision-making and perform OE analysis.

(2) Legal constraints govern intelligence support to operations conducted within the homeland, specifically Defense Support to Civil Authorities (DSCA) and homeland defense. The U.S. is a litigious environment within which the Army operates; intelligence leaders must understand the role legal limitations and authorities play in shaping intelligence support.

(3) Specific legal constraints regarding DOD intelligence activities and intelligence oversight impact intelligence support to DSCA operations directly. Any use of DOD intelligence

community components supporting DSCA operations is permitted only according to specific authorities.

## **2-4. Summary of intelligence challenges**

To support the future Joint Force, Army intelligence forces must help commanders “develop and sustain a high degree of situational understanding while operating in complex environments against determined, adaptive enemy organizations.”<sup>18</sup> Army intelligence leaders and intelligence forces, as part of the intelligence enterprise, establish a knowledge baseline of normalcy, support regional engagement forces, and recognize quickly when conditions change to the point that U.S. interests are threatened. Army intelligence forces support a rapidly employable, scalable, and tailorable, force as it overcomes A2 and AD challenges and operates under austere conditions. Army intelligence forces and capabilities support the force operating in complex and urban terrain. These challenges extend beyond conventional problems. Operations among the people challenge the Army to understand the range of battlegrounds, including physical, cyber, and informational. Understanding the connections between the human and environmental aspects of the OE, the constraints imposed by law and public perception, and the time available to meet national objectives challenges intelligence professionals and commanders.

## **Chapter 3 Military Problem and Solutions**

### **3-1. Military problem**

To support future Army forces conducting joint combined arms operations, how do leaders, Soldiers, and units support situational understanding across the ROMO to a regionally aligned globally responsive force capable of expeditionary operations in complex and urban terrain?

### **3-2. Central idea**

a. The intelligence enterprise exists to support operations. Army forces integrate the cross-domain national to tactical intelligence enterprise, the sum total of the intelligence efforts of the entire U.S. intelligence community, with operations to provide commanders a high degree of situational understanding across the ROMO while operating in complex environments against determined, adaptive enemy organizations. Army forces develop situational understanding through action. This action includes the range of operations from armed reconnaissance to accessing national space-based collection assets to satisfy commanders’ information requirements. As a core member of the intelligence enterprise, Army intelligence forces extend, evolve, and adapt the intelligence enterprise. Intelligence Soldiers station, equip, train, and organize to support a regionally aligned, expeditionary Army. Army intelligence leaders create new solutions to solve complex operational problems. Technology is a central enabler to this effort, but adaptive leaders and cohesive teams that thrive in ambiguity and chaos underpin everything.

b. The intelligence enterprise is a network of capabilities that help develop understanding using data, information, and intelligence. The intelligence enterprise provides presence and capability across time and delivers complementary vice additive capability to all users. Army information collection, encompassing more than intelligence operations, contributes to the intelligence

enterprise. Using mission command information systems, all Army elements have access to the intelligence enterprise as both a contributor and a consumer. The intelligence enterprise is a tool that assists commanders in reducing uncertainty, improving decision making, and reducing risk.

c. The U.S. intelligence community continues to develop an enterprise approach to collection, PED, analysis, and intelligence dissemination.<sup>19</sup> Army intelligence forces transitioned from the combat, electronic warfare intelligence ownership approach (employed during the cold war, when division and corps commanders owned the collection and analysis matched to their area of operations), to the intelligence enterprise approach. The U.S. Army embraced the enterprise approach when it became technologically feasible and, specifically, when the Joint Intelligence Operations Capability–Iraq revolutionized intelligence operations.<sup>20</sup> Technology improves the speed and precision of information to complement the context and judgment of the commander. Shared awareness developed continuously and provided by the intelligence enterprise facilitates mission command.

### **3-3. Implementation of the central idea**

a. To implement the AFC-I's central idea, Army intelligence forces must extend the intelligence enterprise to all Army elements and evolve and adapt the enterprise capabilities to meet the challenges of the future OE. The intelligence enterprise allows intelligence professionals and others using Army mission command information systems access to data collected and processed across the intelligence community. The architecture requires connectivity between all points of presence: information collection, PED, analysis, synchronization, and mission command technical systems across the joint, interagency, intergovernmental, and multinational intelligence enterprise (see figure 3-1 clarification on information sharing partners).

b. Evolving the connectivity effort requires physical, policy, and procedural efforts to overcome current obstacles. This effort includes reliable transport, robust storage, powerful processing, multilevel security, resilient data, and adaptable applications. Policies that facilitate sharing and access across multiple security areas, and standards that ensure interoperability govern the architecture. The Army must also formalize relationships that create a federated approach to geographically distributed capabilities to produce, collect, and access across the joint, interagency, intergovernmental, and multinational intelligence enterprise (see figure 3-1).

### **Interagency, intergovernmental, and interorganizational**

The AOC introduces the term interorganizational in its list of partners. Because of its sensitive nature, intelligence sharing with interorganizational partners may create problems. Authorities and formal agreements govern the intelligence enterprise. Law and policy bind joint and interagency partners. Intergovernmental and multinational elements share bilateral and multilateral Status of Forces Agreements and treaties which codify sharing limits. Sometimes, U.S. forces partner with nongovernmental organizations and the private sector. However, nongovernmental organizations and private organizations, impartial in most cases, do not want to be seen as agents of U.S. policy. These organizations are not bound by formal agreements with the U.S. intelligence community, do not have formal sharing agreements designed to protect sources and methods, and are not part of the intelligence enterprise. Since these organizations are listed as part of the AOC interorganizational definition, the intelligence enterprise uses interagency and intergovernmental, and not interorganizational to show a clear separation of where intelligence sharing begins and ends.

**Figure 3-1. Defining partners in information sharing**

c. Army leaders and capability developers must organize the force. The Army will align the operational force regionally; military intelligence (MI) formations will align accordingly. Army intelligence forces must be available and accessible to understand the commanders' requirements, use the intelligence enterprise to satisfy the requirements, and integrate intelligence into the operations. Due to periods of network degradation, brigade combat teams (BCTs) must retain surveillance, analysis, and intelligence synchronization capabilities and information systems must include data resilience and data refresh into core designs. Army intelligence forces align regionally and continue this approach to provide global support. The U.S. Army Intelligence and Security Command (INSCOM) and MI reserve command MI brigades (theater) (MIB(T)) will anchor the effort, providing dedicated support through Army service component commands (ASCCs) to each combatant command. This anchor will maintain regional databases and relationships with regional partners, providing a gateway for regionally aligned units to support their commanders.

d. The MIB(T) also helps manage the federated production and collection efforts. INSCOM functional brigades reinforce the MIB(T), and provide discipline-specific expertise and key linkages back to national agencies.<sup>21</sup> MI brigades (expeditionary) allow the corps commander to task organize capacity and weight the intelligence effort. This networked force enhances speed and decentralized execution to support operations.

e. The Army must enable intelligence leaders and Soldiers with technology to help identify issues and solve future OE problems. Connectivity across the foundation layer and the sophistication of the components in that layer must keep pace with technology.<sup>22</sup> Sensors will become more deployable, agile, persistent, multi-disciplined, and connected: every platform and the network itself will feed the sensor computing environment. Sensor locations and the relevant information that they collect will readily inform the common operational picture. Analytic applications support decision making using the information available from the intelligence enterprise. The intelligence enterprise resides on redundant communications networks that degrade gracefully rather than fail catastrophically.<sup>23</sup>

f. The Army must recruit, train, educate, and retain intelligence professionals that can operate in the future OE. The Army requires quality leaders at every level, from first-line supervisors to Army senior leaders. The future force requires life cycle talent recruitment, development, education, and management to provide competent and committed leaders needed in the future OE. Human dimension initiatives, nested under cognitive dominance, realistic training, and institutional agility, will help the operational force meet the challenges of the future OE. Technology will not solve stress, uncertainty, friction, or fog issues. Technology will not provide leadership, judgment, or courage. Creating and retaining innovative and agile leaders prepared to execute assigned missions in ambiguous environments is a major future force objective. Army intelligence forces cannot implement the central idea to overcome operational challenges without quality leaders, Soldiers, and Army Civilians.

### **3-4. Extend and evolve the intelligence enterprise**

a. The inherently cross-domain intelligence enterprise is the sum total of intelligence efforts for the entire U.S. intelligence community. The intelligence warfighting function is the Army's contribution to the intelligence enterprise. The intelligence enterprise comprises all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture. The most important element of the intelligence enterprise is the people that make it work.<sup>24</sup> The intelligence enterprise is greater than the sum of its parts, allowing use of far more resources than could ever be available to any given organization. The Army is a contributor and user of the intelligence enterprise. Army intelligence forces engage from home station as well as when forward deployed. To extend, evolve, adapt, and ensure unity of effort, the intelligence enterprise requires architecture, interoperability, a joint, interagency, intergovernmental, and multinational approach, command and support relationships, and people that make it work. The Army benefits from enhanced PED and analysis, more comprehensive collection, and a better focused warning intelligence capability. The intelligence enterprise supports situational understanding through action, ensures no cold starts, and leaves no MI Soldier at rest.

b. The intelligence enterprise architecture provides the data transport, storage, processing, security, applications, and governance used by members of the intelligence enterprise. The Army's intelligence architecture is an integral part of the Army information network.

(1) Data transport includes two-way connectivity between tactical and national users. The Army's information network, and other DOD information networks across multiple security levels, provide the foundational layer's backbone and connect information collection, PED, and analysis from all sources to the decision makers. Soldiers use the latest mobile, handheld, and wireless communications technology to feed and access the intelligence enterprise at the lowest tactical echelons to enable shared situational understanding.

(2) Storage, processing, security, and applications will be a mix between cloud computing and geographically distributed capability at each point on the intelligence enterprise.<sup>25</sup> The CCJO calls for the development of portable, cloud-enabled command and control technologies, and to improve capabilities that better fuse, analyze, and exploit large data sets. The cloud will provide



increased access to data, including the National Security Agency cryptologic cloud, the National Geospatial-Intelligence Agency geospatial intelligence (GEOINT) cloud, and others for geographically dispersed elements.

(3) Cloud technology supports the constant update of flexible, intuitive, powerful tools that help analysts anticipate an adversary's actions. The cloud-based approach solves tactical storage and processing power limitations to leverage advanced analytic software applications, deliver ease of use, and provide intuitive visualization. Cloud technology provides automation hardware, power needed to make it run, and logistics for maintenance to ease the user's burden. Distributed clouds mitigate a single failure point, and support large volumes of structured, unstructured, or differently structured data to complete the threat and environmental portions of the common operating picture. Common processors provide a robust computing environment capable of hosting complex algorithms needed to solve difficult problems. Common processors support both forward and garrison operations, facilitating training and readiness. Distributed processing enables continuous support by organic intelligence assets if connectivity with the cloud is lost.

(4) Army intelligence forces will use INSCOM to provide access and leverage the intelligence enterprise through global presence, functional management, intelligence community relationships, and fixed infrastructure. In some cases, technology will allow organizations to obtain products from intelligence community elements directly via well-structured data bases and common applications.

(5) The intelligence enterprise architecture supports a regionally engaged, expeditionary Army through access to relevant data and products regardless of regional alignment or geographic location. Army leaders command forces from home station, during movement, and when deployed to remote, austere locations. Mission command leadership philosophy principles guide all Army leaders. Enterprise architecture supports improved posturing and allows the Army to distribute capabilities, reducing the forward footprint and providing continuous support to commanders. It provides the infrastructure to keep the commander continuously informed from pre-crisis through movement and joint combined arms operations.

(6) Army intelligence must remain proficient in manual processes and techniques to mitigate network disruption and support semi-independent operations. Intelligence forces must have the capability to continue essential operations during network disruption and resume full capabilities upon network restoration. Intelligence forces should introduce network difficulties during training to maintain proficiencies in basic skills and processes. Additionally, distributed operations reduce risk in the event of localized disruption: units disconnect from the network and continue operations with reduced capability until restoring the network. Army intelligence supports mission command principles which guide continued operations under disrupted network conditions.

(7) Data resilience is the ability of architectural components to recover quickly and continue mission even when there has been a temporary network failure or other disruption. This may require shifting processes in the collection and PED paradigms toward the point of collection. Subsets of existing databases must reside forward while operationally relevant to continue operations during network disruption and to compare with data updates after periods of disruption.

c. Interoperability enables the elements of the intelligence enterprise to operate seamlessly.

(1) Army intelligence information systems must operate with mission command information systems to allow Soldiers with any mission command information system access to the intelligence enterprise while on the move or at the halt. This includes a shared geospatial foundation, operational reporting on the OE, seamless targeting support, and a shared common operational picture. Intelligence databases must ingest reporting from other Army information systems and send reports to those same systems.

(2) Intelligence support to targeting includes three tasks: support to target development, support to target detection, and support to combat assessment. Army intelligence information systems must seamlessly link joint, Army, interagency, intergovernmental, and multinational sensors, with associated intelligence and targeting data to joint, Army, and multinational fires capabilities. These linkages must be reliable and persistent. Where possible, relevant intelligence data must be shared rapidly with joint, interorganizational, and multinational partners to fully enable their own fires systems.

(3) Army intelligence information systems must connect to other intelligence partners across the various disciplines. Interoperability between intelligence disciplines enables cross-cueing, improves fidelity of information and intelligence, and reduces susceptibility to deception. Interoperability is imperative for multi-sensor platforms and PED functions.

(4) Army intelligence information systems must be interoperable with joint and interagency intelligence information systems. Interoperability between the seventeen members of the intelligence community allows collection, PED, analysis, and database sharing. Intelligence enterprise governance must establish and enforce standards to enable technical and procedural interoperability and capability development. Further, the U.S. intelligence community must have the capability to interoperate with intergovernmental agencies, multinational treaty partners, and coalition partners at appropriate security levels. Operations will require Army intelligence support interorganizational partners often with little warning, as when engaged in DSCA in the homeland or disaster relief. Commanders must consider sources and methods used to gather information to maintain information sharing arrangements with partners.

(5) Interoperability allows the intelligence enterprise to support any commander continuously from peacetime military engagement to pre-hostilities through return to home station. Interoperability facilitates reach and reduces lift requirements, forward footprint, sustainment, and force protection. Interoperability supports partnering through preparation of U.S. forces and improving the capability of partners.

d. Intelligence operations must be inherently joint, interagency, intergovernmental, and multinational to provide the full range of capabilities to support the commander. Formal arrangements and governance strengthen the intelligence enterprise. They expand information collection capabilities and capacities beyond Army capabilities. They expand PED and analysis capabilities, capacity, and perspectives, particularly multinational partner's cultural perspectives. This inherently joint, interagency, intergovernmental, and multinational approach strengthens partners and supports Army commanders when Army capabilities are not positioned or available.

The intelligence enterprise may require unique command and support relationships. An enterprise including non-Army, non-DOD, and non-U.S. partners requires unique relationships to ensure support. The Army requires formal agreements with intelligence partners not bound by DOD command and support relationships.

(1) Command relationships define command responsibility and authority while support relationships define the purpose, scope, and effect desired when one capability supports another. Command relationships are hierarchical and include multiple echelons, while the intelligence enterprise provides flat access to information and intelligence across echelons. Commanders establish support relationships when subordination of one unit to another is inappropriate.

(2) Army commanders must fix responsibility for PED and analysis support and collection. Existing command and support relationships establish priority for reach capabilities within the intelligence enterprise. Orders clearly establish relationships and priorities.

(3) An Army unit operating forward with a limited footprint may rely on non-Army organizations for timely intelligence support. Those agencies may support multiple organizations, including non-Army organizations. Intelligence reach is a solution only if it is responsive; however, expeditionary, dispersed, and decentralized operations may require extensive reach. Prioritization and deconfliction is more than a synchronization problem. Senior intelligence officers at the highest level must plan PED and analytic support as precisely as they plan information collection. To ensure accountability of non-Army organizations, future forces require command and support relationships that function in the intelligence enterprise.

(4) Although the intelligence enterprise may require unique command and support relationships, ASCC commanders require robust connectivity to INSCOM, its functional brigades, and the greater intelligence enterprise and firmly established relationships to regional intelligence partners to respond rapidly to their intelligence requirements.

e. Complementary collection layers (space, aerial, and terrestrial) provide a cross domain solution to collection coverage.

(1) The collection layers provide redundancy and variety through complementary information collection; no single layer independently provides optimal support to decision-making and rarely is a single report sufficient for confirmation. Cross cueing between layers and between disciplines increases accuracy and fidelity while reducing susceptibility to deception. Complementary collection layers, including collection in cyberspace, will provide depth and redundancy.

(2) Complementary collection layers, integrated with reconnaissance and security operations, improve capability beyond anything the Army can produce alone. The intelligence disciplines capture different observables to provide context, detect patterns of behavior, provide more accurate and timely answers to information requirements, and counter deception. The Army employs information collection assets in aerial and terrestrial collection layers and draws from other intelligence partner capabilities in those layers, including maritime collection, cyberspace, and the space layer, to feed the PED, advanced analysis, and intelligence synchronization performed in the foundation layer. The Army fights for information and provides excellent collection against close,

dangerous targets but lacks much of the wide area or denied collection provided by joint or national assets. Only together does the intelligence enterprise maximize collection coverage.

(3) Complementary collection layers provide continuous support. Intelligence partners will most likely collect prior to entry operations due to target proximity, and Army forces must access, process, exploit, and analyze that collection. Army units and intelligence partners collect during peacetime engagement. Army intelligence forces use Army and partner collection connected through the intelligence enterprise architecture.

(4) Complementary collection layers integrate non-intelligence sensors. Maneuver, fire control, environmental, and other sensors outside the control of intelligence organizations provide detailed data from more points of presence on the battlespace. The network provides an array of potential sensors without adding unique or additional systems: every tactical radio can support the signals intelligence effort and every video device can support the GEOINT effort. The Internet of things may provide collection and exploitation of commercial and municipal surveillance, data stores, environmental control systems, and much more.

f. Army intelligence forces conduct reach-PED and analysis to meet the commander's requirements. Processing and exploitation in intelligence usage, is the conversion of collected information into forms suitable for intelligence production. Dissemination, in intelligence usage, is the delivery of information or intelligence to users in a suitable form.<sup>26</sup> These two definitions combine routinely into the acronym PED.<sup>27</sup> Intelligence analysis is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production.<sup>28</sup> All PED operations require four fundamental elements: mission command, a collection sensor, communications and processing architecture, and a PED element separate from the collection platform. Data must be resilient to absorb network outages and disruptions.

(1) Commanders decide which capabilities deploy in expeditionary operations, and in what order. Home station reach centers will provide uninterrupted support to commanders through all operational phases. Force limits and other constraints may not allow all PED and analysis to accompany forcible and early entry forces, or in some cases follow on forces. Command and support relationships hold reach capabilities accountable to deployed commanders. Reach PED and analysis must post, and in some cases push, information and intelligence based on the needs and capabilities of the supported commander.

(2) PED is sensor agnostic. Although PED is a single source intelligence activity, it need not rely on a single sensor.<sup>29</sup> Few sensors collect continuously due to movement, weather, maintenance, and other operational factors. Reach PED allows analysts to process and exploit information from multiple sensors and maximize PED resources.

(3) Reach PED and intelligence analysis produces economies and increases capacity. Reach PED and analysis will leverage advanced analytic software and cloud technology to provide continuous support to the commander's information requirements. To support the idea of no MI Soldier at rest, U.S. Army Forces Command (FORSCOM) created the Intelligence Readiness and Operations Capability (IROC). IROC increases readiness of MI Soldiers and units to support leaders and commanders to exercise mission command, conduct overwatch and reach operations,

and conduct reach PED and all source intelligence analysis to support deployed Army units and combatant commanders' daily operational requirements and ASCC validated requirements. Distributing analysis increases capacity and leverages expertise on both a subject and individual level. IROC connects tactical units to the warning intelligence system. Federating PED and intelligence analysis to partners also increases capacity beyond the Army. Data from maneuver sensors and the increasing importance of open source intelligence (OSINT) and the Internet of things adds to the volume and diversity of data. Access to the vast amounts of data available in the intelligence enterprise requires the ability to process and manage that data. The capacity to process and exploit this volume comes from distributing the capability.

(4) Reach PED enables continuous support to forces from peacetime activities through decisive action. During entry operations, reach PED reduces the forward footprint and ensures continuous information processing of joint and national collection assets. Reach PED and intelligence analysis balances the need to satisfy the commander's information requirements with robust intelligence products against lift and forward footprint constraints.

g. Warning intelligence will extend from national to tactical echelons. Historically, indications and warnings provided intense scrutiny of strategic problems such as troop rotations or missile launches. Regionally engaged globally responsive forces will require scrutiny of a larger number of more localized concerns to support planning and operations.

(1) The tyranny of time increases in the rapidly changing future OE. During peacetime, national and joint collection provide awareness over broad areas that Army intelligence, surveillance, and reconnaissance is not capable or resourced to provide. Army forces at home station must have the capability through mission command information systems to tap into the warning intelligence process to reduce reaction time to a given crisis.

(2) The warning problem set expands from conventional military indicators. Political, economic, cultural, criminal, social, and other human factors may threaten U.S. interests and trigger a security response that involves Army forces. Non-state actors, criminal enterprises, enemy and adversary information operations, state actors exercising political subversion, proxy sanctuary, intervention, coercive deterrence, and negotiated manipulation all may threaten U.S. interests. Warning intelligence must include those factors to support operational planning, to build regional knowledge, and to maintain currency in the knowledge base. Influences that affect human behavior and could impact U.S. interests are part of the warning intelligence process in the future OE.

(3) Warning intelligence is critical to operations and intelligence convergence. Activities intended to detect and report time sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against U.S. entities, partners, or interests are the key elements of warning intelligence. Operational contingencies drive the warning intelligence process which analyzes and integrates operations and intelligence information to assess the probability of hostile actions. Warning intelligence extends from national to tactical echelons, and impacts planning and operations as events develop. Warning intelligence provides sufficient warning to preempt, counter, or otherwise moderate situations that threaten U.S. interests. OSINT collection may be the driving source of information, particularly in large urban centers.

(4) Warning intelligence can support regional engagement activities and build knowledge of a potential contingency area. The wider range of warning problems and the greater volume of collection against those problems require drawing fidelity from vast amounts of data. Modeling the OE will help understand stability and normalcy. Using available infrastructure, units can leverage warning intelligence to shorten reaction time and focus collection resources against a crisis area.

### **3-5. Organize the force**

a. Army intelligence forces support situational understanding to a regionally engaged, globally responsive Army. The Army must organize the intelligence force to best use finite intelligence capabilities despite declining resources. To support Army movement and maneuver, information collection capabilities are configured for rapid deployment and immediate employment upon arrival with mobility and survivability commensurate with the supported formation.

b. Army intelligence resources support Army forces regional alignment.

(1) Intelligence organizations have historically been structured for regional alignment: INSCOM MIB(T)s have long supported ASCCs. To support a regionally aligned, globally responsive Army, MIB(T)s continue to serve as the anchor to access theater intelligence, infrastructure, and training opportunities in the six geographic combatant commands plus U.S. Forces Korea, a sub-unified command.<sup>30</sup> INSCOM's subordinate MIB(T)s are global force management implementation guidance assigned and tailored to support each of the separate geographic combatant commands. The MIB(T)s provide a unifying framework across the geographic theaters, utilizing MIB(T) resident and reach capabilities to provide access to theater intelligence, integration into the theater intelligence architecture and training opportunities to regionally aligned forces (RAF) intelligence organizations. MIB(T)s synchronize intelligence requirements and processes with ASCC and combatant command plans and operations.

(2) MI Readiness Command theater support battalions are essential round-out battalions to the MIB(T)s and must remain inextricably linked to the MIB(T) in both a pre-mobilization and post-mobilization status for theater standardization, equipping, training, and mission execution. Of particular note is the relationship between the MIB(T) and the theater special operations command (TSOC), special forces, civil affairs, and military information support operations all have RAFs, and should develop intelligence partnerships with similarly aligned conventional forces, particularly during reach, overwatch and mission preparation activities. MIB(T) access to this valuable contribution through the TSOC supports understanding and prepares conventional forces for RAF missions and vice versa.

(3) Regional alignment provides options short of war. The U.S. Army's regional alignment of forces provides combatant commanders with tailored, responsive, and consistently available Army forces, to include joint task force (JTF)-capable headquarters. Army intelligence forces support regional engagement by preparing forces for engagement and supporting decisionmakers as they prioritize that engagement. It improves partner capacity, sustains strong relationships, and assists partners in building a stronger global security environment.

(4) Regional alignment focuses intelligence efforts. Regional engagement provides the opportunity to develop knowledge on local populations, adversaries and enemies, provide cultural context and threat awareness, provide medical threat awareness, support language proficiency, and improve understanding of space and cyberspace capability and capacity, partners, and the physical environment. Army forces conducting engagement will be a rich source of information on the OE, and Army intelligence forces must routinely focus engagement units and capture observations upon their return. Regional alignment builds understanding of normalcy and supports warning intelligence to recognize when that normalcy changes unacceptably.

(5) Regional alignment reduces surprise. Regional engagement provides a presence that helps understand normalcy in the world and recognize when that normalcy changes unacceptably. Army leaders must develop regional expertise and context to understand the status quo and develop the indicators to know if normalcy is disrupted. Regional alignment does not, however, make forces less globally responsive. The force remains flexible regardless of alignment.

c. Organizational design of Army intelligence forces must support a regionally aligned, globally responsive expeditionary Army.

(1) Army intelligence professionals and formations must be distributed across the force to support globally responsive combined arms teams. Every maneuver formation with a staff structure must continue to have an embedded intelligence officer to plan, prepare, and integrate intelligence into the scheme of maneuver. Every intelligence officer must have some assigned analytic support with reach to the greater intelligence enterprise. To maximize information collection, intelligence collection assets must integrate with maneuver echelons during training and operations. The Army must assign low density collection assets where they can maintain readiness and support expeditionary, dispersed, and decentralized forces. Additionally, intelligence forces must have a close, interdependent relationship with special operating forces (SOF). INSCOM's functional brigades and groups and their associated MI Readiness Command functional organizations will continue to provide dedicated support to departmental and national requirements while sustaining an expeditionary capability to downward reinforce.

(2) Army forces must organize for flexibility. Scarce resources may be centralized to facilitate task organization and optimize productivity of limited assets. Modular organizations will be scalable and tailorable to accomplish their assigned mission(s) successfully immediately upon arrival. These organizations must have multi intelligence collection platforms that reduce size, weight, and power. Forces must prepare to operate under austere conditions for long periods.

(3) The Army must succeed at expeditionary maneuver.<sup>31</sup> Expeditionary maneuver requires force generation that is responsive, sustainable, and significant from the moment of arrival onward, with no break in momentum for force build-up. Future expeditionary operations may lack developed air and sea ports of debarkation or intermediate staging bases. Many MI assets are currently too big to employ during forcible entry operations, arrive too late, and force a greater reliance on joint assets that may not focus on Army problems. MI organizations will provide tailorable teams support to Army commanders at all levels while minimizing the footprint the commander must support. MI organizations may require contract augmentation, particularly

linguist support, to provide timely support. Army forces must have the ability to maintain awareness over great distances and while in transit. Army intelligence forces must provide tailorable teams with a light footprint to collect and enable enterprise capabilities as part of the early entry force.

d. The Army organizes collection assets to improve responsiveness, facilitate task organization, and improve team readiness. BCT collection assets have limited range, making BCTs dependent on intelligence enterprise collection. E-MIB capabilities increase BCT capacity with the addition of limited counterintelligence capability.

(1) Low density ground based collection assets, specifically HUMINT and SIGINT, must be available for engagement and expeditionary operations. If the Army drawdown results in a shortage of these resources in relation to maneuver forces, they must be assigned in a manner that allows access when needed. Centralization will facilitate realistic training and readiness, imitating and fostering partnership and task organization. MI commanders must be diligent during training not to lose relationships with supported units lest they lose integration with those units.

(2) The aerial intelligence brigade will train and prepare the Army's aerial exploitation battalion's manned, all-weather, medium altitude collection systems and the unmanned, medium altitude collection systems designed to meet the dynamic needs of the ground commander conducting decisive action. The Army will employ a complementary array of manned and unmanned airborne technical sensors that collect information not easily or safely accessible by ground collection and with a greater accuracy, precision, or persistence than collected by many joint and national systems. The combat aviation brigade will continue to employ manned rotary wing and medium and low altitude unmanned aircraft systems for missions as determined by the division commander.

### **3-6. Enable Soldiers with technology**

a. Technology must enable Army intelligence leaders and Soldiers to solve complex future OE problems. Improved or new analytic processes to solve emerging problems, sensors to capture emerging signatures, and the comprehensive management of resources will all require advanced technology. Supported by artificial intelligence, analytics will continue to migrate forward to the point of collection, shortening decision cycles and sensor to shooter links. Innovative leaders, skilled Soldiers, and trained and decentralized teams enabled by technology to operate in and among populations provide the most effective solutions.

b. Army forces require a holistic approach to analysis to support understanding the future OE.

(1) The Army develops, trains, and practices advanced analytic techniques to understand the spectrum of problems driven by commanders' information gaps. Intelligence analysis requires creativity and imagination against non-traditional problems, and historical, political, and cultural knowledge to understand the OE. Multi-domain battle requires intelligence preparation of the battlespace that analyzes all domains to find the opportunities in time and space to generate overmatch, present multiple dilemmas to the enemy, and enable joint force freedom of movement and action.



(a) Army intelligence forces will employ advanced analytics (advanced techniques applied against complex problems) that encompass a clear analytic strategy, flexible models, and supporting tools and skills. Intelligence professionals must decompose diverse and complex problems analytically into simpler, more manageable problems, determine the information gaps, gather and produce information to resolve those gaps, and inform decision-makers. In addition to geospatially based analysis, future analysts may approach problems best from a relational or temporal viewpoint. Much of the solution may be doctrinal and training; however, analysts need tools to manipulate very large data sets, understand semantic nuances, and identify behavioral patterns. Analysts will be predictive in their assessments to provide timely support to decision cycles. Additionally, enterprise enabled analysis through reach vastly increases the capacity of a tactical S-2. Technology will increase analytic capacity, but not replace experienced analysts.

(b) Multi-domain battle requires multi-domain situational understanding. Future adversaries will employ sophisticated A2 and cross-domain AD capabilities on physical, electromagnetic, cyber, and human terrain of their choosing. Adversaries will challenge the air, space, cyberspace, and electromagnetic spectrum supremacy the U.S. enjoyed in recent decades. Intelligence preparation of the battlespace must illuminate temporal and spatial windows of opportunity and vulnerability to generate overmatch, protect friendly forces, shape operations, and set conditions for transition throughout the depth of the battlespace.

(c) Understanding the multipolar world and its effect on U.S. interests requires a broader knowledge base and more creative problem solving. Adaptive adversaries will present new problems to attempt overmatch. Analysis must support non-traditional missions in the broader use of national power. Criminal, economic, political, and informational problems will require analytic support. Enforcement of U.S. and international sanctions, law enforcement, and information operations will all require intelligence support and the associated models, tools, and skills.

(d) Current analytic models for understanding intent consider state-sponsored, military oriented methodologies. However, non-state actors and criminals have different motivations and require new analytic models. Understanding human behavior requires understanding the interrelated cognitive, moral, physical, and socio-economic factors of the operating environment. This requires new tools to analyze behavioral factors, create collection indicators, and predict adversarial actions.

(2) Elements of national power come together in cities: cities are the political, economic, and informational hubs of society. Historically, the U.S. Army has largely avoided urban areas, but that may not be the case in the future. The Army must develop tools and techniques to understand the differences and similarities of urban areas. These tools must address complex, adaptive systems and accommodate very large data inputs. Understanding the human dynamic and the urban environment will require creativity and imagination as well as advanced tools to deal with the complexity. Environmental or social information requirements may dominate future intelligence efforts, and the environment can be just as unpredictable and uncooperative as the threat at surrendering capability and intent. Food and water supplies, public health, and utilities may rival threat capabilities as a priority.

(3) There must be analytic models to understand the mechanics of political, social, and criminal organizations to determine the key signatures that develop pertinent knowledge, and there must be techniques to capture those signatures. The Army requires analytic models of operational variables that incorporate a systems approach to large urban areas across all operational phases, particularly population dynamics. Understanding human terrain and infrastructure, (to include subterranean and cyberspace infrastructure), facilitate the understanding of urban areas. Close intermingling of military, civilian, and criminal systems further complicate the urban OE. Dense urban environments complicate rules of engagement, precision targeting requirements, and collateral damage concerns. The Army will need new analytic tools and techniques to understand urban social, cyber, and environmental complexities.

(4) Analytic models must incorporate information from the public domain. Publicly available data accounts for seventy percent of relevant information and the ratio is increasing. Army collection against publically available data sources may offer insights to social interconnectedness, political dynamics and complex cultural, political, historical, or ideological factors that other collection efforts cannot. This information will substantially increase the volume of data used to support situational understanding.

(5) Uncertainty and rapid change elevate the analytic risk associated with decision making and further compound the challenges of the environment.<sup>32</sup> As the rate of change increases, the negative consequences of slow or incomplete intelligence greatly increase. Technology improves analytic speed, particularly when dealing with very large data.

c. Future problems require equal collection of both environmental and threat signatures.

(1) Urban areas pose problems for many traditional collection assets. The population and structural density found in urban areas create challenges to collection and analysis amplified well above conventional formations operating in rural settings. Army sensors must observe both man-made and natural environmental signatures. Tall buildings may mask geospatial collection and complicate SIGINT efforts. Social media and cellular phone traffic is growing exponentially. Few sensors are available that specifically help the commander understand cultural aspects of the environment. Additionally, few current sensors are available that help tactical commanders understand details of the cyberspace environment. The Army needs intelligence for precision targeting and an understanding of the urban systems that bring life to a city, systems that become more fragile as an urban area becomes larger. Access to the Internet of things may provide surveillance by tapping into the private and public security and traffic systems.

(2) OSINT provides insight into human terrain, including social media, search-engines, databases, governmental and nongovernmental organization information sites, biographical data, and publically available business, industry, and economic information. Analysts could use these data sources to perform social network analysis and identify the key personalities within a geographic area or region and to determine their sociological affiliation; civilian, military, law enforcement, government, or other. OSINT could also identify public sentiment to determine if the population is for or against a particular threat group and their narrative or to determine if the population is supportive of blue-force entities and their activities. Information available in the

public domain will continue to grow and the importance of collecting, data-basing, understanding, and using this information will grow.

(3) The Army must collect information against networks or individuals who have access, and the ability, to employ explosive devices, such as hazardous industrial materials and improvised explosive devices. Army forces must predict and detect explosive hazards and their components. Army forces must also identify threat networks that employ explosive devices to interrupt and dismantle lines of communication.

(4) Army intelligence forces must support offensive and defensive measures against enemy unmanned aerial systems, electric fires, electronic warfare, and cyberspace capabilities. Proliferation of these capabilities among state and non-state actors requires identification, tracking, and targeting of advanced systems to achieve U.S. overmatch.

(5) Non-traditional missions require supporting information collection. Criminal activity, economic and travel sanctions, political subversion and support to disaster relief have unique indicators that drive information collection. Soldier interaction is often a powerful information collector, but the Army must develop sensors that identify signatures of non-traditional activity of interest.

(6) Traditional sensor development priorities maximized conventional military signature collection. Recent priorities captured counterinsurgency and stability signatures of interest. Sensor development must keep pace with near peer conventional capabilities as it expands to meet environmental and non-traditional problem sets.

d. The Army requires biometrics, forensics, and document and media exploitation (DOMEX) capabilities to advance identity intelligence.

(1) Threats dispersed into dense, manmade, layered, urban environments will challenge the Army's current sensors and methodologies. Man-made structures and excessive communication traffic will disrupt these Army systems. Hostile elements will use the urban environment to their advantage by seeking cover and concealment amongst the population and dispersing their operations to protect them from U.S. military superiority. To isolate adversaries and enemies from their surroundings, the Army must use identity activities to collect information, control access, and restrict movement to the individual identity level.

(2) Identity activities is a multifunctional capability that enables every Soldier to recognize, monitor, and track adversaries, while protecting personnel and equipment and securing relevant population, resources, and critical infrastructure. Identity activities leverage biometrics, forensics, and DOMEX capabilities to develop identity intelligence, to establish observables and associated signature data, to identify key personnel and organizations, and to support situational understanding. The Army needs identity intelligence to accurately identify and characterize these threats, discover patterns-of-life to enable precision targeting, and minimize the risks of collateral damage. Additionally, identity intelligence supports local and international law enforcement activities and local militaries that reinforce (or police) local law enforcement. Interoperability with partners and others will aid this effort. Open source intelligence provides collection and analytic

capacity and capability through the internet of things. Army forces must locate, identify, characterize, and isolate those characteristics to facilitate military action against them without causing further disruption.

e. The Army requires comprehensive collection management in the future OE. Collection volume in the future may overwhelm analysts unless properly managed.

(1) Commanders must focus available collection as scale can overwhelm collection capacity quickly. Analytic support must decompose information requirements into discreet signatures that satisfy information gaps. Without focused collection taskings, general searches produce volumes of data, only some of which is valuable. Without proper analysis to identify those discreet signatures before tasking collection, analysts may not recognize valuable data once collected.

(2) Collection must be flexible to satisfy unique problems. Creative use of available collectors may be the option until the Army develops new sensors. Access to the Internet of things will provide needed collection in urban areas. Terrestrial and aerial layer collection will leverage common platforms to expand the sensor network. Every radio is a potential signals intelligence receiver and every sight is a potential imagery collector in a mesh network. Using the network as a sensor requires common standards and automated reporting from non-intelligence sensors, and significantly improves situational awareness. Coalition partner collection may be uniquely capable of satisfying specific requirements in their home environment.

(3) Army leaders must understand the entire sensor architecture to manage collection resources, particularly in the urban environment. Information collection planning is an operational commander's responsibility and an operations function. Senior intelligence officers require total visibility of collection resources, their capabilities and limitations, and their availability. Maneuver, target acquisition, and other sensors also provide valuable collection coverage. Improved onboard processing will enable autonomous cross-cueing of sensors, develop knowledge from sensing as it occurs, and permit swarming of platforms and sensors. The sensor computing environment will establish and enforce standards to create the conditions for an integrated and interoperable sensor operating environment. The computing environment will transfer information regarding sensor data, sensor management, and collected information seamlessly to collection managers, decision makers, command posts, and other networked sensors. The design of the sensor architecture will enable collaborative collection and provide timely information to the warfighter at all echelons, regardless of location. Separate systems for managing Army resources, joint and national resources, and coalition partner resources are unacceptable.

f. Intelligence support to cyberspace operations grows in importance to all levels of the force (tactical, operational, and strategic) and requires constant innovation and investment. Signals intelligence provides electronic support measures for electronic warfare and cyberspace operations. This convergence provides the foundation for multi-function capabilities to support the commander across domains to seize, retain, and exploit the initiative in both cyberspace and the electromagnetic spectrum while simultaneously protecting the mission command system.

(1) Multi-disciplined intelligence professionals support the full scope of offensive, defensive, and DOD information network operations. Intelligence is a critical requirement for successful cyberspace operations and cyberspace practitioners will likely increase requirements to the intelligence community over time. Analysts in the cyberspace domain provide comprehensive, virtual, temporal, and physical understanding of the threat to commanders.

(2) Intelligence forces must operate in cyberspace to conduct intelligence activities, produce intelligence, or to add clarity to intelligence assessments produced from multi-disciplined intelligence sources and used in the military decision-making process. Cyber-enabled intelligence is traditional intelligence activities performed using the cyberspace domain as the platform. Cyber-enabled intelligence activities conducted in or through the cyberspace domain enable production of timely, relevant, predictive, and actionable intelligence to support military operations.

### **3-7. Recruit, train, educate, and retain intelligence professionals**

a. The Army cannot implement the AFC-I central idea without adaptive, agile, and innovated leaders, Soldiers, and Army Civilians. This is the intelligence force's human dimension. The most important component of achieving situational understanding is competent leaders who understand collection capabilities and limitations, PED, and analysis in the context of the future OE and know how to synchronize the intelligence competencies to support the commander.

(1) The intelligence enterprise is a vast and complicated network involving the U.S. intelligence community and its partners. Traditionally, leaders understood two echelons higher than the echelon in which they operated. The enterprise approach requires a battalion S-2 to understand national intelligence capabilities; far more than two levels up. To leverage the intelligence enterprise, leaders must understand what it can do, how to access it, and more importantly how to drive it. Intelligence professionals understand collection availability and limitations, PED, and analysis and how to integrate those capabilities to support the commander's situational understanding. Always engaged, competent intelligence professionals will be judged by the ability to answer the commander's critical information requirements using the few resources under their direct control and the vast resources available through the intelligence enterprise.

(2) Conditions in the future OE will require Soldiers, leaders, and teams to thrive in uncertainty. Intelligence professionals must understand unique and evolving threat systems, particularly in urban areas. Intelligence professionals must understand threat motivations in order to defeat rather than accelerate the threat movement. They must understand the physical and social systems that interact to support military and civil engagement and operational planning. They must understand a wide range of cultural settings for activities across the ROMO. They must understand an adaptive threat. Lifelong learning will have no set beginning or end in a leader or Soldier career path and will include institutional training and education, individual learning, and experience. Competent intelligence professionals must thrive in uncertainty.

b. The Army must recruit and develop future Soldiers with the right cognitive, physical, and social skills to succeed and thrive in the uncertain future OE.

(1) The future Soldier must enter the service with a greater potential for mental flexibility, adaptability, critical thinking, and must thrive in ambiguity. Future intelligence Soldiers must analyze large volumes of information rapidly and critically to provide analysis to decision makers. Soldiers must enhance their observation skills, memory, reasoning, and judgment, often while multitasking in a fluid environment. Future intelligence Soldiers must practice analytic skills daily supporting peacetime military engagement and warning intelligence. Future intelligence Soldiers must also understand information technology to operate intelligence tools and understand science, technology, engineering, the mathematics behind weapons technology and the characteristics of complex and dense urban terrain. Future intelligence Soldiers will need an aptitude for languages as well as historical and cultural understanding.

(2) The Army in general and Army intelligence specifically must develop recruiting programs that seek specialized skills and assess Soldiers above the entry level. Academia and industry have professionals with skills relevant to understanding the future OE. This will require programs that assess older recruits at mid grades and programs that integrate them into the force. Additionally, the Army must develop programs that reassess Soldiers that separated from the service, developed specialized skills, and are willing to serve again at a higher grade commensurate with their advanced skills. The Army should explore internships with industry or academia that allow a short sabbatical and return to service without penalty. These programs must support both the active and reserve components.

(3) Future intelligence Soldiers will continue to need the physical and mental toughness to thrive under expeditionary operations. Improved overall health (physical, psychological, social, spiritual, and family preparedness) is important to cognitive dominance and positively impacts readiness. Enhanced fitness promotes Soldier adaptability, reduces stress, improves mental agility, and supports the sustainment of their personal readiness and resilience. Improved health and fitness set conditions for ethical maturity and sound judgment. Realistic training conditions Soldiers to excel under challenging conditions.

(4) Social fitness is critical to team building. Social fitness consists of individual well-being through self-discipline; developing and maintaining trusted, valued relationships; and fostering good communications with others. Army intelligence forces consist of teams with internal and external relationships needed to create holistic intelligence products. Collection teams have internal dependencies and also depend on PED and analytic teams to provide context and meaning to raw observations. Tailoring forces for expeditionary operations requires rapid team building made possible by a socially fit force.

(5) Career mapping Soldiers within their assigned region as well as increasing the focus on language proficiency and increasing cultural immersion and exchange opportunities will provide talent management across the force. Formal training will develop technical competence and focus on advancements in the areas of cognitive and performance enhancement, mental skills training, time management, adaptive and critical thinking, and leadership. The Army must develop evaluation and certification criteria to develop capable analysts through the ranks. Home station training will provide realistic single or multidiscipline intelligence training opportunities at home station and the combat training centers. These competencies extend to leaders at all levels as well as technical training for all Army intelligence Soldiers.

(6) To drive institutional agility, the Army will challenge Soldiers to operate under conditions of uncertainty and rapid change. Soldiers must increase the volume of information they retain and develop cognitive processes to rapidly reassess conditions. Increased emphasis on cultural awareness and situational awareness training opportunities for Soldiers will improve support to RAF. The Army must continue to emphasize industry certifications and licenses and university approaches to learning and precision talent management processes.

(7) Army intelligence includes a civilian component that provides depth and continuity to Army formations. Civilian intelligence professionals require similar skill sets to their military counterparts.

c. Future training includes live, virtual, and constructive simulations. Overwatch will enable training for operational awareness, but will not allow for pre-mission rehearsals and planning. Simulations increase and develop preparedness and readiness. Army intelligence forces must conduct realistic training exercises using synthetic data in a virtually replicated environment. RAF training simulations should mirror the complexity and rigor of a given OE and challenge Soldiers' analytic abilities as well as their critical and creative thinking skills. This allows them to provide realistic intelligence products to support the commander's requirements. Next generation training simulations, including the ability to create massive amounts of realistic multidisciplined intelligence data and virtually locate forces within a given region must be included in the overall intelligence training strategy. Training using these simulations will be critically important at the institution, home station, and deployed locations.

d. Analysts and leaders must train in a complex, realistic, and overwhelming data environment which challenges their abilities progressively. Incorporating decisive action training environment scenarios introduce real-world intelligence data into training, providing depth, complexity to match the operating environment. Scenarios will incorporate actual operational terrain, civil considerations, and partner attributes while enabling virtual unit movement and operations within this simulated environment. Training simulations, enhanced by operational overwatch at home station, will prepare Soldiers for missions across the full ROMO. The Army Foundry intelligence training program currently provides this environment and is a foundation for future training.

### **3-8. Network dependency**

a. The intelligence enterprise approach will not work without reliable communications and the ability to maintain, even when degraded, the network. Warfighters require an agile, robust, and simplified network resistant to cyber-attack that supports joint combined arms operations in a wide variety of OEs. The Army will operate within a global cloud-based network designed to work in austere environments to provide Soldiers access to tailored and timely information at the point of need. The Army will use an integrated intelligence community cloud supporting the mission and other intelligence users through improved discovery, access, and secure information sharing resulting in operations that are more efficient across multiple agencies and increased capability to quickly surge and support unforeseen mission requirements.

b. Latest mobile and handheld communications technology extends the network to the lowest tactical echelons to move data, information and intelligence between sensors, processors, storage centers, and analytic centers. Effective networks require substantial protection, consisting of DOD information networks and aggressive defensive cyberspace operations, generation of intelligence and signals information, all which professionals understand and use. Army intelligence forces will be dependent on the network to connect from the national enterprise to the lowest tactical echelon.

c. Although the goal is expeditionary, uninterrupted mission command, the network will experience degradation and limitation. The intelligence enterprise will minimize network disruption through processing at the point of collection, resilient data, automated sensor cross-cueing, and analog training. Disconnected users must resynchronize rapidly with enterprise data stores upon network restoration.

### **3-9. Conclusion**

a. Future Army forces will develop situational understanding through action, both through physical presence and ready access to the vast resources available across the U.S. intelligence community, their multinational partners, and coordination with other subject matter experts such as academia and industry, as required. Army intelligence forces will use the intelligence enterprise to develop and sustain a high degree of situational understanding while operating in complex environments against determined, adaptive enemy organizations.

(1) The Army must first extend the enterprise to the lowest tactical echelon and evolve the enterprise to meet the ever changing needs of the commander. Only then can the intelligence enterprise integrate fully to support operations.

(2) Army intelligence forces organize to provide responsive support to operations through both presence and reach to the intelligence enterprise. Through support to a regionally aligned globally responsive force, intelligence forces shape the security environment and set the theater while working closely with conventional forces and SOF. Through support to an expeditionary Army, intelligence forces project national power and enable combined arms maneuver and wide area security.

(3) The Army must embrace developing technologies to enable Soldiers to win in the future OE. Information collection and analytic technologies will enable Soldiers to satisfy commanders' requirements quickly. Operations in complex urban terrain will be possible through operations in the cyberspace domain.

(4) Using human dimension initiatives, Army intelligence professional will learn to operate in a rapidly changing, uncertain world. Intelligence professionals train to solve a wide range of problems that match the challenges of the OE.

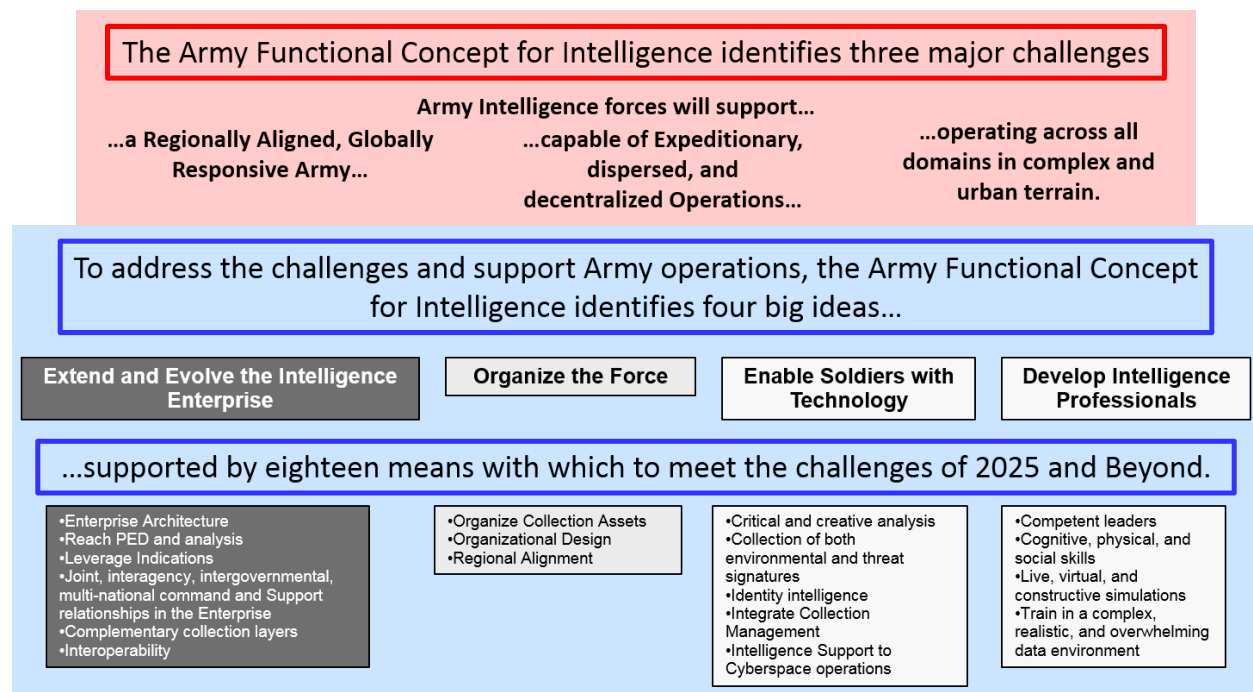
b. Integrating intelligence into operations enables joint combined arms operations to achieve national security objectives. This all occurs in a joint and multinational environment conducted by highly competent and committed leaders.



## Chapter 4

### Conclusion

- a. The AFC-I describes how the intelligence enterprise supports a regionally aligned, globally responsive, expeditionary Army across the ROMO in the most difficult conditions. It describes how the Army must extend and evolve the intelligence enterprise, how Army intelligence forces must organize, how technologies enable Soldiers to succeed in the future OE, and how the Army must recruit, train, educate, and retain intelligence professionals (see figure 4-1.). These intelligence leaders bring the capabilities together from anywhere to Army, joint, and coalition commanders worldwide, aid their understanding of fluid, complex environments, support decision making, and reduce risk.
- b. For further discussion of how Army intelligence might support the future force see the operational vignette at appendix F.



**Figure 4-1. AFC-I summary**

## **Appendix A**

### **References**

#### **Section I**

##### **Required references**

Army regulations, Department of the Army pamphlets (DA Pams), Army field manuals (FMs), Army doctrine publications (ADPs), Army doctrinal reference publications (ADRs) and DA forms are available at Army Publishing Directorate Home Page <http://www.apd.army.mil>. TRADOC publications and forms are available at the TRADOC public website at <http://www.tradoc.army.mil/tpubs>. Joint publications (JPs) are available at the Joint Electronic Library at <http://www.dtic.mil/doctrine>.

ADP 1

The Army

DA, TRADOC, Army Capabilities Integration Center (ARCIC). (2012, August 20). *Operational Environments to 2028: The Strategic Environment for Unified Land Operations*. Fort Eustis, VA.

DOD, Joint Staff. (2012, January 17). Joint Operational Access Concept, Version 1.0

DOD, Joint Staff. (2012, September 10). Capstone Concept for Joint Operations: Joint Force 2020

DOD, Joint Staff. (2013, November 1). Joint Concept for Entry Operations

TP 71-20-3

The U.S. Army Training and Doctrine Command Concept Development Guide

TP 525-3-0

The U.S. Army Capstone Concept

TP 525-3-1

The U.S. Army Operating Concept: Win in a Complex World

TP 525-3-6

The U.S. Army Functional Concept for Movement and Maneuver

TP 525-5-500

Commanders Appreciation and Campaign Design

#### **Section II**

##### **Related references**

ADP 2-0

Intelligence

ADP 3-0  
Unified Land Operations

ADP 5-0  
The Operations Process

ADRP 2-0  
Intelligence

ADRP 3-0  
Unified Land Operations

ADRP 5-0  
The Operations Process

Air Sea Battle Office. (2013, April). AIR-SEA BATTLE: Multi-Service Collaboration to Address Anti-Access & Area Denial Challenges. Retrieved from <http://www.navylive.dodlive.mil/files/2013/06/ASB-26-June-2013.pdf>

Atlantic Council. (2012). *Envisioning 2030: U.S. Strategy for a Post-Western World*. Retrieved from <http://www.atlanticcouncil.org/publications/reports/envisioning-2030-us-strategy-for-a-postwestern-world>

Cameron, Robert S. (2010). *To Fight or not to Fight? Organizational and Doctrinal Trends in Mounted Maneuver Reconnaissance from the Interwar Years to Operation Iraqi Freedom*. Retrieved from [http://usacac.army.mil/cac2/cgsc/carl/download/csipubs/cameron\\_fight.pdf](http://usacac.army.mil/cac2/cgsc/carl/download/csipubs/cameron_fight.pdf)

Chairman, Joint Chiefs of Staff. (June 2014). *Intelligence, Surveillance, and Reconnaissance, Joint Force 2020 White Paper*.

Chief of Staff of the Army, Strategic Studies Group. (2014, June). *Megacities and the United States Army, Preparing for a Complex and Uncertain Future*. Retrieved from [http://www.army.mil/article/128636/Megacities\\_and\\_the\\_United\\_States\\_Army\\_Preparing\\_for\\_a\\_complex\\_and\\_uncertain\\_future/](http://www.army.mil/article/128636/Megacities_and_the_United_States_Army_Preparing_for_a_complex_and_uncertain_future/)

DA. (2014, April 30). *2014 Army Strategic Planning Guidance*. Retrieved from <http://www.defenseinnovationmarketplace.mil/resources/ASPG2014.pdf>

Director of National Intelligence. (2014). *The National Intelligence Strategy of the United States of America*. Retrieved from [http://www.dni.gov/files/documents/2014\\_NIS\\_Publication.pdf](http://www.dni.gov/files/documents/2014_NIS_Publication.pdf)

DOD. (2012, July). *Cloud Computing Strategy*. Retrieved from <http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf>

DOD. (2014, Mar 4). *Quadrennial Defense Review Report*. Retrieved from [http://archive.defense.gov/pubs/2014\\_Quadrennial\\_Defense\\_Review.pdf](http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf)

DOD. (2012, January). *Sustaining U.S. Global Leadership: Priorities for 21<sup>st</sup> Century Defense*. Retrieved from [http://www.defense.gov/news/Defense\\_Strategic\\_Guidance.pdf](http://www.defense.gov/news/Defense_Strategic_Guidance.pdf)

DOD Directive 5100.01: *Functions of the Department of Defense and its Major Components*. Retrieved from <http://www.dtic.mil/whs/directives/corres/dir.html>

HQ INSCOM. (15 December 14). *Concept Paper: INSCOM Theater Intelligence Brigade as an Anchor Point*. Available upon request through the proponent.

JP 1-02

DOD Dictionary of Military and Associated Terms

JP 2-0

Joint Intelligence

JP 2-01

Joint and National Support to Military Operations

JP 3-0

Joint Operations

JP 4-02

Health Service Support

Legere, M. A. (2013, October). *Army Intelligence 2020: Enabling Decisive Operations While Transforming in the Breach*. The Army Green Book. Retrieved from [http://www.ausa.org/publications/armymagazine/archive/2012/10/Documents/Legere\\_GB2012.pdf](http://www.ausa.org/publications/armymagazine/archive/2012/10/Documents/Legere_GB2012.pdf)

National Intelligence Council. (2012, December). *Global Trends 2030: Alternative Worlds*. Retrieved from [http://www.dni.gov/files/documents/GlobalTrends\\_2030.pdf](http://www.dni.gov/files/documents/GlobalTrends_2030.pdf)

Odierno, R. (2012, January). *Marching Orders. 38<sup>th</sup> Chief of Staff, U.S. Army. America's Force of Decisive Action*. Retrieved from <http://usarmy.vo.llnwd.net/e2/c/downloads/234187.pdf>

Odierno, R. (2013, January). *38<sup>th</sup> Chief of Staff of the Army Marching Orders, Waypoint #1*. Retrieved from <http://usarmy.vo.llnwd.net/e2/c/downloads/280914.pdf>

TP 525-3-3

The U.S. Army Functional Concept for Mission Command

TP 525-3-4

The U.S. Army Functional Concept for Fires

TP 525-3-5

The U.S. Army Functional Concept for Maneuver Support

TP 525-3-6

The U.S. Army Functional Concept for Movement and Maneuver

TP 525-3-7

The U.S. Army Human Dimension Concept

TP 525-4-1

The U.S. Army Functional Concept for Sustainment

TP 525-8-2

The U.S. Army Learning Concept for 2015

Treverton, Gregory F. (June 2007). Risks and Riddles. Smithsonian Magazine. Retrieved from <http://www.smithsonianmag.com/people-places/risks-and-riddles-154744750/?no-ist>

U.S. Army Combined Arms Center (CAC). (2012, May 17). [Briefing]. *FY 13/14 Regionally Aligned Forces*. Briefing presented to the Chief of Staff of the Army as part of a periodic Strategy and Future Force Review session. Available upon request through the proponent.

U.S. Army Combined Arms Center. (2014, October 14). *The Human Dimension Whitepaper: A Framework for Optimizing Human Performance*. Fort Leavenworth, KS. Available upon request through the proponent.

U.S. Army Combined Arms Center (CAC). (2015, June 15). *The Mission Command Network Vision and Narrative*. Briefing presented to the Chief of Staff of the Army as part of a periodic Force 2025 and Beyond Update session. Retrieved from <http://www.benning.army.mil/mcoe/maneuverconference/content/pdf/Mission%20Command%20Network%20Narrative%20Final%2016%20June%202015.pdf>

U.S. Army Cyber Command/2nd U.S. Army. (2013, September 9). *The U.S. Army LandCyber White Paper 2018-2030*. Available upon request through the proponent.

U.S. Army Space and Missile Defense Command. (2012, April 3). *Army Space White Paper: Gaining and Maintaining Access to Space Capabilities 2012-2030*. Available upon request through the proponent

---

## **Appendix B**

### **Required Capabilities (RCs)**

#### **B-1. Introduction**

Intelligence RCs describe capabilities needed to execute the missions under the conditions described within this functional concept. RCs identify and focus intelligence capability development efforts in 2020-2040. Three of the RCs listed below are new efforts (sections B-4, B-5, and B-6), while the remaining RCs expand or refine existing intelligence requirements.

#### **B-2. Army functional concept for intelligence (AFC-I) RCs**

a. To support commanders' situational understanding in all operational environments, Army forces require the capability to do the following:

(1) Future forces require the ability to integrate an intelligence enterprise architecture which provides data transport, storage, processing, and functionality to support commanders' situational understanding in all operational environments. (AFC-I 3-4.b.; AOC 3-3.c.; CCJO p. 9, 1<sup>st</sup> para)

(2) Future forces require the ability to interoperate between Army mission command systems, intelligence partner systems, and across intelligence disciplines to support commanders' situational understanding in all operational environments. (AFC-I 3-4.c.; AOC C-2.a (5); CCJO p. 10, 2d para)

(3) Future forces require the ability to create unity of effort among joint, interagency, intergovernmental, and multinational intelligence partners using command and support relationships to support commanders' situational understanding in all operational environments (AFC-I 3-4d; AOC 2-2c & 3-3d; CCJO p. 6, 1st para & p. 10, 1st para)

(4) Future forces require the ability to create cross domain synergy through complementary collection layers (space, aerial, and terrestrial) of Army and intelligence partner collectors to support commanders' situational understanding in all operational environments. (AFC-I 3-4.f.; AOC 3-3.c; CCJO p. 7, 1<sup>st</sup> para)

(5) Future forces require the ability to distribute processing, exploitation, dissemination, and analysis to support commanders' situational understanding in all operational environments. (AFC-I 3-4.g.; AOC 3-3.b; CCJO p. 5, last para)

(6) Future forces require the ability to direct warning intelligence against military, political, economic, and social problems, to support commanders' situational understanding in all operational environments. (AFC-I 3-4.h.; AOC 3-3.b; CCJO p. 3. 3d para)

(7) Future forces require the ability to align collection, analysis, and synchronization capabilities regionally to build understanding over time, to support commanders' situational understanding in all operational environments. (AFC-I 3-5.a.; AOC 3-3.a; CCJO p. 11, 4<sup>th</sup> para)

(8) Future forces require the ability to design modular, flexible organizations that provide minimal footprint forward while supporting all levels in all operational environments. (AFC-I 3-5.b.; AOC 3-3.b; CCJO p11, 3d para)

(9) Future forces require the ability to organize collection assets to improve responsiveness, facilitate task organization, and improve system readiness to support commanders' situational understanding in all operational environments. (AFC-I 3-5.c.; AOC 3-3.b; CCJO p.11, 3d para)

(10) Future forces require the ability to conduct critical and creative intelligence analysis to support commanders' situational understanding in all operational environments. (AFC-I 3-6.a.; AOC 3-4.a (4); CCJO p. 10, 4<sup>th</sup> para)

(11) Future forces require the ability to collect both environmental and threat signatures of all operational environments to support commanders' situational understanding. (AFC-I 3-6.b.; AOC 2-3.b (5); CCJO p. 7, 2d para)

(12) Future forces require the ability to develop identity intelligence through biometrics, forensics, and document and media exploitation to support commanders' situational understanding across the ROMO. (AFC-I 3-6.c; AOC 3-3.c; CCJO p.3 4<sup>th</sup> full para)

(13) Future forces require the ability to integrate information collection across the Army and the intelligence enterprise to support commanders' situational understanding in all operational environments. (AFC-I 3-6.d.; AOC 3-3.c; CCJO p. 7, 1<sup>st</sup> para)

(14) Future forces require the ability to provide intelligence support to cyberspace operations and to conduct cyberspace enabled intelligence, to support commanders' situational understanding in all operational environments. (AFC-I 3-6.e.; AOC 3-4.b.6; CCJO p. 2, 3d para)

(15) Future forces require the ability to develop competent, agile, and resilient intelligence leaders who thrive in conditions of uncertainty and rapid change, to support commanders' situational understanding in all operational environments. (AFC-I 3-7.a.; AOC 3-3.j.)

(16) Future forces require the ability to develop Soldiers with the right cognitive, physical, and social skills and political, historical, and cultural knowledge to succeed and flourish in all operational environments. (AFC-I 3-7.b.; AOC 3-3.g. and j.)

(17) Future forces require the ability to develop live, virtual, and constructive simulations that reflect the complexity of the future OE, to support commanders' situational understanding. (AFC-I 3-7.c.; AOC B-3.b.)

(18) Future forces require the ability to train in a complex, realistic, and overwhelming data environment that replicates the vast operational and mission variables of the future OE, to support commanders' situational understanding. (AFC-I 3-7.d.; AOC C-2.a.(6).)

(19) Future forces require the ability to expand capabilities through open-source intelligence collection and analysis, including social media and publicly available information exploitation and

analysis, to enhance threat network analysis, trend analysis, pattern-of-life analysis, and predictive analysis, to support commanders' situational understanding in all operational environments. (AFC-I, 2-3.b.(1); 2-3.d.(2); 2-3.d.(4); para 3-6.a.(3); 3-6.b.(2); and 3-6.a.(2))

(20) Future Army forces require the capability to understand the interrelated cognitive, moral, physical, and socio-economic factors of the operating environment influencing human behavior in order to inform campaign and operations planning. (AFC-I, 3-6.b.(1)(d))

b. Collectively, these RCs support commanders' situational understanding in all operational environments enabling future Army forces to conduct joint combined arms operations.

### **B-3. Prioritizing future capability efforts**

a. The AFC-I RCs are not all equally important. While all may apply to the military problem identified in paragraph 3-1, they do not apply equally to the priorities that implement the central idea. Priorities align with paragraph 3-3, implementation of the central idea.

b. Three of the RCs are new efforts while the remaining RCs build on current work. This concept proposes three priority bands of capability development effort for the AFC-I RCs. The new efforts are expanded in paragraphs B-4, B-5, and B-6.

(1) Priority 1. (extend and evolve the intelligence enterprise and develop leaders)

(2) Priority 2. (organize the force)

(3) Priority 3. (enable Soldiers with technology)

### **B-4. Collection of both environmental and threat signatures (new)**

a. Future Army intelligence forces require the capability to collect environmental and threat signatures that support commanders' situational understanding of military and non-military aspects of all operational environments.

b. Description.

(1) Future OEs will be complex in their variety. Urban areas and remote locations challenge the Army's ability to conduct surveillance and understand the environment. The rise of nonstate actors complicates the human dynamic. Ideology based transnational movements add a nonhierarchical challenge to the ability to understand the environment and to attempt to predict the future. Targeting individuals rather than military resources heightens the need for biometric and other identity related capabilities, and the ability to find and track an individual in a crowd of individuals. Including biometrics, forensics, and DOMEX capabilities into identity activities enables greater precision to targeting high valued individuals, while decreasing the risks of collateral damage to innocent civilians.



(2) The rise of social media has led to the ability to influence informally very large masses. The information age has also fed the disinformation age and influenced the low information populations. The Army must also prepare for the full ROMO including nontraditional, nonmilitary, or nonlethal. These problems require U.S. forces to understand enemy systems that make decisions differently, and may have different objectives. Shaping activities may also stress the ability to understand the environment over a given threat.

c. Action.

(1) The Army must develop sensors that help the commander understand non-military aspects of the environment, including technical sensors to understand power grid capacity, water supply purity, air quality, urban weather phenomena, resource scarcity, or sewer system capacity. Commanders must understand the public health challenges to both local populations and U.S. forces and the medical capacity of the local infrastructure. Public sentiment and the impact to people of resource scarcity and insufficient infrastructure are future OE information requirements. Social infrastructure in the form of social media and economic data are rich human environment information sources.

(2) Human terrain mapping is an important tool in understanding societal, economic, political, historical, and cultural aspects and must keep pace with changes in human behavior. Non-DOD agencies and interorganizational partners collect against many of these problem sets routinely. There must be analytic models to understand infrastructure and the mechanics of political and social organizations to determine the key signatures that develop pertinent physical and social knowledge, and there must be techniques to sense those signatures.

(3) Access to targets and understanding non-military problems will force the U.S. to develop new sensors or to harness existing sources of information. Sensors must be platform flexible and report across the network to a common processor. Collection from Soldiers, including high resolution imagery, elevation data, and surface weather data will feed situational understanding. Law enforcement and private security capabilities may be critical in urban areas while new technologies may be needed in other complex terrain. Cyber capabilities may be able to diagnose the capacity and functionality of urban life support systems, and may help to influence the effectiveness of those systems.

(4) Russia, China, and other modernized states will challenge the U.S. and its allies with advanced technology. Peer adversaries have advanced precision guided munitions, lethality, protection, and mobility. Adversary UAS and EW capabilities have advanced faster than U.S. countermeasures. Sensor development must keep pace with peer or near peer conventional capabilities.

d. Result. Comprehensive collection of both environmental and threat signatures improves decision-making. Understanding the non-military aspects of the terrain, including the human terrain, improves understanding of the human element.

## **B-5. Critical and creative analysis (new)**

a. Future Army intelligence forces require the capability to conduct holistic intelligence analysis, to include decomposition of problems and the synthesis of collection against the entire operational environment, to support commanders' situational understanding in all operational environments.

b. Description. Intelligence analysis is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production.<sup>33</sup> Intelligence analysis provides awareness and knowledge of the threat, terrain and weather, civil considerations, and their impact on operations. Analysis reduces uncertainty, derives clarity, and predicts the future. Analysis is a methodical, continuous, cognitive process that requires a strategy, models, and tools which make the analyst effective. The Army default strategy for intelligence analysis centers on observing and understanding the threat. The current and future operating environments portend that the threat may not always be the deciding factor for mission accomplishment.

c. Action.

(1) Army intelligence professionals will employ advanced analytics (advanced techniques applied against complex problems) that encompass a clear strategy, flexible models, and supporting tools and skills. Currently, the strategy is threat centric, the model is geospatially oriented, and the tools and skills support this approach. While IPB is a proven geospatially based analytic model, future problems may call for a relational or temporal viewpoint. Human terrain mapping is another approach to understand better the future OE. IPB must analyze all domains to determine opportunities to generate overmatch and protect friendly freedom of action. While analysts have good tools and the skills to use them, many tools were developed for threat analysis. The intelligence architecture must support the constant update of flexible, intuitive, powerful tools that help analysts stay ahead of adversaries. The operational mission should drive the analytic approach, not the available tools.

(2) The Army must advance a holistic approach to analysis. Analysis is a cognitive skill composed of a mix of art and science: training alone will not guarantee success. Science improves speed and accuracy while the art of analysis makes the human component irreplaceable in the process. Intelligence analysis requires a complete approach beginning well before collection: the decomposition of information requirements, the research to determine information gaps and to determine best how to satisfy them, and the synthesis of information to create a timely, accurate, complete answer is all part of intelligence analysis.

(3) Uncertainty and rapid change elevate the analytic risk associated with decision-making and further compound the challenges of the environment.<sup>34</sup> Environmentally focused primary intelligence requirement may dominate future intelligence efforts, and the environment can be just as unpredictable and uncooperative at surrendering capability and intent as the threat. Primary intelligence requirement may revolve around food supplies and utilities before focusing on threat capabilities. Intelligence analysis will require creativity and imagination against non-traditional problems: these problems resemble mysteries more than puzzles.

d. Result. An option of analytic strategies and models will better satisfy commander's requirements in a more uncertain world. Good analysis during collection planning improves the quality, controls the quantity of collection, and improves the timeliness of post collection analysis.

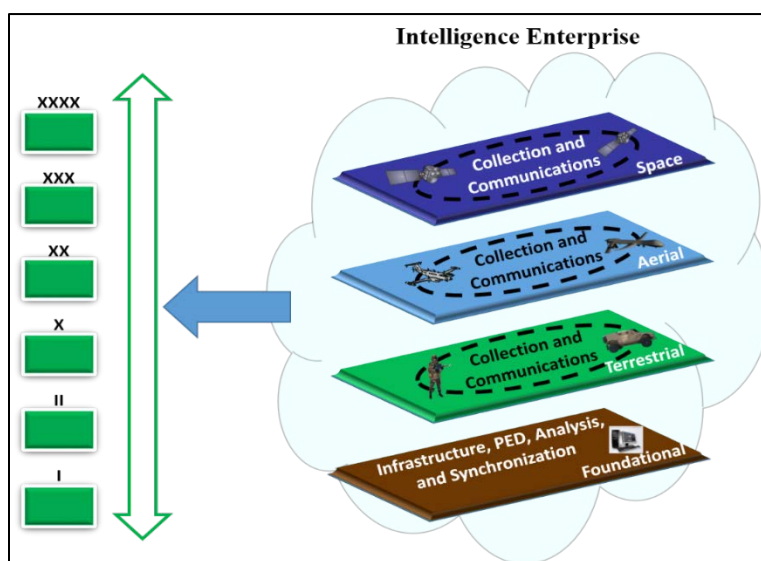
#### **B-6. Joint, interagency, intergovernmental, and multinational command and support relationships in the intelligence enterprise**

a. Future Army intelligence forces require the capability to control intelligence resources across the joint, interagency, intergovernmental, and multinational intelligence enterprise while providing responsive support to commanders' situational understanding in all OEs. When practical, command relation (tactical, operational control or general support) should also be established.

b. Description. Commanders organize the force to accomplish missions using command and support relationships. Command relationships define command responsibility and authority while support relationships define the purpose, scope, and effect desired when one capability supports another. Technical channels, while not a command or support relationship, ensure adherence to applicable laws and policies and provide technical support and guidance to plan, prepare, execute, and assess the unit's collection effort. Command relationships are hierarchical; thus a chain of command. Commanders establish support relationships when subordination of one unit to another is inappropriate. Historically, the Army assigns or attaches intelligence structure to support command structure.

c. Action.

(1) Army intelligence forces have evolved from a mostly dedicated relationship to a flatter but more capable intelligence enterprise support structure. Battalion intelligence officers (S-2) now access national capabilities through the intelligence enterprise, capabilities the Army cannot afford to assign to tactical echelons. The power of the intelligence enterprise exceeds the power of assigned or attached capabilities. The intelligence enterprise is accountable to the multiple supported commanders through a balance between command relationships and control



**Figure B-1. Intelligence support relationships**

relationships. The intelligence enterprise, specifically elements outside the U.S. military, may require a support relationship that somehow “time shares” direct support. Additionally, there may be an expansion of the technical channel construct for analysis (see figure B-1.).

(2) The Army intelligence core competencies will have different solutions for command and support relationships. Intelligence synchronization is the purview of the intelligence primary staff officer and will remain assigned to various echeloned organizations to provide the conduit between information requirements and intelligence enterprise capabilities. Intelligence collection elements must be responsive to commander’s needs; need does not need to be assigned or attached to be successful.

(3) PED and intelligence analysis may be organic or available through reach. While some analytic capacity is needed for the unique context and requirements of a specific commander; much analysis, including processing and exploitation, can be done by a supporting organization before the information is applied against a specific information gap.

d. Result. The flat intelligence enterprise will be accountable through prioritized effort supporting multiple commanders. Intelligence resources will be employed more fully throughout the OE. Command and support relationships will be clear for all collection, PED, and analysis.

---

## **Appendix C**

### **Science and Technology**

#### **C-1. Introduction**

a. Force modernization must prepare Army intelligence to support multi-domain battle (MDB), operations in dense urban areas, and highly mobile warfare. Army capability developers must extend and evolve the intelligence enterprise; modernize collection platforms and sensors to enable penetrating intelligence, surveillance, and reconnaissance and cross domain fires; integrate artificial intelligence to enable autonomous threat detection and tracking; and engineer technologies and analytic tools that manipulate large, complex data sets (including social media and open source intelligence) to enable identity intelligence.

b. The prospect of fighting in dense urban areas imposes several technical challenges. These include modern signal sets and signal propagation; identifying and understanding subterranean threat activities; mitigating the constant threat of electronic surveillance; and how to process and exploit ambient sensing yielded by the internet of things, local security and safety sensors, and the digital wakes of targeted entities. Small, numerous, affordable, and highly dispersible sensors will complement those systems already in the portfolio. Artificial intelligence and autonomous, fast flight for small unmanned aerial systems will improve manned-unmanned teaming for highly mobile reconnaissance.

c. The prospect of fighting a peer or near peer possessing sophisticated A2 and AD capabilities imposes adaptation of systems capable of continuing mission in degraded space, under GPS outage, and capable of dominating the fight for control of the electromagnetic spectrum.

## **C-2. Near-term (fiscal year (FY) 14-20) objectives: Adapt**

a. In the AOC near-term (present-2020), Army intelligence will optimize existing capabilities focused on augmented training (live and virtual); pooled analytical resources; and establishing an integrated PED strategy.

b. The Army will extend and evolve the intelligence enterprise. The intelligence enterprise comprises all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture that ensures interoperability, an inherently joint, interagency, intergovernmental, and multinational approach to intelligence operations, enabled command and support relationships, and is tailored to the professionals who make it work. Cross-domain information exchange enabled by a maturing intelligence enterprise in turn enables the quality of interoperability demanded by multi-domain battle and the requirement to fight cross-domain.

c. Army intelligence must modernize its aerial layer portfolio by integrating high-definition electro-optical/infrared, precision geolocation, hyperspectral imagery, light detection and ranging, foliage penetration, and advanced synthetic aperture radar/moving target indicator radar sensors onto airborne platforms. Army modernization will replace legacy SIGINT sensors with open-architecture software-defined receivers that are capable of theater net-centric geolocation.

d. Other near-term imperatives. The Army must extend the intelligence enterprise down to battalion and below maneuver units; enhance MIB(T)s and E-MIBs through PED centers for reach-back and analytic support; and augment virtual training of Soldiers to expand their experience and maturity to rapidly develop junior Soldiers. The pooling of analytic capability supports improved expeditionary capacity providing the commander additional flexibility and reducing the number of forward-deployed Soldiers. E-MIBs would provide training readiness assessments and employment guidance to corps and below MI assets. The analytic program of record, the Distributed Common Ground System - Army (DCGS-A) continues to integrate with federated infrastructure. SIGINT collection continuously evolves keeping pace with emerging communications technologies. The complementary collection layers will integrate into a comprehensive collection plan that incorporates the PED strategy improving analysis and processing of data received from the air and on the ground.

## **C-3. Mid-term (FY 20-30) objectives: Evolve**

a. Modernization must improve home station mission command and distributed operations which include fielding a suite of analytic processing tools to maximize the exploitation of big data.<sup>35</sup> Improving home stations capability significantly reduces the forward footprint.

b. The Army will modernize the terrestrial layer portfolio by developing a multi-role, multi-domain system that processes, fuses, and analyzes large data sets at the sensor, thus reducing the volume of off-board data transmissions, reducing the cognitive workload on analysts, and expediting actionable intelligence in formats conducive to the Army DODIN services infrastructure, mobile-handheld, mounted, and sensor computing environments. Army intelligence modernization will provide greater stand-off, non-cooperative collection and

verification capability of identity data to mitigate the threat. The Army will develop advanced multi-modal capabilities that integrate behavioral characteristics, such as gait, with biometrics (such as, facial, vascular and voice matching) and general physical characteristics linked to analytical software that will cue analysts observing persistent surveillance digital video feeds to identify individuals and their associates.

c. In the foundation layer, Army intelligence modernization will increase collaboration and integration of sensor data with predictive modeling and data analytics to allow for further increased situational understanding. The Army will expand PED capabilities with a focus on joint intelligence analysis capabilities and enterprise-enabled PED. The Army will improve continuous training with newer capabilities such as, synthetic training environment and future holistic training environment—live, synthetic. The Army will initiate the discreet use of organic networks while using data feeds from dense urban area or megacities, human machine interfaces; quantum computing, sensing, and fusion; agent-based simulation and improved predictive analysis and intelligence with a substantial increase in human dimension incorporation.

d. The Army will develop agile and adaptive Soldiers who think critically and creatively and can respond in constantly evolving environments. Advanced technology will maximize Soldier processing and analytical capacity. Improved predictive analysis technology will project future complex OEs using virtual reality to increase a Soldier's ability to process and exploit the situation. The Army will improve the capability to gather all sources of data, signals, signatures, and imagery (active or passive) including information from commercial, industrial, and other non-military domain devices (such as, the Internet of Things), support predicting social and cultural behaviors.

#### **C-4. Far-term (FY 30-40) objectives: Innovate**

a. The AOC far-term (2030-2040) focus is developing capabilities that facilitate agile intelligence operations such as optimized sensor production and exploitation of existing sensor systems (that is, the Internet of Things, joint sensor arrays), use of data analytics to discover previously unknown threat signatures, integration of those signatures in an automated pattern detection, and activity-based intelligence for a comprehensive sensor common operational picture.

b. In the space layer, Army intelligence modernization will develop autonomous networked sensors in an agnostic intelligence space layer. The Army will introduce new space capabilities that expand a self-synchronizing sensor computing environment and expand the network to include national, coalition, service, and commercial assets. Similarly, the aerial layer will improve sensor situational awareness and synchronicity with joint, interagency, intergovernmental, and multinational sensors; implement energy-saving/regenerating techniques to improve persistence and lower operating costs; and develop improved optics, precision radar sensing, and laser sensing capabilities that detect micro changes in biometry and biometric data.

c. Real-time event processing, artificial intelligence, and neuromorphic computing enable machine learning to enable more accurate and faster all-source understanding of complex situations. Agent-based simulations and game theoretic means will enable significantly improved intelligence support to deliberate planning and wargaming.

#### **C-4. Training and education**

Army modernization will integrate successive Intelligence Electronic Warfare Tactical Proficiency Trainer increments into the future live, synthetic training environment. The long term goal is to fully integrate intelligence training at all echelons and levels through one seamless live, virtual, constructive–integrating architecture within joint, interagency, intergovernmental, and multinational operations, replicating real-world conditions as much as technologically possible and affordable. Army intelligence will improve supported training for collection of environmental and threat signatures (power grids, air quality, sewer system capacity, fresh water availability, and others); integrate training for ambient sensing and exploitation of the Internet of Things”; and provide access to commercial open-source collection.

---

### **Appendix D Risk and Mitigation**

#### **D-1. Introduction**

The risks found in joint concepts, the ACC, and the AOC apply to the AFC-I. These risks inform experimentation and wargaming which follow concept development. They also serve as guideposts when developing priorities. The CCJO identifies eight risk areas created if the concept is adopted. The ACC highlights five significant risk areas. Finally, the AOC highlights six significant risk areas.

#### **D-2. Insufficient funding and inadequate capacity**

a. Advanced technology may prove unaffordable.

b. Inadequate network. The greatest dependency to adopting the ideas and capabilities in this concept is the network. A robust network and reliable connectivity between mobile, tactical elements, and fixed capabilities are critical to the intelligence enterprise. Army intelligence forces must bridge from the strategic echelon to the lowest level at the tactical edge. The intelligence enterprise requires fixed, multilevel secure networks capacity and extending two-way access to the wireless maneuver element flexibility. The network, supporting Army intelligence forces, must connect sensors, transport, computing and storage, enterprise data services, application services, and end user devices while providing assurance in a secure, interoperable, standards-based environment.

(1) The network allows the complementary collection layers to support one another, cross-cue one another, and allows tactical and strategic collection and intelligence partners to work in concert. An inadequate or unreliable network would require huge forward movement of intelligence capabilities. Reach PED and analysis, leveraging intelligence enterprise sensors, and continuous awareness all depend heavily on a robust network. In addition, storage, processing power, and analytic software all depend on a solid network to reduce forward footprint. Dynamic re-tasking of collection assets and sensor awareness would be difficult in a severely constrained network.

(2) An adequate network requires a total doctrine, organization, training, materiel, leadership and education, personnel, and facilities approach: it is not simply a materiel solution. An adequate network is a joint, interagency, intergovernmental, and multinational solution. The network is the single greatest dependency to the future Army intelligence force.

(3) The network is vulnerable to attack. The intelligence enterprise must distribute the capability among the many nodes to provide capability in the event of local disruption. Intelligence Soldiers and leaders must understand analytic processes in the event they must operate manually.

c. Inadequate lift could affect information collection, particularly during early operations. Reach capabilities will reduce lift and sustainment burdens, but relationships with supported commanders must continue. Deployability may improve if the knowledge base is complete and accessible, and reaction capabilities may improve if the intelligence force engages continuously.

d. Intelligence operations are inherently joint, interagency, intergovernmental, and multinational with dependencies on partners, both U.S. and coalition. The Army provides many unique capabilities to the intelligence enterprise, as do other partners. In some areas, the intelligence enterprise provides capabilities the Army lacks. Cuts to the intelligence enterprise outside the Army will affect Army units. Realistic training, education, and leader development will be critical to understanding the intelligence enterprise and how to leverage it to solve diverse problems.

e. The Army may not have sufficient capability to conduct cyberspace operations in a contested environment. Operating in cyberspace is a growing field that intelligence forces must support. Future policy decisions drive this risk.

### **D-3. Bureaucracy**

a. Reach capabilities across the intelligence enterprise will require command and control to remain responsive to deployed forces. Too much centralization could result in insufficient capacity to handle multiple crises. Overemphasis on decentralization may lead to lack of coordination and inefficient use of scarce resources or lack of responsiveness to commanders.

b. Standardization may lead to decreased diversity, flexibility, versatility, and effectiveness.

c. Intelligence forces rely on technological advances and infrastructure. Flexible collection capabilities and agility in adjusting to new targets requires the latest technology.

---

## **Appendix E**

### **Intelligence Teams: The Army Contribution to the Intelligence Community**

#### **E-1. Overview**

Army intelligence forces support commanders in three ways: embedded into their staffs, as multidiscipline and multifunctional units dedicated to a specific echelon, and as discipline or functionally specific units that provide general support to the force.



## **E-2. National intelligence**

Army intelligence forces continue to support the national intelligence effort through dedicated INSCOM units embedded in national agencies or operating independently with specific missions. Army intelligence professionals also serve on other agency staffs and in the national chain of command up to the White House. Army airborne intelligence collection assets, specifically the aerial exploitation battalions, will consolidate under INSCOM to provide greater worldwide flexibility.

## **E-3. Theater intelligence**

Army intelligence forces will continue to support the theater level from both a joint and a service standpoint. Army intelligence professionals will continue to serve on geographic combatant command joint intelligence staffs and will serve in geographic combatant command intelligence centers. From a service perspective, multidiscipline and multifunctional MIB(T)s are assigned under global force management to combatant commands, which typically delegate operational control to their respective ASCCs; INSCOM retains primary administrative control responsibilities for the MIB(T)s. The MIB (aerial intelligence) flies missions supporting ASCC requirements. Intelligence Soldiers will also serve on the ASCC staff.

## **E-4. Corps intelligence**

Army intelligence forces will continue to support the corps with a presence on the corps staff and a unit structure capable of satisfying the corps commander's collection requirements, accepting reinforcing capabilities, or pushing capability downward to lower echelons. The corps G-2 will have an analytic capability to satisfy the corps commander's information and intelligence requirements. An expeditionary MI brigade will be available to conduct intelligence operations, accept and integrate collection assets from outside the corps, and command corps intelligence collection assets.

## **E-5. Division intelligence**

Army intelligence forces will continue to support the division with a presence on the division staff to conduct intelligence synchronization and limited analysis. The division will receive augmentation from corps or higher to conduct collection to satisfy the commander's intelligence and information requirements. The division intelligence officer has limited organic analytic capacity.

## **E-6. Brigade combat team (BCT) intelligence**

Key to the BCT intelligence structure will continue to be the resource constrained MI company. Army intelligence forces continue to support the BCT with a presence on its staff to conduct intelligence synchronization and limited analysis. Collection and PED resources will be available from higher echelons, but the MI company will retain analytic capability and a command structure able to receive augmentation.

## **E-7. Army SOF**

Army intelligence forces will continue to support Army SOF with a presence on unit staffs down to the battalion level to conduct intelligence synchronization and analysis, with extensive reach to the intelligence enterprise. In special forces groups and the 75th Ranger Regiment, military intelligence companies, and detachments conduct multidiscipline collection to meet the

commander's collection requirements, accepting reinforcing capabilities, or pushing capability downward to lower echelons.

---

## **Appendix F**

### **Intelligence Enterprise Support to Engagement and Expeditionary Operations**

#### **F-1. Introduction**

This vignette describes how the elements in this concept might work together. Experimentation and further analysis will validate or disprove these ideas and will develop into an eventual organization and operations plan. This vignette does not address every option or nuance that might affect this scenario. To establish contrast, the appendix first describes the events in the 2015 timeframe, followed by the 2030 approach to the same circumstances.

#### **F-2. Setting**

a. The country of Landlocked is located north of the Caspian Sea in central Asia. Landlocked is a developing country with rapid growth in its largest city, Capital, a megacity, due to migration from rural areas and surrounding countries. Significant U.S. manufacturing investment has created job growth. Rapid growth has outstripped infrastructure and created societal instability. Foreign radicals have agitated the Landlocked people, causing the government concern. As explosive growth continued in Capital, services fell far behind demand resulting in sprawling slums, vast areas with no utilities, and significant public health challenges: essentially austerity in an urban environment.

b. Radicals viewed the resulting social unrest as an opportunity to challenge the Landlocked government. U.S. corporations, a significant employer in Capital, worried that production was vulnerable and their investment was at risk. Further, U.S. citizen population in Capital had grown significantly as corporate management, their families, and U.S. support structures such as schools for dependent families and private support ventures outstripped the Embassy's ability to monitor all U.S. interests. As Landlocked grew in size and economic capacity it became an increasingly important U.S. partner in a region threatened by instability.

#### **F-3. Current prevent, shape, and win scenario**

a. 1<sup>st</sup> Infantry BCT (IBCT), located at Fort Homestation, U.S.A., was heavily involved in the wars in Iraq and Afghanistan over the previous decade. The unit has many combat veterans, but 1<sup>st</sup> IBCT has not deployed in over two years. The unit trains aggressively at Ft. Homestation and has had a combat training center rotation in the past year. Many Soldiers have attended Army schools. The IBCT has an average readiness rating.

b. 1st IBCT leadership monitored Landlocked through news and theater intelligence reporting and the commander directed the IBCT S-2 to prepare a situation overview for the IBCT leadership. The S-2 contacted the 1<sup>st</sup> Division G-2 who in turn contacted the U.S. Army Central (USARCENT) G-2 asking for background on the situation and access to additional intelligence reporting. The USARCENT G-2 directed the 1<sup>st</sup> IBCT to contact the supporting MIB(T) which provided several

briefings describing the background and basic IPB of the country. Access to current information collection reporting was not immediately available due to permissions from intelligence enterprise partners and automation security authorities. The MIB(T) did, however, add 1<sup>st</sup> IBCT to distribution of finished products relating to Landlocked. Leadership canvased the 1<sup>st</sup> IBCT for anyone with experience on the ground in Landlocked or anyone who spoke the local language with limited results.

c. USARCENT increased planning in the event unrest threatened U.S. interests and the National Command Authorities directed military action to restore stability to the country. A warning order directed 1<sup>st</sup> IBCT to begin preparations for operations in Landlocked. The 1<sup>st</sup> IBCT staff began planning and identified initial information gaps. The S-2 requested information from 1<sup>st</sup> Division which in turn requested information from USARCENT. USARCENT satisfied some gaps from existing holdings, but 1<sup>st</sup> IBCT collection requirements were not yet a priority to the combatant command. As the situation in Landlocked continued to deteriorate, the U.S. Government decided to intervene militarily. FORSCOM identified 1<sup>st</sup> IBCT as available and directed deliberate planning.

d. The 1<sup>st</sup> IBCT staff identified challenges and information gaps. There was no intermediate staging base within 500 miles of Landlocked which would create problems to entry operations. A near peer conventional power often unfriendly to the U.S. loomed across the Landlocked border. The staff identified numerous capability shortfalls and requested augmentation for information collection, linguists, PED, analytic capacity, and requested access to current intelligence reporting on the crisis. Meanwhile, the 1<sup>st</sup> IBCT MI Company began packing collection and other intelligence systems for movement. The 1<sup>st</sup> Division G-2 established an overwatch cell to support the 1<sup>st</sup> IBCT until it could operate forward. Three issues caused serious concern to the IBCT commander: maintaining continuous situational understanding, interoperability with partners, and continuous reconnaissance and surveillance from entry operations through redeployment.

e. The 1<sup>st</sup> IBCT, as part of a joint task force, positioned forward in Turkey to prepare as a follow on force into Landlocked. Upon arrival, the IBCT S-2 established secure connectivity with the MIB(T) to maintain awareness. The S-2 was able to access intelligence prepared for the USARCENT commander, but it lacked the fidelity necessary for 1<sup>st</sup> IBCT operations. The S-2 submitted requests for information, but theater priority supported other service anti access activities. 1<sup>st</sup> IBCT waited for successful entry by SOF and subsequent transport into Landlocked. U.S. dominance of air, space, and cyber domains convinced regional players to remain neutral.

f. After SOF secured the Capital airport, 1<sup>st</sup> IBCT arrived in Landlocked. The JTF assigned 1<sup>st</sup> IBCT a sector near the airport to organize for combat operations. The IBCT MI company arrived late in country, complicating IBCT information collection. Additionally, the IBCT S-2 lacked connectivity directly with anyone except the JTF J-2 and could not access raw collection from intelligence partners. The IBCT commander deployed ground reconnaissance, but assets had limited range and capabilities. In time, combat operations drove the organized resistance elements away from Capital and further from Landlocked.

g. After offensive operations ceased, the JTF commander assigned a sector of Capital to 1<sup>st</sup> IBCT to reestablish rule of law. 1<sup>st</sup> IBCT established liaison with local government agencies, but

relied on local nationals for language support. The 1<sup>st</sup> IBCT S-2 requested JTF provide counterintelligence support for screening linguists and other local officials, but no support was available. The 1<sup>st</sup> IBCT MI Company provided HUMINT Soldiers to conduct limited screening. After 30 days, 1<sup>st</sup> IBCT prepared for transition of authority with a unit better prepared to assist Landlocked rebuild. 1<sup>st</sup> IBCT redeployed to Ft. Homestation and assessed their recent deployment.

h. 1<sup>st</sup> IBCT was not prepared for the mission in Landlocked. It had no institutional knowledge and was unable to establish timely relationships with supporting intelligence agencies. 1<sup>st</sup> IBCT could not maintain continuous awareness and understanding of developments in Landlocked due to connectivity and permissions. Additionally, the IBCT lacked cultural and language capabilities. There were also intelligence discipline specific capabilities unavailable to the IBCT. Upon arrival in country, the IBCT lacked immediately available information collection capability and lacked access to intelligence partner collection. The IBCT lacked the organic capacity to provide detailed, timely, and uninterrupted intelligence support to the IBCT commander and was unable to access support until late in the process.

#### **F-4. Future prevent and shape scenario**

a. The timeframe for this vignette is 2030. The intelligence enterprise provides access to focused intelligence collection, data, and products driven by commanders at all levels and available to all echelons. Technically and procedurally, the intelligence enterprise delivers ease of use and access to enormous amounts of data, information, and intelligence. Intelligence forces align and organize to provide focused, responsive, tailorable support across the ROMO. Intelligence collection sensors are multi-disciplined, deployable, survivable, and versatile. Intelligence analysts train to solve a wide range of problems that match the challenges of the OE and have tools which quickly use the vast amounts of data available to them. Intelligence professionals enter the Army with a solid understanding of technology and have a basic grasp of global dynamics.

b. U.S. Army Central is following the situation in Landlocked. The ASCC G-2 has an intelligence architecture centered on the USARCENT-aligned MIB(T). The MIB(T) is structured and resourced to meet theater requirements. It provides intelligence products to support the ASCC commander, maintains a common operational picture, conducts and synchronizes intelligence collection, and provides training for FORSCOM units regionally aligned to USARCENT and has DCGS-A connectivity down to battalion level. The MIB(T) has well established relationships across the intelligence enterprise. The MIB(T) has unfettered access into interagency and national databases and understands the relevant intergovernmental and multinational structures and their data stores. The MIB(T) coordinates closely with the U.S. Army Europe MIB(T) as this potential crisis is on the unified command plan seam. The MIB(T) understands the formal relationships with central Asian countries and alliances for intelligence sharing and has informal relationships with nongovernmental organization and leading commercial entities. The MIB(T) has relationships with host nations for identity related data. This established the country's identity database and will be used for the identification and vetting of possible threat and/or criminal personnel. The MIB(T) trains regionally aligned Army forces and offers focused products to units conducting engagement. The MIB(T) has a close relationship with the TSOC to facilitate SOF missions into the theater.

c. As part of the regional alignment of forces, FORSCOM aligned the 1<sup>st</sup> Division to USARCENT and 1<sup>st</sup> IBCT of the 1<sup>st</sup> Division to the region containing Landlocked. 1<sup>st</sup> IBCT, stationed at Ft. Homestation, USA, immediately established a relationship with the MIB(T) and began building a knowledge base on Landlocked to support future IBCT missions. The S-2 established relationships with PED and production centers (includes the IROC). The S-2 learned the collection resources available to the combatant commander and established accounts to request collection. The S-2 worked with the IBCT commander to establish intelligence requirements as he educated the IBCT leadership on the Landlocked operational environment. USARCENT included 1<sup>st</sup> IBCT in their engagement plan, further focusing the IBCT intelligence effort. Because Landlocked much larger northern neighbor, Robust, has significant conventional capabilities and has been known to interfere in Landlocked internal affairs, USARCENT alerted the 1<sup>st</sup> Division to prepare to deploy if the situation escalates.

d. Steady state monitoring of the region provided awareness of the situation in Landlocked. Joint and national collection as well as engagement opportunities provided awareness of the normalcy in the region. The combatant commander's theater engagement plan provided engagement and training opportunities. Military engagement identified demands on sustainment, fixed and mobile communications, cyber electromagnetic activities, security, and mobility that generated information requirements. The MIB(T) leveraged those engagement opportunities to fill these and other information gaps. Engagement also established relationships between U.S. forces and authorities in Landlocked, setting conditions for future interoperability. Through engagement, the ASCC and RAFs had an improved understanding of the geography, extent and condition of the infrastructure, society culture and language, security forces capability, and those wishing to destabilize Landlocked capabilities. Partnering with Landlocked improved knowledge of the OE while posturing for future operations. Meanwhile, theater and national intelligence collection monitored Robust conventional forces moving near Landlocked's northern border while Robust announced an aggressive exercise schedule near the border.

e. Engagement activities allowed the MIB(T) to build considerable multi-domain knowledge of Landlocked and Capital, focusing on many non-traditional problem sets. Understanding of the Capital urban area required a multidimensional view of the terrain and society. Understanding the surface, subsurface, supersurface, interior, and exterior dimension of the urban terrain, understanding the cyber and electromagnetic environment that supported Capital, understanding the cultural, societal, criminal, and governmental factors of Landlocked all expanded the creativity of analysts. Using area, structures, capabilities, organizations, events, sewage, water, electricity, academics, trash, medical, safety, and other considerations, as well as the information structure to understand the urban environment was far different from preparation based primarily on terrain, weather, and the enemy. The National Geospatial-Intelligence Agency updated geospatial databases and all available geospatial products. The National Center for Medical Intelligence produced medical intelligence analysis focused on potential health risk assessments; identification, assessment, and reporting on infectious disease risks; assessment of foreign military and civilian medical capabilities; assessment of foreign and domestic medical S&T across joint combined arms operations; and other medical intelligence issues to protect U.S. interests in Landlocked. The National Security Agency updated electronic databases to support intelligence, electronic warfare, and cyber activities. The MIB(T) placed collection and production demands on the system and monitored activity for potential future action.

f. The 1<sup>st</sup> Division also developed multi-domain IPB products along Landlocked's northern border. Robust represents a sophisticated adversary with traditional, irregular, catastrophic, and disruptive capabilities. Robust has mechanized brigades, sophisticated long-range fires that overmatch U.S. capabilities, a dense air defense and AD integrated system of disruptive capabilities, insurgent forces, weapons of mass destruction, and technological capabilities to disrupt friendly cyber and space systems. Robust also has significant space and air capabilities and limited maritime capabilities on the Caspian Sea. U.S. access to Landlocked is limited to air with equipment pre-positioned in Turkey. As part of the engagement effort, the U.S. moved an armored BCT (ABCT) equipment set to Landlocked for a joint training exercise.

g. Radicals, with clandestine support from Robust, viewed the mounting challenges in Capital as an opportunity to topple the government and establish control of Landlocked. Radicals viewed U.S. manufacturing ventures as a ready source of plunder to finance the transition to a fundamentalist theocracy. Radicals fueled discontent among the working population fostering widespread protests and lawlessness. Landlocked security forces could not protect both government and U.S. interests. U.S. corporations and citizens flooded the U.S. Embassy with requests for protection. After a week of continuous unrest radicals seized the Capital airport and the Landlocked government requested military support from the U.S. Government.

h. The ASCC G-2 anticipated the potential intervention because of the seamless operation between the G-2 and MIB(T) and their effective utilization of activity based analysis and query of the dynamic world-graph as a part of their warning intelligence requirements. The engagement presence of Army forces provided contextual support to the events happening in the country. The MIB(T) shifted collection and production focus to confirm and update intelligence to overcome the entry challenges, monitor the threat on the northern border, and support follow-on missions. As the theater commander surged collection using joint and national assets, other Army analytic resources in INSCOM and FORSCOM shifted focus to reinforce joint and national PED and analytic centers. The increase in collection required an increase in processing, exploitation, and analysis to support operational planning and early entry forces. Select IROC facilities across FORSCOM re-focused from lower priority missions to support the collection surge.

i. At Ft. Homestation, regionally aligned units began planning with specific intelligence requirements. The Army drawdown had reduced the MI assets assigned to the BCT, so the expeditionary MI brigade provided augmentation for tactical collection assets and the architecture to provide the PED and analytic support. Integration of non-intelligence sensors organic to combat and other vehicles also increased tactical signals and imagery collection capacity. Intelligence enterprise relationships established during prevention and shaping were confirmed. Aerial and space collection layers provided GEOINT and SIGINT information while the U.S. Embassy provided HUMINT and OSINT reporting. INSCOM formed a task force of manned and unmanned assets from the Military Intelligence Brigade (Aerial Intelligence) (MIB(AI)). The isolation of Landlocked and lack of a close intermediate staging base would impact Army collection prior to entry operations. This placed increased dependence on intelligence partners and connectivity to associated PED centers for awareness until the division established itself in country. The division

G-2 planned for continuous support from pre-deployment preparation at Ft. Homestation through movement and entry operations until forces could establish a functioning architecture on Landlocked soil.

j. Due to range and access considerations, much of the collection supporting early entry forces would come from joint, national, and partner assets. The G-2 and BCT S-2s planned to remain connected to the MIB(T) for continuous updates during movement and initial operations. The MIB(T) remained the anchor point for two way information flow between the intelligence enterprise and committed forces. As operational planning progressed, the MIB(T) ensured geospatial products of the entry site were current as well as routes into Capital. Mobility in Landlocked would be a challenge as Capital was urban, austere, and far from potential operations along the Landlocked northern border. The S-2s would need to confirm and update infrastructure studies conducted during engagement and vet relationships established during engagement (see figure F-1).

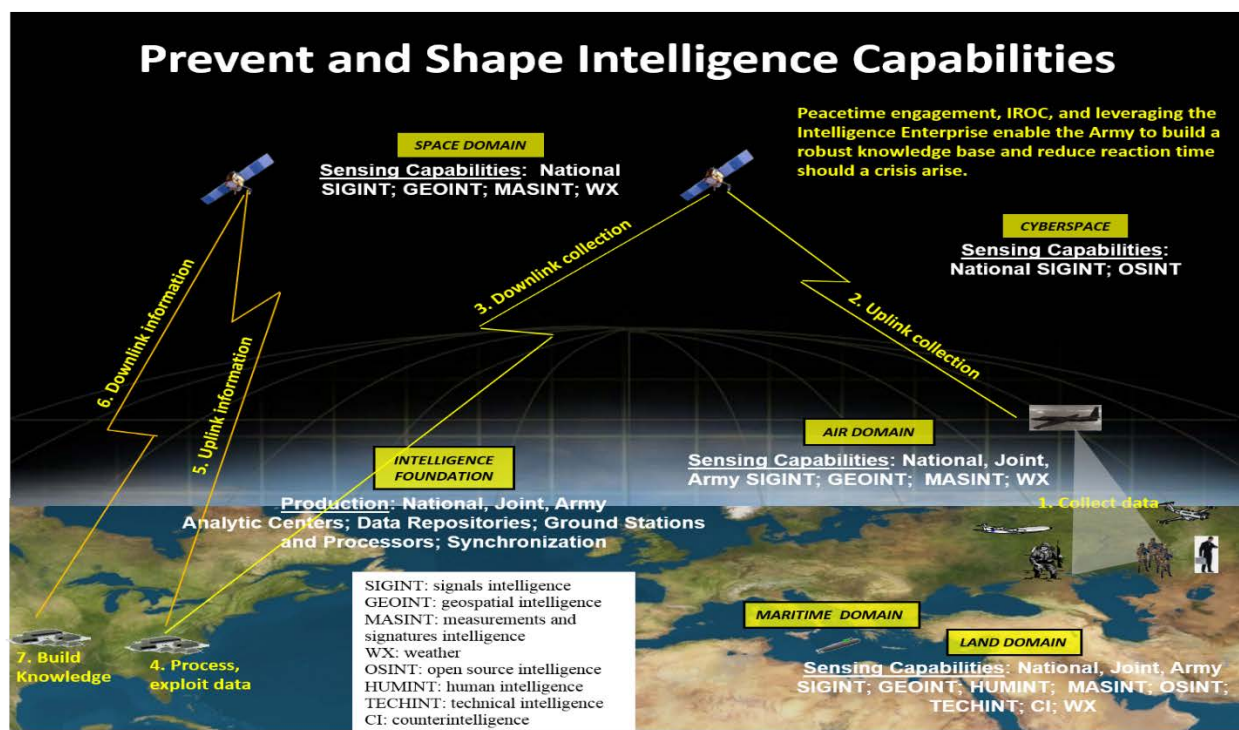


Figure F-1. Prevent and shape intelligence capabilities

## F-5. Future win scenario

a. As more of the intelligence enterprise focused on the worsening situation in Landlocked and satisfaction of information requirements resulting from detailed operational planning, the MIB(T) remained the focal point between the intelligence enterprise and the operational units. The MIB(T) deconflicted requirements and ensured the intelligence enterprise delivered support to the 1<sup>st</sup> Division. The operational plan called for the initial location of the forward command post at Outback, a remote airfield in Landlocked that was still securely in government control but distant from Capital. The ABCT prepositioned set was moved to Outback located midway between

Capital and the northern border region. The MIB(AI) task force deployed forward and ensured overflight rights between stationing and Landlocked. The MIB(T) embedded a support team into the forward and main command posts to ensure uninterrupted flow of intelligence to entry units.

b. The JTF headquarters designated 1<sup>st</sup> IBCT as the initial conventional entry force. As 1<sup>st</sup> IBCT completed planning and loaded onto transport, the division G-2 assumed responsibility for providing situational awareness during movement. Limited communications into the transport aircraft required prioritized reporting. The G-2 understood the IBCT commander's primary intelligence requirement and knew his reporting thresholds. The G-2 also understood the database updates the IBCT S-2 would need once established in Landlocked and ensured the information was available from the MIB(T). Because Landlocked did not have a good alternate airport, SOF had the forced entry mission to secure the Capital airport prior to 1<sup>st</sup> IBCT's arrival. Success or failure of joint airpower and SOF entry was unknown when the initial elements of 1<sup>st</sup> IBCT departed Ft. Homestation, so updates determined if the IBCT would enter Capital directly or divert to the alternate airfield at Outback. 1<sup>st</sup> IBCT was two hours from Capital when the IBCT received word the Capital airport was secure, allowing 1<sup>st</sup> IBCT to execute its primary plan.

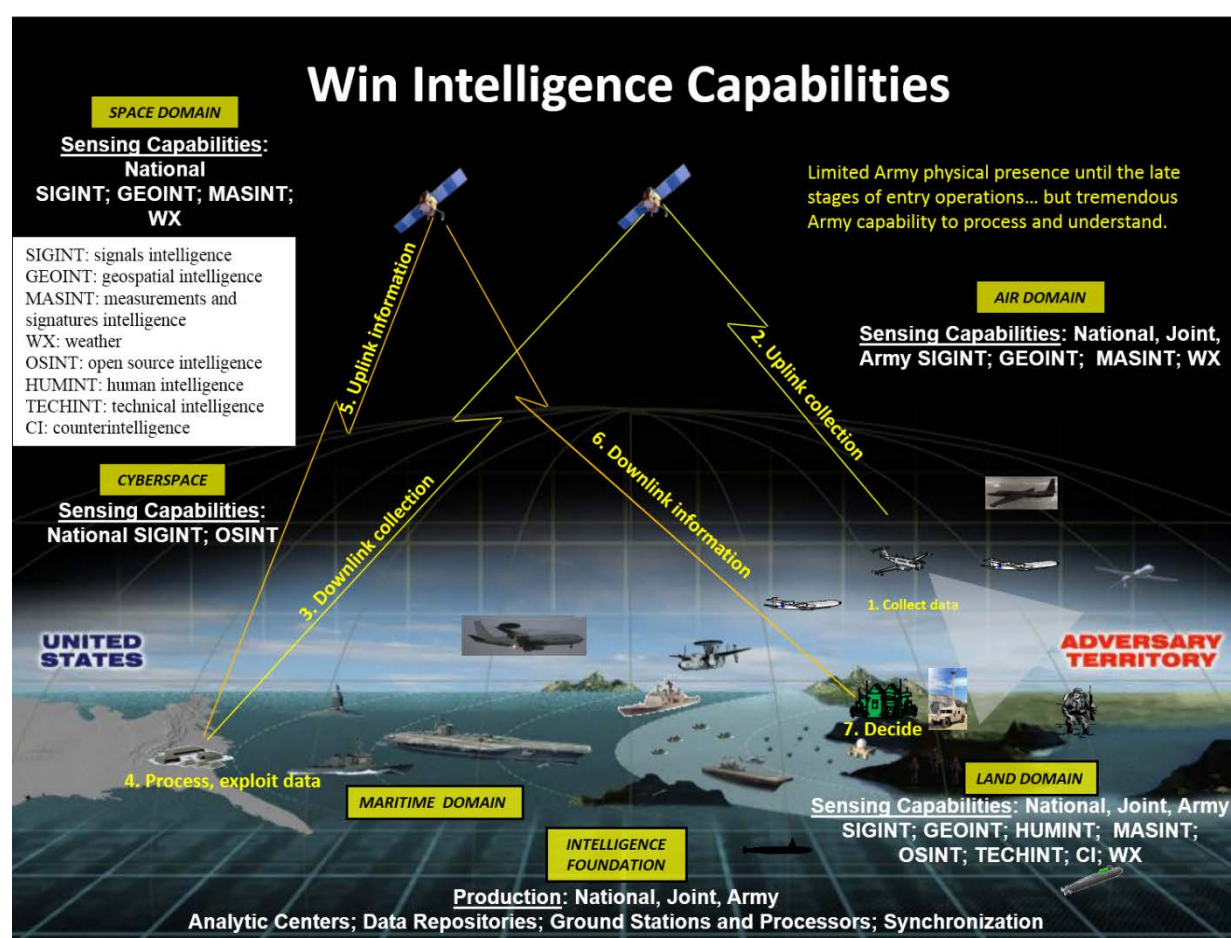
c. 2d ABCT had the mission to flow into Outback, occupy the prepositioned equipment set, and move north to block any conventional threat from Robust. 3d Stryker BCT (SBCT) would then flow into Outback and reinforce 2d ABCT as needed. The division G-2 planned collection to support the non-contiguous operations of forces in Capital and the northern border region. Support for 1<sup>st</sup> IBCT relied heavily on HUMINT, OSINT, and SIGINT while support for 2d and 3d BCTs relied heavily on SIGINT and GEOINT. Of note, the internet of things heavily supported situational understanding in Capital while FM communications intelligence and moving target indicator (MTI) GEOINT was crucial to understanding the situation along the northern border. Multi-domain IPB identified windows in time and space where U.S. forces could achieve positions of advantage over Robust forces across the domains. The JTF J-2 coordinated with Landlocked maritime forces in the Caspian Sea to attach U.S. teams with sophisticated maritime surveillance equipment to monitor the JTF southern flank.

d. Within 24 hours of landing and offloading the IBCT established headquarters near the Capital airport. The headquarters established communications with the MIB (T) and thus the intelligence enterprise, providing updates and access to collection platforms. The IBCT MI company, including assets attached from the expeditionary MI brigade, immediately employed improved expeditionary tactical collection assets to protect initially the force and transition to offensive operations to defeat the insurgents. MICO HUMINT and E-MIB CI elements established liaison with local security and law enforcement agencies. Intelligence partner assets continued to collect against threat forces in Capital and in the countryside while assessing infrastructure damage that would affect military operations. 1<sup>st</sup> IBCT quickly engaged hostile forces as it began planning for re-establishing stability in the Capital area. While hostile forces were destroyed or dispersed quickly, the local unrest and lack of confidence in the Landlocked government kept tensions high (see figure F-2).

e. 2d ABCT fell in on prepositioned equipment and departed Outback for blocking positions along the northern border. 2d ABCT developed a comprehensive SIGINT picture networking all combat radios with MICO SIGINT systems, aerial collection systems, and space systems. This



electronic mapping directly supported ABCT offensive and defensive cyber and electronic warfare efforts. UAS cleared routes ahead of the semi-independent ABCT while joint systems mapped forward positions. Joint MTI detected Robust forces marshalling along the northern border: the attached PED platoon from the E-MIB tracked the MTI while on the move. Meanwhile, 3d SBCT arrived in Outback, offloaded equipment, and configured for movement to reinforce 2d ABCT. 3d SBCT S-2 connected to the network, populated databases, and initiated collection to establish local situational awareness.



**Figure F-2. Win intelligence capabilities**

f. After the immediate combat operations subsided and the radical threat was dispersed, 1<sup>st</sup> IBCT shifted to support the Landlocked government. Intelligence forces' focus shifted from offensive operations to force protection and to rebuild the nation: the area, structures, capabilities, organizations, events area, structures, capabilities, organizations, events, sewage, water, electricity, academics, trash, medical, safety, and other considerations factors. The conflict damaged the systems and infrastructure of the city and other areas of Landlocked. The MIB(AI) task force searched for any indication of an insurgent resurgence while providing imagery of damaged infrastructure. In the north, Robust forces stood down and redeployed to garrison locations after the situation in Capital stabilized. Restoration of adequate utilities and services was a priority for both U.S. forces and the Landlocked government, and the MIB(T) focused collection

efforts to determine capability and capacity. MIB(T) counterintelligence assets and other INSCOM counterintelligence assets entered the country to screen local nationals and identify remaining radicals or criminal elements seeking to capitalize on the instability.

g. GEOINT efforts focused on the condition of the local infrastructure and confirmation of Robust redeployment. The U.S. Ambassador's priority was to restore U.S. corporate capabilities which would re-employ local nationals and restart the economy. This would further support Landlocked efforts to rebuild from the destruction caused by the fundamentalist generated unrest. U.S. forces provided security and facilitated the reception and distribution of U.S. and international aid. The ASCC requested and received foreign disclosure authority to bolster Landlocked intelligence. As part of transition planning, the 1<sup>st</sup> IBCT S-2 developed plans to transition to another U.S. force, coalition force, or local authority. These sequels differed due to the interoperability and authority capabilities of the options. 2d ABCT and 3d SBCT returned to Outback and prepared for redeployment.

h. As the situation in Landlocked stabilized the 1<sup>st</sup> IBCT transitioned efforts to local intelligence and security forces while narrowing focus to force protection as the IBCT prepared to redeploy. The MIB (AI) task force redeployed. The MIB(T) arranged for a HUMINT team to remain in the U.S. Embassy after the bulk of U.S. forces departed. Upon return to Ft. Homestation, the 1<sup>st</sup> Division G-2 re-established relationships needed to support home station operations and prepare for any future contingency. The MIB (T) returned to daily operations as well, updating databases and addressing intelligence architecture issues resulting from the recent crisis. Members of the intelligence enterprise resumed normal patterns of collection and analytic production.

---

## **Appendix G**

### **Intelligence Force Modernization Strategy**

#### **G-1. Force 2025 and Beyond**

The Army intelligence force modernization strategy is Force 2025 and Beyond. The theme of the strategy is to optimize Army intelligence forces to support a force operating in complex environments against determined, adaptive enemy organizations. The strategy has three phases: adapt (now-2020); evolve (2020-2030); and innovate (2030-2040).

#### **G-2. Adapt (2014-2020)**

a. Adapt existing capabilities to support the regionally aligned globally responsive forces to achieve Army Force 2020. The Army will extend the intelligence enterprise from space to mud, national to tactical, establish the theater MI brigades as regional "anchor points," and establish the Army PED center for reachback and enhanced PED support.

b. Redesign military intelligence brigades to provide expeditionary and regionally aligned support to the force. (AFC-I 3-5.)

c. Pool capabilities and establish reach PED and architecture to support expeditionary operations more efficiently. (AFC-I 3-4.b.f.)

d. Facilitate operations and intelligence convergence integrating Distributed Common Ground System-Army into the federated infrastructure. (AFC-I 3-4.c.)

e. Modernize SIGINT collection to maintain overmatch. (AFC-I 3-6.b.)

f. Conduct cognitive enhancement proof of concept into source operations course (35M HUMINT course). (AFC-I 3-7.b.)

g. Migrate collection systems to multi-intelligence platforms. (AFC-I 3-5.b.)

h. Integrate foundational, terrestrial, aerial, and space layers. (AFC-I 3-4.e.)

### **G-3. Evolve (2020-2030)**

a. Evolve new and existing capabilities through learning, careful modernization, and limited investment to achieve Force 2025. The Army expands distributed operations to include analysis and to enhance Soldier cognitive ability for learning and analysis.

b. Support RAF through distributed analysis using federated data and collaboration. (AFC-I 3-4.f.)

c. Develop analytic processing tools to harness big data and include social media in OSINT. (AFC-I 3-6.a.)

d. Link operational and institutional training through improvements in the synthetic training environment. (AFC-I 3-7.b.)

e. Increase collection capabilities through a tactical meshed network and the network as a sensor. (AFC-I 3-4.b.)

f. Implement new instructional approaches for accelerating learning (such as, cognitive learning techniques). (AFC-I 3-7.b.)

g. Develop a sensor common operating picture for rapid visualization and fine tuning of collection systems. (AFC-I 3-6.c.)

h. Reduce size, weight, and number of single function sensors significantly. (AFC-I 3-5.b.)

### **G-4. Innovate (2030-2040)**

a. Develop new and existing capabilities to achieve fundamental change to meet future OE requirements and Force 2025 and Beyond. The Army improves predictive analysis and to optimize sensor employment and exploitation.

b. Exploit the Internet of Things, social media, and advanced encryption techniques, including open source sensors. (AFC-I 3-6.b.)

- c. Improve predictive analysis to project the future operating picture in non-deterministic and complex situations. (AFC-I 3-6.a.)
  - d. Improve intelligence, surveillance, and reconnaissance synchronization by reducing the need for unplanned sensor maneuver. This involves automated synchronous sensors. (AFC-I 3-6.c.)
  - e. Implement energy saving techniques to enable persistent surveillance. (AFC-I 3-5.b.)
  - f. Utilize live and virtual environments patterned after complex urban terrain, specifically megacities. (AFC-I 3-7.b.)
  - g. Predict threat behavior in all models, experiments, and wargames. (AFC-I 3-6.a.)
- 

## **Appendix H**

### **Implications of a Regionally Aligned and Globally Responsive Force to Army Intelligence Forces**

#### **H-1. Introduction**

Regional engagement is a central element of the AOC and RAF support is a primary challenge to Army intelligence identified in the AFC-I.<sup>36</sup> This appendix expands the discussion to identify the challenges to Army intelligence as it supports an RAF that is also globally responsive. Support to an RAF and globally responsive force Army requires situational understanding and providing that understanding requires setting the theater for intelligence, building regional partners, and managing Army intelligence talent effectively.

#### **H-2. Support situational understanding**

- a. An RAF requires situational understanding to prevent conflict, shape security environments, and win wars. Regional alignment provides focus to a CONUS-based force across a wide range of threats and operating environments. It provides opportunities to increase readiness. Situational understanding allows commanders to engage across the ROMO.
- b. For an RAF to engage, it must have some understanding of culture and language. Army intelligence must have greater depth in culture and language to support the commander with timely and predictive analysis and to prepare forces for engagement opportunities.
- c. Army intelligence must develop situational understanding through action. This action includes leveraging the intelligence enterprise for non-Army capabilities and supporting Army engagement. Engagement opportunities develop understanding if managed properly. Providing engagement forces awareness of gaps and capturing observations upon return build knowledge.
- d. Understanding normalcy allows commanders to recognize change. RAFs may influence events across the ROMO if they understand conditions have changed. Continuous presence provides a baseline of normalcy and the ability to recognize change that may require a change in engagement.

### **H-3. Setting the theater for intelligence**

a. Setting the theater for intelligence purposes is an activity that sets conditions for intelligence operations across the ROMO. Setting the theater occurs early and is a combatant commander responsibility. For the Army, the ASCC G-2 must ensure Army capabilities are included.

b. Intelligence architecture is fundamental to setting the theater for intelligence.<sup>37</sup> All available information collection must be connected to the PED, analysis, and decision-making capabilities of the theater. The architecture allows the foundation layer of the intelligence operational framework to function. Intelligence architecture requires interoperability, security, policies, and procedures. Architectures incorporate different intelligence partners in each operational circumstance.

c. Building theater knowledge is a continuous part of setting the theater.<sup>38</sup> It requires establishing a baseline knowledge of threat and environmental factors that could impact military operations. Building knowledge facilitates mission analysis for joint combined arms operations across the ROMO. OSINT contributes significantly to building knowledge. Cooperation with industry may provide the most detailed and current information on infrastructure and demographics. Engagement opportunities are an excellent source of information gathering if there is an effort to satisfy gaps and detect changes. Conventional and SOF teams that rotate through a region gain valuable insights but must be interviewed methodically to capture insights for the benefit of future teams. This is a collection management problem.

d. Army intelligence must support operations into theater. U.S. forces travelling into a region must prepare for potential threats. Army intelligence must replicate the theater architecture and organization for FORSCOM MI units at home station and at the combat training centers. Teams must prepare for public health challenges, cultural differences, and language issues. All engagements are military operations and require intelligence support to prepare the force and provide appropriate overwatch while deployed. The ASCC G-2 must oversee all activity in the region to influence preparation, provide overwatch, and satisfy information gaps.

### **H-4. Assisting partners and building relationships**

a. RAFs assist partners and build relationships.. A global land power network requires partners with mutual interests. Often in the past, the U.S. recruited surrogates to further U.S. foreign policy with varying results. Partners are not surrogates. Partners are members of the intelligence enterprise even if participation varies due to formal agreements.

b. Building partner relationships establishes standards and facilitates interoperability. Initially, partners bring different levels of technology and different cultural perspectives to intelligence operations. There are several coalition technology solutions to improve interoperability, but the issue is more than hardware and software. Capability development must consider partner interoperability. Cultural perspectives are consideration for policies and procedures.

c. Building partner intelligence capabilities involves improving what partners contribute to, leverage, and learn from, the intelligence enterprise. Partners may add entire capability portfolios based on relationships established with RAFs. Training partners in techniques and procedures improves the quality of their contribution and reliability of information. Training also may influence respect for human rights and democratic values in some partners.

d. Assisting partners increases trust and information sharing. Engagement and training build trust at the individual and institutional levels. As trust builds, the U.S. and partner nations explore areas of mutual interest and benefit. These areas develop into intelligence sharing agreements. Sharing agreements established before military operations help build regional knowledge and facilitate warning.

e. Building intelligence partners strengthens the global land power network. The intelligence enterprise is larger than Army intelligence forces, and intelligence partners offer options across the ROMO. Partners offer different cultural insights, language capability and capacity, and access to information sources.

#### **H-5. Talent management of an RAF**

a. An RAF needs proper management. Army talent management practices (including accessions, education, assignments, and advancement) must align with requirements of an RAF. Without institutional agility, the Army will not reap the maximum benefits of regional alignment.

b. Accessions. Access Soldiers with the technical, cultural, cognitive, and physical potential to succeed in a complex world.

c. Education. Realistic and challenging training develops Soldiers after accession. Formal training and education create Soldiers that thrive in uncertainty. Soldiers require joint, interorganizational, and multinational educational opportunities to prepare them for future operational assignments.

d. Assignments. Assign Soldiers consistent with their training and education. Recurring assignments within a regional problem set are important for Soldiers at all levels. Soldiers must remain stabilized to develop the expertise and relationships that are the benefits of an RAF.

e. Advancement. Reward Soldiers regardless of the region for which they specialize. Evaluations, promotions, and command-selections should remain consistent across the Army. Soldiers who excel in one region should rarely transfer to an unfamiliar region at the expense of Soldiers who have spent extensive time in the region.

---

## **Appendix I**

### **Expeditionary implications to Army Intelligence Forces**

#### **I-1. Introduction**

Future Army forces will be more expeditionary and its support must be equally expeditionary. The AOC defines expeditionary as the ability to deploy task-organized forces on short notice to austere locations, capable of conducting operations immediately upon arrival.<sup>39</sup> Army intelligence forces must be available quickly, relevant immediately, and productive under austere conditions. A properly organized, trained, and equipped force reduces the number of tradeoff decisions required in time of crisis.

#### **I-2. Available rapidly**

- a. Speed to the crisis is a critical element of expeditionary operations.
- b. Army intelligence forces must organize to support tailoring. Organization must facilitate rapid task organization of trained and ready forces across intelligence disciplines to provide the capabilities and capacity to support the mission. Capability must be accessible to the commander responsible for the mission, with the training and readiness gained from large densities, and the integration that develops from frequent interaction.
- c. Army intelligence forces must have a smaller forward footprint. Equipment and teams must be smaller. Size, weight, power, and cooling considerations determine which capability deploys early and which deploys later. Each Soldier assigned to a team must be agile and versatile; formations must be expeditionary. As strategic lift decreases, capability must fit efficiently into available transport and be immediately employable. Forced entry units require immediately employable collection capability and the associated PED and analysis to support decision-making. Forward stationing or prepositioning reduces the need for lift.
- d. Capability does not need to be deployed forward to be effective. Army intelligence forces must examine opportunities for reachback and leverage available intelligence partner assets to provide the capability and capacity the commander needs. Capability that does not deploy is available immediately.

#### **I-3. Relevant immediately**

- a. Army intelligence forces support the commander before initial warning uninterrupted through mission accomplishment. A CONUS-based Army requires lift from another service and support until established on the ground. Operations from an intermediate staging base or unopposed entry may be common, but Army forces must prepare for forcible entry.
- b. Expeditionary operations require continuous support for routine engagement or detailed planning for forcible entry and operations to achieve strategic objectives. Complex, fluid situations could change during the time required to deliver the force to the crisis area. Army intelligence forces must use all means available from the intelligence enterprise to meet these needs.

c. Army intelligence forces alone do not have the capability or access to priority targets to meet continuously the commander's information requirements. Army collection, PED, analysis, and intelligence synchronization assets must work with intelligence partners to eliminate any gaps in support due to capability, timing, or capacity. Army intelligence forces must be available early in the force flow but must have access to capability prior to establishment in a forward area.

d. Army intelligence forces must support targeting in fluid situations, often using non-Army collection, PED, or even analysis. In anti-access situations, Army PED and analysis may support joint attack platforms using reachback. Intelligence leaders must ensure no gaps in support to the commander.

#### **I-4. Austerity component**

a. Army forces work under austere conditions, both technically and physically.

b. Army intelligence forces require a robust network to support reach operations. Many scenarios involve semi-independent operations in areas that lack a sophisticated information network, stable power and trained personnel to operate it. Moreover, Army forces are vulnerable to adversaries' efforts to compromise or further disrupt and or degrade the network, resulting in loss or lack of technological superiority. Additionally, it may take time before DOD information networks are robust enough to support operations. Army intelligence forces must have procedures to mitigate this technical austerity. Additionally, physical austerity in the form of extreme weather or climate conditions may negatively affect Soldiers and equipment.

c. The size of the Army force may compound the impact of austerity. Austerity impacts life support, force protection, sustainment, and the health of the force. For disaster relief and humanitarian missions, austerity may be the greatest challenge to the commander.

d. Army forces require the ability to expand capability to accomplish strategic objectives. Austere conditions may require significant resources to sustain the force before it can transition to offensive operations. Army intelligence forces must integrate into the force flow with many competing priorities.

---

## **Appendix J**

### **Complex and Urban Terrain**

#### **J-1. Introduction**

a. Despite having similar components of urban terrain, each megacity has unique complexities and characteristics that complicate understanding the strategic environment and challenge existing intelligence collection and analysis capabilities. Currently, traditional DOD information collection techniques are not robust enough to understand the rapidly changing urban environment located in large urban areas. The AFC-I describes issues facing the Army given the challenges of declining budgets while improving its ability to monitor large urban populations. The AFC-I also discusses



capabilities for collecting information for phase 0 (shaping) situational awareness and providing situational understanding should the Army become involved.

b. The Army has capabilities suitable for urban operations; however, megacities are different due to size and complexity. In 2030-2040, megacities challenge military operations aimed at securing vital national and partner interests. Due to its complexity and size, the Soldier's ability to operate in the megacity requires new capabilities, concepts, and doctrine.<sup>40</sup>

c. The Army gained urban combat experience during Operation Iraqi Freedom in Fallujah (pre-war population estimate 350,000) and Baghdad (pre-war population 6 million); however, it has not yet conducted operations in a megacity. Army intelligence forces must develop a deep situational understanding of city-level analysis that defines the nature of major urban areas. Changes are required for the Army to adapt its intelligence warfighting function to meet the challenges in this emerging global security environment.

d. Army intelligence forces are ill prepared currently to support operations in growing megacities where host nation governments have difficulty keeping up with infrastructure and resource requirements. Regional instability drivers already present and in many places grow daily. Further, megacities are not the focus of the joint and national intelligence communities. This lack of focus further complicates phase 0 preparation and adds risk particularly in regions where the Army has minimal collection capability and access in place.

e. Megacities exhibit numerous characteristics that make them a unique and extremely complex operational environment. Taken individually or as a whole, these variables can change quickly and complicate ground operations exponentially. Figure J-1 summarizes some of the challenges the Army faces regarding megacity situational awareness and situational understanding.

**Table J-1.**

**Variables that converge to make megacities a complicated operational environment (OE)**

<ul style="list-style-type: none"> <li>• Magnitude/Scale – Do not scale linearly</li> <li>• Phase 0/1 preparation (shaping/deter) <ul style="list-style-type: none"> <li>- Role of special operations forces</li> <li>- Embassy/Department of State</li> </ul> </li> <li>Regionally aligned forces, joint, interagency, intergovernmental, multinational by nature</li> <li>• intelligence, surveillance, reconnaissance challenges <ul style="list-style-type: none"> <li>- SIGINT / HUMINT surveys</li> <li>- Subterranean layers</li> </ul> </li> <li>• Socio-cultural sensitivity</li> <li>• Extremely complex environment <ul style="list-style-type: none"> <li>- Multiplicity of actors</li> <li>- Adaptive threats</li> <li>- No controlling actor</li> <li>- Asymmetric threats (No rules)</li> <li>- Chaotic conditions</li> <li>- Key terrain</li> <li>- Population centric (human dynamic)</li> <li>- Intelligence preparation of the battlefield</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Key influencers (people)</li> <li>• Denial and deception / anti-access</li> <li>• Advanced niche weapons</li> <li>• Hit and run/stand-off attacks</li> <li>• Political engagement/operations</li> <li>• Impact of cyber domain <ul style="list-style-type: none"> <li>- Sophisticated information operations</li> <li>- Technology enabled</li> </ul> </li> <li>• Coalition warfare</li> <li>• Criticality of local police capability <ul style="list-style-type: none"> <li>- Intelligence</li> <li>- Legitimacy</li> </ul> </li> <li>• Necessity of indigenous capability</li> <li>• Simultaneous full spectrum</li> <li>• Morphing/multiple adversaries</li> <li>• Conventional force planning ratios obsolete <ul style="list-style-type: none"> <li>- Insufficient forces to clear/isolate city</li> </ul> </li> <li>• Tactical success not necessary</li> <li>• Non-linear dispersed operations</li> <li>• End state versus victory difficult to define</li> </ul>
--	---

## **J-2. Current gaps and RCs**

a. The six key variables discussed in this appendix are drivers that influence future intelligence concepts refinement, intelligence warfighting function gaps identification, RCs, and force modernization decisions. The work to correct deficiencies is on-going; however, more work and coordination is required.

b. IPOE.

(1) IPOE is currently country-based and inadequate for analyzing a large, complex city as a system. Information collection in phase 0 is most accurate, easiest and cheapest to acquire, but becomes less so as the situation develops. The Army intelligence forces must begin to ramp up megacity IPOE now to prevent a cold start. The Army must update doctrinal urban analytical models to cover unique megacity variables and complexity. Current IPB doctrine lacks objective measures and definitions to characterize megacities. To facilitate IPOE the Army needs better mechanisms to get tactical information from local sources to Soldiers and planners.

(1) Data access is critical. The Army should engage, as necessary, with industry and academia for local expertise, information, and views on the situation. Army intelligence forces need access to multiple sources, such as SOF, local law enforcement, interagency, intergovernmental, industry, and academia, while on the move. Big data management and information overload requires automated data mining tools for balancing priorities and managing data latency. The RAF concept is a key component to the IPOE solution. A possible solution to performing city IPOE is to tie RAF to MIB(T)s.

c. Geographic combatant command operational requirements. Combatant commander's missions provide priorities and context for planning. Combatant commander requirements must be defined clearly in terms of the types of operations forecasted and intelligence production requirements identified and prioritized for relevant intelligence to the edge to be effective. Combatant command requirements affect RAF intelligence production and required capabilities. Large urban environment analysis is critical to advising the commander concerning the OE for RAF. Knowing all partners is a key component of building RAF relationships and sharing information. Interagency engagement and education is required through integration of defense attaches with RAF forces, as is educating RAF intelligence Soldiers on roles and capabilities of TSOCs to improve SOF integration with conventional capabilities. Combatant commands seek ways to develop RAF relationships by exercising relationships through integrated RAF-oriented exercises and training from combatant command to squad level.

d. Multidimensional sensors.

(1) Population and structural and signal density in urban environments produce physical and virtual clutter that reduces the effectiveness of intelligence collection, and complicates target acquisition. Market saturation of cell phones and other web-enabled devices produce a signal-dense environment which complicates target acquisition and SIGINT collection. Further, three dimensional maneuver spaces in urban environments present a departure from the horizontal target engagement that Army intelligence analysts are accustomed to supporting. The cumulative effect

of the sheer density of the environment creates a scenario of sensory and capability overload. Physical flows and connectedness are easy to see in a city; however, information-based relationships are difficult to see in most complex systems.

(2) Increasing proliferation of personal mobile communications is making connectedness more robust at the personal level adding to the difficulty of identifying relationships. The density of information and communications technologies may slow our ability to identify actionable intelligence. Non-digital information flows remain an important form of connections and are more difficult to detect or monitor than digital systems. In many cities, information still spreads by word of mouth in the market, on the street, or from the pulpit. Further, standard communication systems may not work in or under cities (for example, satellite communications, and line-of-sight radios).

e. The Army does not have enough resources to solve all sensor issues. Some capabilities required to support large, complex urban operations include:

- Stand-off and unattended biometrics capabilities (such as, facial and iris recognition).
- Ability to geo-locate (beyond line of sight, multi-intelligence), analyze, and affect networks.
- Interoperability with host nation, interagency, law enforcement, and others.
- Enhanced virtual training (modeling and simulation).
- Persistent surveillance (“unblinking eye”).
- Minimize human-in-the-loop for data to decision process.
- Single-pass collection assets to reduce orbits.
- Automated human language technology.
- Exotic sensors—micro-unmanned aerial systems, sense-through-the-wall, ground-penetrating radars.
- Scalable and not platform-specific assets.
- Ability to tap into existing infrastructures and systems.
- Enable partners to collect, store, and share information.

f. Human dynamic. Megacities bring new requirements for understanding the population’s impact on the OE and conflict drivers. This will require new technical capabilities, human terrain mapping, and modeling obtained through open source study, engagement, and staff expertise prior to action. Determining the causes of a conflict may not be possible due to the variables involved. Neighborhood-level knowledge is critical to understanding the complex interactions in cities. Socio-cultural analysis should start in phase 0; made available widely, and updated continuously. Socio-cultural analysis should attempt to minimize humans in the loop, as this capability will allow more area analysis at greater fidelity.

g. Engagement. The intelligence community must engage aggressively and continuously with partners during phase 0 and phase 1 (deter) operations to avoid surprise. Access to and interoperability with SOF and U.S. government interagency knowledge and databases (specifically Department of State) fill many of these information needs. Interoperability with host nation law enforcement, local governments, civilian agencies, and unofficial authorities facilitate information sharing between interagency, SOF, and conventional forces.

h. Infrastructure. Megacities are key strategic terrains. Initially, cities emerged along trade routes, such as harbors, ports, rivers, and ground transportation, and are now hubs of modern economies. Megacities such as Cairo and Karachi occupy unique positions in relative proximity to global commons like the Suez Canal and the Indian Ocean. These urban centers continue to evolve into condensed networks of economic hubs which drive the global economy. Some megacities hold access to critical natural resources, like petroleum; other cities are global commerce hubs or possess untapped or unidentified resources critical to the global economy.

### **J-3. Characteristics of complex and urban terrains**

a. Unified Quest 14 identified the tactical, operational, and strategic megacity operational challenges for Force 2025 and Beyond. At the tactical level, megacities are a complex terrain challenge. Within the megacity, terrain has multi-level layers: subsurface, surface, elevated (buildings), and airspace. Additional factors within the megacity are cyber, communication, and information realms. Multi-level terrain and complexity pose unique challenges. Successfully operating in a megacity requires forces to maneuver throughout multiple layers (surface, subsurface) and domains (air, space, and others) simultaneously to achieve required effects.

b. At the operational level, the megacity is an obstacle that hinders access to entire regions and requires new approaches to sustaining operations. Population congestion, enemy fires, security, disease, or a persistent threat environment may prohibit basing in a megacity. Joint Force vulnerabilities include dependency on improved ports or intermediate staging bases and an inability to secure lines of communication through a megacity.

c. At the national and strategic levels, the megacity is linked inextricably to global economic prosperity. The catastrophic implications of future conflict affecting specific megacities warrant significant attention across all tenets of national power. Ideally, the megacity will prove a source of continued progress globally, and allow nations and people access to the freedoms and benefits currently available to developed states and highly structured population centers. However, the strategic risk associated with emerging megacities resides at the convergence with other well documented trends, such as resource scarcity, wealth disparity, and others.

d. Megacities are complex systems that demand highly agile and adaptive forces to operate successfully within them. Infrastructure varies radically, with concentrations of high-tech transportation and globally connected air- and sea- ports intermixed with open landfills, overburdened sewers, and makeshift power grids. Living habitats extend from the high-rise to the ground level tenement to subterranean labyrinths. Social structures in many cities are challenging, if not dysfunctional. Historic ways of life clash with modern living, and ethnic and racial differences often intensify in the crowded and impersonal urban space. In this environment, criminal and ideological networks offer opportunity for the growing masses of unemployed. Megacities have the potential to become the native environment for non-nation state, unaligned individuals, and organizations that live and work in the shadows of national rule.

e. The digital environment has limitless potential to multiply and expand. Over 100 countries in the world already have cell phone subscriptions that exceed their populations.<sup>41</sup> By 2030, the number of Internet-capable telecommunications devices in megacities around the world will

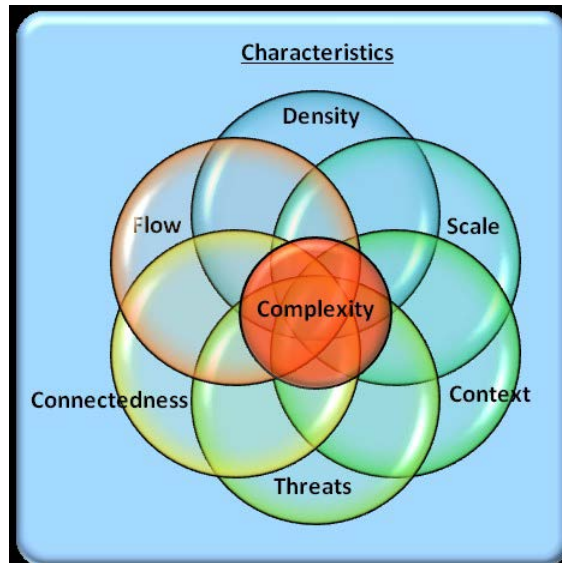
exceed their populations.<sup>42</sup> Sophisticated and illicit economies and decentralized crime syndicates threaten digital security and trade. Growing access to global communications give adversaries unprecedented global reach. Increases in connectivity add to human targeting complexity as a smaller number of adversaries intermingle with the larger and increasing number of mobile-connected citizens.

f. “The subterranean environment (tunnels, subways and sewers) is a sub-condition of the OE infrastructure. The subterranean environment is particularly important for the U.S. military to understand as it represents a potential area of vulnerability for U.S. forces. When properly exploited by the threat, it provides countermeasures and an effective level of protection against weapons systems and intelligence collection assets. U.S. adversaries have shown they are extremely adept in this environment, which presents a situation in which a threat could potentially overmatch the U.S. despite the U.S.’s technological superiority. Historical examples of threats exploiting the subterranean environment include, the Vietnam War (combination of regular and irregular forces) modern day Korea (regular force), Afghanistan (irregular forces), and the U.S.-Mexican border (criminal elements). Technologically inferior adversaries have secured tactical, operational, and strategic victories over the U.S. by using the subterranean environment.”<sup>43</sup> To overcome these urban challenges, the Army must integrate the technological enablers with reconnaissance and security efforts.

#### **J-4. IPOE analytical methodologies**

a. The Army has current doctrinal analytical frameworks directed at analyzing urban environments; however, these methods do not adequately address the complexity in a megacity scenario.<sup>44</sup> Army intelligence forces need refined theater, strategic, and operational concepts to address better intelligence support to large, complex urban operations and missions. The Army should revise FM 2-91.4 to include cyber, local governance and socio-cultural (human dynamic) analysis at a minimum, and then republish. The proper IPOE or analytical construct for megacity operations must include cause and effect relationships, connectedness, demographics, and socio-cultural interaction across all domains.

b. The scale of megacities, the multiplicity of relationships at play within them, and their global connectedness defy efforts to map or fully understand them. Application of reductionist approaches discussed in current doctrine fails to address the multi-domain variables and behaviors of the city as a whole. Multi-domain IPB must consider different approaches to modeling cities. The Chief of Staff of the Army’s special studies group proposed a new analytical methodology (see figure J-1) to achieve strategic appreciation that involves consideration of characteristics including context, scale, density, connectedness, flow and a threat profile. The city-specific interplay between these characteristics, combined with unique combinations of instability and capacity drivers reveals a typology that can be useful for categorizing megacities and thinking about what the Army might do if operating in cities.



**Figure J-1. Megacities complexity**

c. Rapid ungoverned population growth, separation, gentrification, environmental vulnerability, resource competition, and hostile actors drive instability in urban environments. These drivers individually will probably not compel military action; however, when these factors combine to exceed city capacity to modify its systems or adapt, the situation may require additional resources to reestablish a stable state.

## **J-5. Conclusion**

a. Success requires the Army to take a long-term approach to building a strategic appreciation for each megacity environment, and developing regionally focused, urban competent forces for the regions and cities where they operate. Army intelligence forces must conduct experimentation and exercises to identify the required capabilities needed to ensure successful support to future ground operations in large, complex urban environments.

b. Megacities are the result of on-going global urbanization and are becoming the epicenters of human activity. As such, they generate most of the friction which compels future military intervention. Threats to U.S. interests abroad and to the homeland will emanate from these globally connected and chaotic urban centers.

c. Understanding how these environments may become magnets for international instability and demand military intervention aids military planners in avoiding future strategic surprises. The growing significance of large, complex urban environments will make their stability critical for U.S. policy objectives and global balance. Failure to focus attention on megacities will create strategic vulnerability for the U.S. in the future.

## **Appendix K**

### **RC Crosswalk with Army Warfighting Challenges**

#### **K-1. Introduction**

The AFC-I RCs support the twenty Army warfighting challenges as they implement the central idea of this concept. (See table K-1 for a graphic rollup.)

#### **K-2. Army warfighting challenges**

a. Develop situational understanding. Each RC identified in the AFC-I supports situational understanding.

b. Shape the security environment. The AFC-I supports shaping activities. Interoperability allows partner integration at the data level for each unique environment. Command and support relationships will vary by environment and time. Reach architecture will vary by environment and each environment will require a unique warning set. Regional alignment will match linguists and analytic expertise to specific theaters. Analytic techniques must be tailorable to unique problem sets, each environment will have a unique collection posture requiring a unique collection common operating picture. Each environment will have a unique cyberspace footprint. Multiple environments require multiple complex simulations rich in tailored open source data. The Army intelligence force engages from peacetime through combat operations across the ROMO.

c. Provide security force assistance. The AFC-I supports security force assistance through a unique and established intelligence enterprise architecture, including reach, interoperable with the unique partners of the region. Regional alignment ensures the proper skill sets to exercise unique analytic techniques. Identity intelligence enhances security force assistance with individual level detail on key players. RAFs leverage the intelligence enterprise to support engagement and satisfy information gaps.

d. Adapt the institutional Army. The AFC-I supports an institutional Army through leader development and training. Complex simulations using very large data sets allow the Army to make informed decisions regarding force modernization.

e. Counter-WMD. The AFC-I supports reduction, elimination, and mitigation of WMD using focused, comprehensive collection against unique signatures and cooperation with enterprise partners.

f. Homeland operations. The AFC-I supports homeland operations within the limits of Army regulation 381-10, U.S. Army Intelligence Activities, with an interoperable, intelligence architecture, connecting partners using focused collection and analysis against homeland threats.

g. Conduct space and cyber electromagnetic operations and maintain communications. The AFC-I supports cyber electromagnetic activities through an interoperable intelligence architecture among intelligence community partners focused collection in the cyberspace domain. Simulations using big data enable the force to operate in the cyberspace domain.

h. Enhance training. The AFC-I supports enhanced training using advanced analytic techniques to enhance Soldier skills. Complex simulations using big data improve analytic skills.

i. Improve Soldier, leader, and team performance. The AFC-I supports Soldier, leader, and team building through a joint, interagency, intergovernmental, and multinational intelligence architecture that supports leader development and training. Complex simulations using big data sharpen Soldier and leader use of advanced analytic techniques.

j. Develop agile and adaptive leaders. The AFC-I supports agile, adaptive, and innovative leader development through continuous engagement and warning within the complex OE using the joint, interagency, intergovernmental, and multinational intelligence enterprise. Realistic training supports operations across the ROMO.

k. Conduct air-ground reconnaissance. The AFC-I supports air-ground combined arms reconnaissance through an interoperable, joint, interagency, intergovernmental, and multinational intelligence architecture across all domains. The AFC-I supports a comprehensive collection common operating picture and collection against all relevant targets in the operational environment.

l. Conduct joint expeditionary maneuver and entry operations. The AFC-I supports forcible and early entry leveraging available partner capabilities in concert with Army capabilities through the extended, interoperable intelligence enterprise. Collection across all domains supports warning and partners support Army forces when Army information collection is not yet available.

m. Conduct wide area security. The AFC-I supports security across wide areas through cross domain synergy of focused collection which is processed and analyzed across the interoperable, joint, interagency, intergovernmental, and multinational, distributed intelligence enterprise to provide timely support to combined arms teams.

n. Ensure interoperability and operate in joint, interorganizational, and multinational environment. The AFC-I supports working with partners through a properly organized Army intelligence force serving as a member of a global network of partners bound by agreements to share collection and analysis to support common interests. The intelligence enterprise is inherently joint, interagency, intergovernmental, and multinational.

o. Conduct joint combined arms maneuver. The AFC-I supports combined arms air-ground maneuver through cross domain synergy of focused collection which is processed and analyzed across the interoperable, joint, interagency, intergovernmental, and multi-national, distributed intelligence enterprise to provide timely support to combined arms teams.

p. Set the theater, sustain operations, and maintain freedom of movement. The AFC-I supports setting the theater using a tailored architecture and a properly organized force supporting engagement during peacetime and crisis in order to develop a relevant knowledge base. Army intelligence forces develop partners to strengthen the global intelligence network. Complex simulations support knowledge development for unique theaters, develop warning indicators, and develop information gaps.



q. Integrate fires. The AFC-I supports Army, interorganizational, and multinational fires integration through cross domain synergy of focused collection which is processed and analyzed across the distributed intelligence enterprise and interoperable with fire control information systems to provide timely targeting support to defeat the enemy and preserve freedom of action. Complex simulations support increased sensor to shooter linkage and identify sensor to shooter gaps.

r. Deliver fires. The AFC-I supports fires through cross domain synergy of focused collection which is processed and analyzed across the distributed intelligence enterprise and interoperable with fire control information systems to provide timely targeting support and battle damage assessment to defeat the enemy and preserve freedom of action. Complex simulations support increased sensor to shooter linkage and identify sensor to shooter gaps.

s. Exercise mission command. The AFC-I supports the mission command philosophy through a properly organized force leveraging the interoperable, distributed intelligence enterprise to develop situational awareness for commanders to make decisions and reduce risk. Information collection against all targets, to include individuals, supports situational understanding across the ROMO. Complex simulations using big data stress the network to identify gaps and weaknesses.

t. Develop capable formations. The AFC-I supports formations capable of rapid deployment and operations across the ROMO through a properly organized force that is trained, ready, tailorable, and agile. The Army intelligence force provides multidiscipline and single discipline teams with the right language and cultural skills able to integrate into combined arms teams capable of expeditionary, dispersed, and decentralized operations.

**Table K-1.**  
**AFC-I RCs and warfighting challenges crosswalk**

[illegible]

## **Glossary**

### **Section I Abbreviations**

A2	anti-access
ABCT	armored brigade combat team
ACC	Army Capstone Concept
AD	area denial
ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AFC-I	Army functional concept for intelligence
AOC	Army Operating Concept
ARCIC	Army Capabilities Integration Center
ASCC	Army service component command
BCT	brigade combat team
CAC	Combined Arms Command
CCJO	Capstone Concept for Joint Operations
CONUS	continental United States
DA	Department of the Army
DA Pam	Department of the Army pamphlet
DCGS-A	Distributed Common Ground System - Army
DOD	Department of Defense
DOMEX	document and media exploitation
DSCA	defense support of civil authorities
FM	field manual
FORSCOM	U.S. Army Forces Command
FY	fiscal year
GEOINT	geospatial intelligence
GPS	global positioning satellite
HUMINT	human intelligence
IBCT	infantry brigade combat team
INSCOM	U.S. Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
IPOE	intelligence preparation of the operational environment
IROC	intelligence readiness operations capability
JCEO	Joint Concept for Entry Operations
JOAC	Joint Operational Access Concept
JP	joint publication
JTF	joint task force
MI	military intelligence
MIB(AI)	military intelligence brigade (aerial intelligence)
MIB(T)	military intelligence brigade (theater)
OE	operational environment
OSINT	open source intelligence
PED	processing, exploitation, dissemination

RAF	regionally aligned forces
RC	required capability
ROMO	range of military operations
SBCT	Stryker brigade combat team
SIGINT	signals intelligence
SOF	special operations forces
S&T	science and technology
TRADOC	U.S. Army Training and Doctrine Command
TSOC	theater special operations command
U.S.	United States
WMD	weapons of mass destruction

## **Section II**

### **Terms**

#### **allocation**

Distribution of limited forces and resources for employment among competing requirements (JP 5-0).

#### **apportionment**

Distribution of forces and capabilities as the starting point for planning (JP 5-0).

#### **assign**

To place units or personnel in an organization where such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel (FM 3-22).

#### **cloud computing**

Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as, networks, servers, storage, applications, and services) that can be provisioned rapidly and released with minimal management effort or service provider interaction (National Institute of Standards and Technology).

#### **cognitive dominance**

A position of intellectual advantage over a situation or adversary that fosters proactive agility over reactive adaptation, facilitating the ability to anticipate change before it occurs (Human Dimension white paper).

#### **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 (JP 2-01).

#### **identity intelligence**

The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest (JP 2-0).

**intelligence community**

All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role (JP 1-02).

**intelligence enterprise**

The sum total of the intelligence efforts of the entire U.S. intelligence community, comprising all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture, and the Army's intelligence warfighting function (ADP 2-0).

**intelligence warfighting function**

The related tasks and systems that facilitate understanding the enemy, terrain, and civil considerations (ADRP 3-0).

**regionally aligned forces**

Army units assigned to combatant commands, those Army units allocated to a combatant command, and those Army capabilities distributed and prepared by the Army for combatant command regional missions (AOC).

**situational understanding**

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

**special operations**

Operations requiring unique modes of employment, tactical techniques, equipment, and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk (JP 3-05).

**special operations forces**

Those forces designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations (JP 3-05).

**warning intelligence**

Those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against U.S. entities, partners, or interests (approved for inclusion in JP 1-02).

**Section III****Special terms****expeditionary maneuver**

The rapid deployment of task-organized combined arms forces able to transition quickly and conduct operations of sufficient scale and ample duration to achieve strategic objectives.

**joint combined arms operations**

Synchronized, simultaneous, or sequential application of two or more arms or elements of one service, along with joint, interorganizational, and multinational capabilities combined with leadership and education across services to ensure unity of effort and create multiple dilemmas for the enemy to seize, retain, and exploit the initiative.

**intelligence layers \***

The operational framework for the intelligence enterprise; includes three collection layers and a foundation layer with intelligence disciplines applied across the layers.

**Internet of things**

The network of physical objects or things embedded with electronics, software, sensors, and connectivity to enable the Internet to achieve greater value and service by exchanging data with the manufacturer, operator, and/or other connected devices.

**Resilient data**

Architectural components that recover quickly and continue mission even when there has been a temporary network failure or other disruption.

---

**Endnotes**

---

<sup>1</sup> AOC, p. 17.

<sup>2</sup>Situational understanding: The product of applying analysis and judgment to relevant information to determine the relationship among the operational and mission variables to facilitate decision making (ADP 5-0).

<sup>3</sup> AOC p. 8.

<sup>4</sup> AOC, pp. 11-12.

<sup>5</sup> AOC, p. 31.

<sup>6</sup> Multi-domain is inherent in the operational environment per JP 3-0: The JFC's operational environment is the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment (which includes cyberspace).

<sup>7</sup> Commanders identify, accept, and mitigate risk to the mission. Intelligence information and analysis is often incomplete if timely or untimely if complete. Intelligence information and analysis informs the commander on environmental and threat factors, factors which are uncooperative at best and often intentionally deceiving. How the senior intelligence officer manages intelligence analysis could amplify the risk a commander must accept or mitigate.

<sup>8</sup> Warning intelligence replaced indications and warnings in JP 2-0, Intelligence 22 Oct 13.

<sup>9</sup> JCEO, p. 28.

<sup>10</sup> Processing, exploitation, dissemination is the execution of the related functions that converts and refines collected data into usable information, distributes the information for further analysis, and provides combat information to commanders and staffs.

<sup>11</sup> JCEO, p. 25.

<sup>12</sup> JOAC, p. 34.

<sup>13</sup> JCEO, p. 27.

<sup>14</sup> JCEO, p. 27.

<sup>15</sup> JOAC, p. 34.

<sup>16</sup> Megacities are ones with a population of 10 million or more.

<sup>17</sup> Mission variables are mission, enemy, terrain and weather, troops and support available, time available, civil considerations. Operational variables are political, military, economic, social, information, infrastructure, physical environment, time.

<sup>18</sup> This is Army warfighting challenge #1. AOC, p. 31.

<sup>19</sup> The intelligence community includes the Central Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of Treasury, Defense Intelligence Agency, Drug Enforcement Administration, Federal Bureau of Investigation, National Geospatial Intelligence Agency, National Reconnaissance Office, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Air Force Intelligence, Army Intelligence, Coast Guard Intelligence, Marine Corps Intelligence, Naval Intelligence.

<sup>20</sup> JIOC-I was the first instantiation of access to theater and national databases by tactical units.

<sup>21</sup> For example, INSCOM functional brigades that specialize in all-source analysis, counterintelligence, HUMINT, or SIGINT.

<sup>22</sup> The infrastructure and systems that convert collection to intelligence products. See glossary for further description of intelligence layers.

<sup>23</sup> AOC, p. 42.

<sup>24</sup> ADP 2-0, p. 5.

<sup>25</sup> As defined by National Institute of Science and Technology, cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (such as, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing services can be described by their shared characteristics, by the computing resources provided as a service, and by the method of deployment (DOD Cloud Computing Strategy, July 2012).

<sup>26</sup> JP 2-01.

<sup>27</sup> ADRP 2-0, p 4-12.

<sup>28</sup> ADRP 2-0, glossary 4.

<sup>29</sup> ADRP 2-0, p 4-12.

<sup>30</sup> Concept Paper: INSCOM Theater Intelligence Brigade as an Anchor Point. p. 2.

<sup>31</sup> Expeditionary maneuver is the rapid deployment of task organized combined arms forces able to transition quickly and conduct operations of sufficient scale and ample duration to achieve strategic objectives.

<sup>32</sup> Commanders identify, accept, and mitigate risk to the mission. Intelligence information and analysis is often incomplete if timely or untimely if complete. Intelligence information and analysis informs the commander on environmental and threat factors, factors which are uncooperative at best and often intentionally deceiving. How the senior intelligence officer manages intelligence analysis could amplify the risk a commander must accept or mitigate.

<sup>33</sup> ADRP 2-0.

<sup>34</sup> Commanders identify, accept, and mitigate risk to the mission. Intelligence information and analysis is often incomplete if timely or untimely if complete. Intelligence information and analysis informs the commander on environmental and threat factors, factors which are uncooperative at best and often intentionally deceiving. How the senior intelligence officer manages intelligence analysis could amplify the risk a commander must accept or mitigate.

<sup>35</sup> Big data, from a military intelligence perspective, is defined as, "deliberately and peripherally collected volumes and varieties of data made available at varying velocities and veracities (the four V's) that has the potential to yield insight and context beyond the commander's priority information requirement and information requirement if exposed to the analyst's attention, machine learning, or automated analytic software." From ICOE.

<sup>36</sup> An RAF is defined as, those Army units assigned to combatant commands, allocated to a combatant command, and those capabilities service retained, combatant command aligned, and prepared by the Army for combatant command missions.

<sup>37</sup> Establishing an intelligence architecture includes complex and technical issues that include the following: sensors, data flow, hardware, software, communications, communications security materials, network classification, technicians, database access, liaison officers, training, and funding FM 2-0, p. 6-2.

<sup>38</sup> Generate intelligence knowledge is a continuous task driven by the commander. It begins before mission receipt and provides the relevant knowledge required regarding the operational environment for the conduct of operations. (FM 2-0, p 6-3)

<sup>39</sup> AOC, special terms.

---

<sup>40</sup> See the Chief of Staff of the Army's Special Study Group report at [http://www.army.mil/article/128636/Megacities\\_and\\_the\\_United\\_States\\_Army\\_Preparing\\_for\\_a\\_complex\\_and\\_uncertain\\_future/](http://www.army.mil/article/128636/Megacities_and_the_United_States_Army_Preparing_for_a_complex_and_uncertain_future/)

<sup>41</sup> International Telecommunications Union, The World in 2013, ICT Facts and Figures, 2013, <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf> (accessed April 14, 2014).

<sup>42</sup> Ibid.

<sup>43</sup> This paragraph relied heavily on the *Subterranean Environment: Tunnel to Victory, the 2006 Lebanon War*, TRADOC G2 Intelligence Support Activity (TRISA), Complex Operational Environment and Threat Integration Directorate (CTID), APR 2014.

<sup>44</sup> a) ASCOPE: areas, structures, capabilities, organization, people and events (Army Intel FM 2-91.4, *Intelligence Support To Urban Operations*, 2008); b) Sewage, water, electricity, academics, trash, medical, safety, other considerations (Army ENG FM 3-34.170/MCWP 3-17.4 (FM 5-170) *Engineer Reconnaissance*, 2008); c) PMESII-PT: political, military, economic, social, information, infrastructure – physical environment, time (FM 2-0, Operational Variables for Planning).