Civilian Reserve Intelligence Program: A Fundamental Requirement for Army Intelligence Transformation

A Monograph
By
MAJ David W. Tohn
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas
AY 02-03

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Civilian Reserve Intelligence Program: A Fundamental Requirement for Army Intelligence Transformation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Command and General Staff College,School of Advanced Military Studies,Fort Leavenworth,KS,66027**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**83**	

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major David W. Tohn

Title of Monograph: Civilian Reserve Intelligence Program: A Fundamental Requirement for Army Intelligence Transformation

Approved by:

_____ LTC Jeffrey R. Witsken, MMAS	Monograph Director
_____ Robert H. Berlin, Ph.D.	Professor and Director Academic Affairs, School of Advanced Military Studies
_____ Philip J. Brookes, Ph.D.	Director, Graduate Degree Program

Abstract

Civilian Reserve Intelligence Program: A Fundamental Requirement for Army Intelligence Transformation by MAJ David W. Tohn, US Army, 52 pages.

The Army Intelligence Community (AIC) is fully engaged in the Army's Transformation process. However, the AIC's on-going transformation risks overlooking one critical, systemic shortfall – the perennial inability to provide sufficient intelligence to deploying forces under crisis-response conditions. Specifically, the AIC is hard-pressed to provide unconventional threat, cultural, demographic, and political/social intelligence down to individual villages, towns, or cities in a manner that supports initial employment operations. This intelligence requires a long-term presence in order to collect and understand the relevant information - a commitment that the AIC cannot meet for all potential contingency areas due to resource and operational constraints.

However, the AIC *can* leverage commercial and private organizations that already have a presence and a vested interest in these regions. They *do* maintain the long-term presence and understanding of the area as an inherent element of their operations. In this, they represent an untapped national resource. By building and sustaining *formal* relationships with these organizations, the AIC can leverage existing capabilities. Thus, given clear requirements and relatively minor funding (when compared to conducting the collection and analysis itself), the AIC can guide these organizations in closing any gaps between their existing knowledge base and the Army's requirements. Moreover, the Army/DoD can offer numerous incentives and benefits to make the effort worthwhile and mutually beneficial to participating organizations. The recommended program to achieve this goal is modeled after the US Transportation Command's (USTRANSCOM) Civilian Reserve Air Fleet (CRAF) Program, tentatively named the "Civilian Reserve Intelligence Program (CRIP)."

While leveraging other knowledge centers is certainly not a new idea, it can only become effective if the AIC deliberately optimizes its organizations, infrastructure, training, and manning to do so. Further, the AIC must coordinate, practice, and execute this linkage. CRIP will complement the existing AIC processes and would focus on shrinking the intelligence ramp-up to meet crisis support requirements. This work suggests that CRIP would best be executed within the Intelligence and Security Command (INSCOM) and recommends additional formal studies to validate and implement the program.

TABLE OF CONTENTS

Abstract I

TABLE OF CONTENTS i

LIST OF FIGURES iii

LIST OF TABLES iii

CHAPTER 1: Introduction 1

Background – How We Got Here 2

The Initial Assessment and Recommended Solution 3

An Army-Centric Framework 5

Analytic Framework 6

Summary 7

CHAPTER 2: Operational Structure and Performance Objectives for Intelligence Support to Army Operations 9

Army Intelligence Performance Standards 9

Intelligence Community Structure and General Description 10

Conclusion 14

CHAPTER 3: Case Studies – Patterns in Shortfalls 15

OPERATION RESTORE HOPE 15

TASK FORCE EAGLE 19

OPERATION DESERT SHIELD 22

Common Themes and Analysis 24

Organizational Dynamics of Intelligence Support 25

Conclusion 28

CHAPTER 4: Does Army Intelligence Transformation Meet the Challenge? 29

Intelligence Transformation in the ATCP 30

AIC Transformation: The AI-TCP **31**

Will the AIC Meet the Challenge? **34**

Conclusion **36**

CHAPTER 5: A Better Strategy **38**

Why this Approach? **39**

Not a Technology Solution **40**

Modeling the Solution on Successful Program **41**

The AIC's "CRAF" - The Civilian Reserve Intelligence Program **42**

Recommended Organizational Placement **48**

Comments on Resourcing **48**

Conclusion **49**

CHAPTER 6: Conclusion **50**

Recommended Actions **52**

BIBLIOGRAPHY **55**

Appendix A: Evaluation Criteria **A-1**

Intelligence Requirements – Specifying the AIC's Tasks **A-1**

Intelligence Support Standards **A-8**

Intelligence Support Conditions **A-9**

Summary **A-10**

Appendix B: National Intelligence Community **B-1**

DOD Agencies **B-1**

Non-DOD Agencies **B-2**

Other Government Agencies **B-3**

LIST OF FIGURES

Figure 1: National Intelligence Community……11

Figure 2: Defense Intelligence Production Centers……..……12

Figure 3: Joint Intelligence Architecture……..……12

Figure 4: Intelligence Crisis-Response Cycle……..……26

LIST OF TABLES

TABLE 1: NON –GOVERNMENT REACH RESOURCES 43

CHAPTER 1: Introduction

"Transformation," arguably the most fundamental reform of the United States Army since World War II, is forcing virtually every element of the Army to adapt and change to meet our present and future security challenges. The Army Intelligence Community is fully engaged in the process and is charting its path to ensure support to the Objective Force. Unfortunately, the Army Intelligence Community's transformation risks overlooking one critical, systemic shortfall – the perennial inability to provide sufficiently detailed social, political, cultural, economic, and unconventional threat intelligence to deploying forces under crisis-response conditions.

Transformation to the Objective Force exacerbates the risk – and increases the urgency - for the Army Intelligence Community to correct this critical shortfall.

> Objective force units will conduct operational maneuver from strategic distances, creating diverse manifold dilemmas for our adversaries by arriving at multiple points of entry, improved and unimproved….Objective force units arrive immediately capable of conducting simultaneous, distributed, and continuous combined arms, air-ground operations, day and night in open, close, complex, and all other terrain conditions throughout the battlespace. Army units conducting joint and combined operations will *see first, understand first, act first, and finish decisively* at the strategic, operational, and tactical levels of operation. [Emphasis in original][1]

To meet deployment and lethality requirements, the Objective Force deliberately trades survivability attributes (armor, mass, and quantity) for superior battlespace characterization, knowledge management, and situation understanding. Thus, *seeing first* sets an exceptionally high bar for pre-deployment intelligence support in depth, breadth, scope, and detail.[2]

---

[1]U.S. Department of the Army, "U.S. Army White Paper: Concepts for the Objective Force," not dated, accessed on 21 August 2002, URL: http://www.objectiveforce.army.mil/pages/objectiveforcewhitepaper.pdf., p. iv.

[2]A detailed description of the OF is found in the following documents: the "U.S. Army White Paper: Concepts for the Objective Force; the U.S. Army Training and Doctrine Command Pamphlet 525-3-93 (or 100 – pending final titling), *"Objective Force Unit of Employment Concept (Final Coordinating Draft),"* (Fort Monroe, VA, 7 August 2002); and the U.S. Army Training and Doctrine Command Pamphlet 525-3-90, *"The United States Army Objective Force Operational and Organizational Plan for Maneuver Unit of Action," (*Fort Monroe, VA, 22 July 2002).

Given these requirements, the critical question is: Will the Army Intelligence Community's transformation be effective in correcting the long-term, pervasive challenge of providing highly detailed, tactical-level intelligence within the framework of no-notice/short-notice operations typified by the Objective Force? The obvious follow-up question is: If not, what is an alternative or adjunct approach to better meet the requirement?

Background – How We Got Here

The Army Intelligence Community is historically challenged in providing the necessary detail for sustained combat operations until forces are deployed, conducting operations, and collecting intelligence. The hardest intelligence to gather is that which requires collection assets on the ground with direct and sustained access. More than just conventional order of battle and basic infrastructure, the greatest challenge is unconventional threat, cultural, demographic, physical environment, and political/social intelligence down to individual villages, towns, or cities in a manner that supports initial employment operations.[3] Gathering and producing this level of intelligence requires a long term collection and analytic effort, which is typically HUMINT-centric. It requires collectors and analysts who are intimately familiar with the area. This type of high fidelity, detailed, and very specific information is generally unnecessary for strategic or operational analysis or planning, but is critical to tactical planning:

> There is a critical period, a 'windows of opportunity' in which the commander must make crucial decisions…that set the tone for the remainder of the operation.[4]

As the evidence will show, the Army Intelligence Community's shortfalls in this area are long term and systemic.

---

[3]James A. Kirk, *Putting Social, Cultural, and Political Factors into the Joint Doctrine Playbook*. (Newport, RI: Naval War College, 04 February 2002); available from DTIC, ADA401839, abstract.

[4]Center for Army Lessons Learned, *Operation Restore Hope: Lessons Learned Report*, (Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 3 DEC 1992 – 4 MAY 1993), 5.

The shortfalls are deeply rooted in deliberate policy, organizational, resource, and doctrinal decisions tracing back to the Cold War. Within that context, the challenge was to gain conventional military intelligence from denied areas – leading to an emphasis on remote sensing to generate intelligence about the Warsaw Pact military threat. Indeed, the Nation's entire military intelligence system was successfully tailored and focused to that purpose.

However, intelligence on other, "lesser" regions and threats suffered greatly from a lack of emphasis and collection/analytic resources. Often, these issues lacked technically collectable 'observables.' Additionally, they rested much lower on the Nation and Army Intelligence Community's priority list, leading to gaps in the baseline pool of intelligence available to support contingency operations. Bottom line, the Army Intelligence Community was unable to build and sustain a collection and analytic capability in these regions. If and when employed, a commander had to wait until forces were on the ground, conducting operations, in order to fill in the gaps.

As many contemporary military writers note, the threat is no longer singular and defined. Not only are the potential locations worldwide, the character of the threat at each location is almost infinitely varied. It is unreasonable to expect the same Army Intelligence Community structure and organization to perform significantly better in a more chaotic and dynamic environment than it did during the Cold War.

The Initial Assessment and Recommended Solution

The Army Intelligence (AI) strategy for transforming will not solve this fundamental problem. The Army Transformation Campaign Plan (ATCP) and Army Intelligence Transformation Campaign Plan (AI-TCP) plans to meet future requirements by dramatically improving existing processes (collection, analysis, collaboration, etc.), with a particular emphasis on technology-enabled systems improvements. All of this will definitely assist in extracting more

value and production from the existing 'base line' pool of intelligence developed "in-house" - within the National Intelligence Community (NIC)[5] - to support operations.

However, while necessary, this approach is insufficient. It does not address the fundamental problem: building and maintaining an adequate social, political, economic, ethnic, and cultural baseline for contingency areas. The effort to overcome the structural gaps result in a predictable crisis-response cycle: reviewing existing data, collecting additional data, seeking and building *ad hoc* teams of experts (including non-governmental sources), and eventually developing sufficient understanding to support operational requirements. This cycle is the defining characteristic of intelligence support to crisis operations.

An addition to the AI-TCP's efforts to better weave the AIC together may be to tap information assets outside of the NIC. Tapping additional knowledge centers will improve the baseline *and* establish the linkages to smooth out the crisis-response cycle. The AIC can *embrace* the existing ad hoc process of drawing outside experts, streamlining, formalizing, and optimizing the effort in order to come closer to meeting operational timelines.

Specifically, the AIC can leverage commercial and private organizations that already have a presence and a vested interest in the respective areas of interest. They maintain the long-term presence and understanding in a region as a fundamental element of their operations. In this, they represent an untapped national resource. By building and sustaining *formal* relationships with these organizations, the AIC can harness and integrate *their* organic capabilities in meeting *Army* requirements. Incentives for the commercial and private organizations may include funding, transportation and support during contingency operations, etcetera. This proposal is modeled after the US Transportation Command's (USTRANSCOM) Civilian Reserve Air Fleet (CRAF) Program; tentatively retitled the Civilian Reserve Intelligence Program (CRIP).

[5]"Intelligence Community" includes all of the DoD and Federal intelligence agencies and organizations. There are thirteen formal members of the IC, as outlined in Chapter 3 and Appendix B. AIC refers only to US Army Intelligence organizations, a subset of the IC.

While leveraging other knowledge centers is certainly not a new idea, it can only become reliably effective if the AIC deliberately optimizes the organizations, infrastructure, training, and manning to do so. Further, the AIC must coordinate, practice, and execute this linkage between these organizations, the AIC, and the Army.

Managing the CRIP is essentially a collection management function, matching Army requirements with potential collection and analytic capabilities in the private and commercial sector. CRIP will complement the existing AIC process and would focus on shrinking the intelligence ramp-up by expanding the readily-available pool of knowledge and establish those formal links. The thesis will suggest a structure and organization to achieve this end state.

An Army-Centric Framework

The author recognizes that the intelligence community challenges noted extends to the Joint Intelligence Community. As a result, CRIP could be a Joint program for all of the right reasons: unity of effort, economy of scale, cross-Service coordination, etc. However, this research deliberately limits its scope to an Army-centric solution for the following reasons:

- As the Service that traditionally occupies a theater for extended periods of time, the Army is the primary consumer of the intelligence that the AIC and MIC are so challenged to provide – local social, economic, political, and cultural information. Routinely and extensively interacting at the face-to-face level within an area of operations (with all of the challenges, risks, and complexities inherent), the Army requires a level of detail far beyond much of the Joint Community. The Air Force or Navy typically does not require the social, cultural, ethnic, or even micro-terrain information to the same level of resolution as an infantry battalion conducting stability operations. An Army-only CRIP can focus on the Army-specific requirements that routinely fall below the national and defense intelligence community thresholds for support.
- The Army can establish the pilot program and provide a proof of concept to the Joint community; and finally,
- Experience suggests that establishing a new organization at a Joint level inevitably dilutes the initial focus and effort as Service requirements are negotiated during the chartering process.

CRIP may rightly evolve into a Joint program, but that would be the topic of further study, at a later date.

Analytic Framework

This work is divided into three major sections that build the argument for the AIC adding a critical addition to its transformation effort:

Section One

The first section confirms the assertion that the AIC has the challenge described. To do this, Chapter 2 describes how the intelligence community supports military operations and then clearly identifies the tasks and criteria for assessing success or failure. Specifically, the paper focuses on describing order of battle, physical and informational infrastructures, population, demographics, culture, economics, and religion, refugee/displaced persons and international NGOs/PVOs disposition. The criteria include accuracy, timeliness, usability, completeness, preciseness, and reliability. These requirements are drawn from established doctrine and are outlined in detail in the chapter.

Chapter 3 then assesses the AIC's performance in three operations spanning the spectrum of military operations. This review confirms that the AIC's shortfalls are clear and can be attributed in great part to a lack of sufficient "in-house" information and expertise. The gaps in the baseline result in a crisis-response cycle during the time-sensitive execution phase in order to fill the knowledge voids.

Section Two

The second section reviews and assesses the AIC's transformation efforts to determine if they address and solve the problem. Any proposed solution must substantively and systematically fill the gaps in information collection and analysis and better prepare the AIC to support crisis-action planning and execution.

Chapter 4 examines the Army Transformation Campaign Plan (ATCP) and the AI-TCP and determines that they only marginally address this problem. As well, it reviews the associated

staff actions and operational programs to show that they do not address the problem. This assessment focuses on whether the program/action clearly identify the root problem, is resourced with funding and personnel, and has a clearly defined proponent tasked to ensure completion.

Section Three

The final section provides a relatively low-cost, feasible solution. Chapter 5 details essential components of the CRIP and suggests an organizational structure for the program. CRIP answers the institutional and systemic challenges identified. It will prove more effective and efficient while avoiding the potential pitfalls of the crisis-response cycle. More importantly, if properly resourced and executed, it will help the AIC to meet the intelligence support requirements projected for the transformed Army. Chapter 6 concludes with recommended actions to further develop and execute the solution.

Summary

The Army Intelligence Community has a long and almost intractable challenge in providing intelligence in support of contingency operations. These shortfalls incurred far less risk due to the robust characteristics of the Army force structure and equipment. However, with the transformation to the Objective Force, these mitigating factors are being deliberately discarded in favor of strategic responsiveness. As such, the Army can no longer accept the risk inherent in the legacy intelligence-support business practices.

The ATCP and AI-TCP do not adequately address one critical cause for much of the crisis-action inadequacies. Rather, they improve existing processes without making a fundamental shift in assumptions, resources, organization, or processes to meet the root requirement. As such, they will not be singularly effective in supporting the Transformed Army.

Revising the focus and priorities would meet this shortfall. By formally leveraging alternate knowledge centers (private and commercial) that already maintain situational

understanding of areas of interest to the Army, the AIC could overcome systemic roadblocks and meet the existing and future requirements. To do so effectively in a crisis, the process, relationships, and organizations must be established and practiced beforehand.

CHAPTER 2:

Operational Structure and Performance Objectives for Intelligence Support to Army Operations

In order to confirm that the AIC is challenged in providing the intelligence necessary to support crisis-action planning and initial ground combat operations, it is first necessary to clearly establish what "right" looks like – what the standards of success are. After establishing a doctrinally based standard, a brief review of how the massive National Intelligence Community organization and processes is prudent. Of course, since the AIC is a fully integrated component within a larger intelligence community, it is challenging to draw clear lines of responsibility. However, understanding the institutional environment and structure is critical for assessing themes and patterns in the three case studies that follow.

Army Intelligence Performance Standards

The AIC's mission can be crudely summarized as "provide intelligence." It is more clearly described in a variety of Joint and Army doctrinal publications, ranging from the Universal Joint Task List (UJTL) to the Joint Publication 2-x series, to Army Field Manuals 3.0 and the 2-x series and are detailed in Appendix A. The single inclusive task that lends itself to evaluating the AIC's effectiveness is "Provide General Military Intelligence (GMI) for the Joint Operations Area." [6] GMI is defined in detail in Appendix A, and includes virtually all imaginable aspects of the environment, threat, and other actors that are outlined in Joint and Army doctrine. However, it is distilled down to the following five tasks:

[6] OP 2.4.2.3 "Provide General Military Intelligence (GMI) for the Joint Operations Area," as specified in the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3500.04B, *Universal Joint Task List*, (Washington, DC: GPO, 1 October 1999), 2-324 to 2-327.

- **Describe the Order of Battle (Conventional, Unconventional, and Political)**
- **Describe the Physical and Information Infrastructure**
- **Describe the Population, Demographics, Culture, and Religion**
- **Describe the Refugee/Displace Persons & International NGOs/PVOs**
- **Describe the Economic Structure**

Given this task, Army Field Manual 3.0, *Operations*, provides the evaluation criteria, or conditions and standards:[7]

- **Accuracy**. The information conveys the actual situation; in short, it is fact.
- **Timeliness**. The information has not been overtaken by events.[8]
- **Usability**. The information is easily understood or displayed in a format that immediately conveys the meaning.
- **Completeness**. The information contains all required components.
- **Precision**. The information has the required level of detail, no more and no less.
- **Reliability.** The information is trustworthy, uncorrupted, and undistorted**.**

In short, the assessment mechanism is clear – "historically, has the AIC provided sufficient GMI, as defined above, to support the first 96 hours of combat operations? Will it be able to do so in the future?"[9] Appendix A includes a more detailed description of the criteria. Given these standards, a quick review of the intelligence community structure will illustrate how the requirements are met.

Intelligence Community Structure and General Description

The National Intelligence Community (NIC) is a complex grouping of agencies designed to support military and civilian policy and operational requirements. Often referred to as a

[7]U.S. Department of the Army, *Field Manual 3-0, Operations.* (Washington, D.C.: GPO, June 2001), 11-13.

[8]If the timeliness requirement of the case study is tighter than the OF's projected timeline, then a 48-hour requirement will be applied . This will be done because, arguably, given that intelligence is necessary *before* deployment to better package the force and prepare the soldiers, the requirement for adequate intelligence is shorter than the 96-hour employment requirement cited in the Objective Force White Paper. The more stringent condition attempts to enable the commanders to effectively plan operations and force structure in a timely manner.

[9]The 96 hour threshold will be used in assessing past operations and future capabilities because, according to U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-93 *(*or 100 – pending final titling), *Objective Force Unit of Employment Concept*, the OF will achieve minimum self-sustaining combat power at that point and should presumably be capable of detecting and mitigating unanticipated threats.

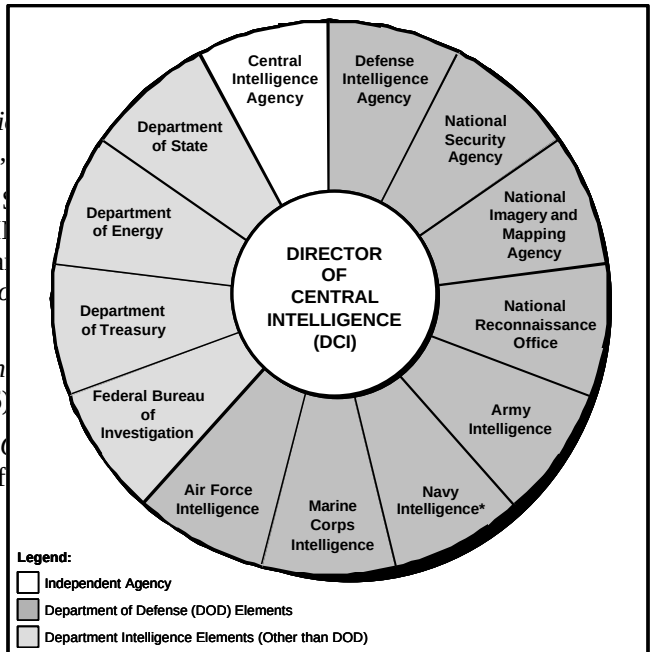
'federation' rather than a 'community,' the NIC constituents support their respective consumer/parent organization, while collaborating with the other members to support the US Government as a whole. Figure 1 illustrates the constituent organizations. [10] Appendix B provides a detailed description of each organization's charter and functions.

A subset of the NIC is the Military Intelligence Community (MIC)[11] with processes and procedures established to focus intelligence for both defense policy and combat operations. The MIC conducts both Routine and Crisis Action intelligence operations. They are interrelated and mutually supporting. As the Routine structure is the basis for crisis action operations, a brief explanation is important in understanding the systemic and structural shortfalls within the crisis system.[12]

Routine Production

The Department of Defense Intelligence Production Program (DoDIPP) is the structure for the MIC. It is the framework for "sharing intelligence resources, eliminating duplication, maintaining quality, encouraging widespread dissemination, exploiting electronic technologies, and improving efficiency and timeliness." [13] The National Military Joint Intelligence Center (NMJIC), run by the Defense Intelligence Agency (DIA), coordinates the MIC's support to military operations.

Figure 1: National Intelligence Community



[10] Joint Chiefs of Staff, *Joint Publicati*
(Washington, DC: GPO, 28 September 1998),

[11] The MIC includes the DIA, and the
organizationally within the DOD, the NSA, NI
effectively straddle the line between the MIC a
National Intelligence Support to Joint Operatio

[12] For a more detailed description, see
Intelligence Training Center, *National Foreign*
Defense Intelligence Agency, September 1996)

[13] Joint Military Intelligence College,
*Intelligence Readiness, (*Washington, DC: Def

In order to reduce redundant collection and analysis, the MIC assigns "lanes in the road" to the various Defense Intelligence Production Centers (DIPC) (see Figure 2)[14]. This essentially divvies-up the various facets of intelligence analysis and production to different organizations based upon their technical expertise and/or institutional focus. For example, the Army's National Ground Intelligence Center, as the Army's DIPC for the DoDIPP, is responsible for producing all ground order of battle and equipment intelligence. Similarly, the National Air Intelligence Center is responsible for production on foreign aircraft, air forces, air defenses, and associated areas of interest. Theoretically, this system reduces redundancy and ensures expert analysis and production. Of particular note, while the DIPCs coordinate with civilian and other government organizations as they deem necessary, no single organization is responsible for coordinating and integrating the leveraging of non-MIC/NIC resources as a whole.

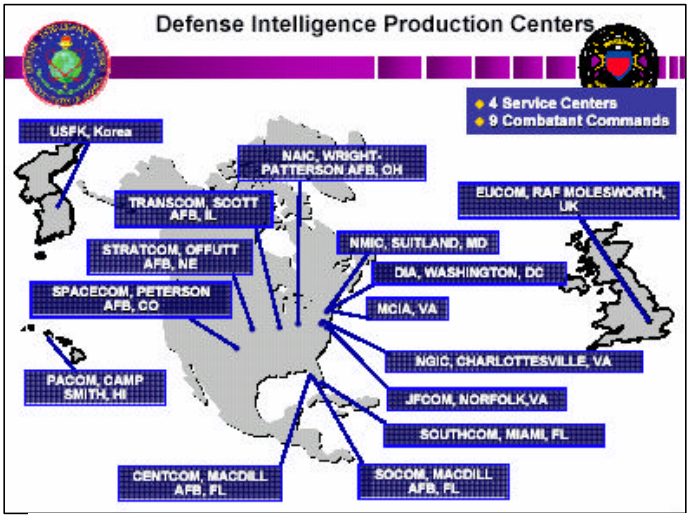


Figure 2: Defense Intelligence Production Centers

Operational intelligence comes to a focal point at the Regional Combatant Commands (RCC). Specifically, each RCC's Joint Intelligence Center[15] is "responsible for providing and producing the intelligence required to support the joint force commander and staff, components,

[14]Defense Intelligence Agency, Paul Gregory, "Agency Operations and Training Assessment System," presented to the World Wide Joint Training Conference, 2002, URL: http://www.dtic.mil/doctrine/jel/training_pubs/19_dia.pdf, accessed on 20 September 2002.

[15]In the U.S. European Command (EUCOM), the JIC is called the Joint Analysis Center (JAC), but performs the same function as JICs. For ease of reference, this paper will use "JIC" to refer to both the JICs and the JAC.

task forces, elements, and the national intelligence community."[16] Thus, while the MIC and NIC organizations have regional as well as functional desks, the Joint Intelligence Centers are responsible for consolidating and maintaining baseline military intelligence data for their assigned regions.[17] Figure 3 illustrates the overall joint intelligence architecture.[18]

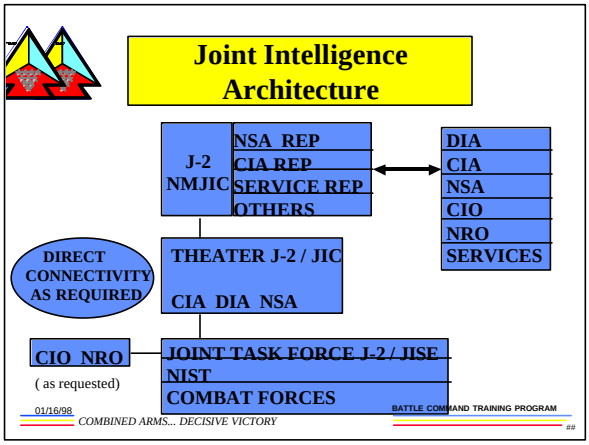


Figure 3: Joint Intelligence Architecture

In summary, this system is a distributed production effort designed to respond to baseline and specific intelligence requirements of the RCCs and the various consumers within the Department of Defense. The NIC interfaces with the MIC through the National Military Joint Intelligence Center and at each of the JICs. The JICs serve as the regional knowledge centers, prepared to support operations in their AOR as well as to provide finished intelligence back to the rest of the intelligence community. The net result should be a baseline of current, detailed military intelligence ready to support Deliberate and Crisis Action Planning and Operations.

Crisis Action Operations

Support to crisis action operations builds upon the peacetime structure. The JIC remains the focal point for intelligence support to the Joint Force Commander. If the RCC forms a Joint Task Force (JTF), the JIC supports the JTF J-2. The JTF J-2 has primary staff responsibility for planning, coordinating, and conducing overall joint intelligence preparation of the battlefield at the

[16]Joint Military Intelligence Training Center, *National Foreign Intelligence Community Course Textbook*. 8-7.

[17]Joint Chiefs of Staff, *Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*, (Washington, DC: GPO, 24 May 2000), 1-11.

[18]United States Army Training and Doctrine Command, Battle Command Training Program, "Force Projection Intelligence, Electronic Warfare Operations," (Fort Leavenworth, Kansas. 16 January 1998).

joint force level. It forms a Joint Intelligence Support Element to conduct intelligence operations. Additionally, each Service's intelligence organization provides detailed support directly to their respective components as well as the Joint Intelligence Support Element. National and military intelligence organizations surge and augment the supported organizations to meet the crisis requirements.[19] As Chapter 3 will show, this surge and augmentation process is the systemic root of the MIC's challenge to develop and sustain a sufficient intelligence baseline.

Conclusion

The National and Military Intelligence Community's role in supporting combat operations is fundamentally clear. The challenge is in meeting the arduous requirements for accuracy, timeliness, usability, completeness, preciseness, and reliability. The AIC, as an integral component of the larger intelligence community, is tasked to leverage this massive capability to meet the ground force commander's planning and execution requirements.

This larger intelligence structure is organized in a logical and efficient manner, at least on paper. It clearly identifies responsibilities, roles, and functions that should provide a robust baseline of intelligence. Moreover, the MIC has a mature process for providing intelligence support to a joint force commander and the subordinates during a crisis. Unfortunately, as the following chapter will illustrate, this structure fails to meet the Army's requirements. This failure is due to deliberate, rational decisions, influenced by resource constraints and competing priorities.

[19]Joint Chiefs of Staff, *Joint Publication 2-01.3*, 1-12 to 1-13.

CHAPTER 3:

Case Studies – Patterns in Shortfalls

Given the requirements and the general structure established to meet them, a review of past performance confirms that the operations were consistently initially hindered by inadequate intelligence. The existing databases and analytic expertise was insufficient, inefficient, or worse, non-existent. Ground forces consistently deployed with inadequate basic information and intelligence to be effective immediately. It was not until forces were on the ground and the intelligence collection/analysis capabilities matured that the commander was effectively served.

The three case studies are RESTORE HOPE (Somalia), TASK FORCE EAGLE (generally including Bosnian, Kosovo, and Macedonian deployments), and DESERT SHIELD (Iraq), with emphasis on the initial phases of the operation. These operations span the spectrum from a Support operation to Stability and Support operation to a Mid-intensity combat operation. The assessment is by exception – noting only areas where the AIC fell short. Of note, the following case studies extensively cite the after action reviews and studies to ensure great fidelity in capturing the nuance and intent in the criticisms.[20]

OPERATION RESTORE HOPE

OPERATION RESTORE HOPE represented an almost pure no-notice deployment, exhibiting all of the challenges and systemic shortfalls inherent in preparing for and executing these types of missions. Prior to alert, neither the NIC, MIC, AIC, nor the 10th Mountain Division had ever seriously considered Somalia a potential deployment location. The Division was

[20]For readability's sake, only major conclusions are presented in support of the findings. Again, these assessments apply to the initial phases of the respective operation and do not characterize intelligence support over the duration. See the supporting studies for a detailed assessment and supporting data.

designated ARFOR on D-2 and had initial forces on the ground on D+3. The total time was less than a week.[21]

> The division was executing an almost no-notice alert and deployment. They never had time to adequately plan, rehearse, or train for the operation. The lack of time would adversely affect the mission planning and force packaging. The effect was to plan for the worst-case scenario, clan resistance. This did not initially occur. The result was the unnecessary deployment and redeployment of 18% of the equipment….[22]

Performance Assessment

The databases and initial IPB were virtually non-existent. Even mapping products were unavailable; with US forces ultimately relying on old Soviet maps to navigate. As a result, all of the trends and issues discussed are evident in the extreme.

Shortfall 1:

The AIC failed to describe the order of battle (conventional, unconventional, and political) and the physical and information infrastructure with the requisite accuracy, usability, completeness, precision, or reliability. As a result, the inadequate IPB had direct and immediate operational effects. The following assessments clearly show the level of frustration and dissatisfaction with the initial intelligence support:

> Application of the traditional warfighting IPB process in the predeployment phase of Restore Hope failed to capture the unique character of the operation. It was therefore of lesser assistance in planning, force design, and TPFDD development than should have been the case. [I]t must include paramilitary and non-governmental organizations that might interface with US organizations in addition to incorporating joint and other considerations altered by the nature of the undertaking. MG Arnold's after-action report noted that an IPB analysis resulting in a better definition and description of the Somali situation might have influenced the type of units brought into the country and their positions on the TPFDL.[23]

> The problems with IPB began with the description of the battlefield. The [area of operation] and [area of interest] were not properly addressed. No historical data was

[21]Todd R. Wood, Major, U.S. Army, *Can IPB Eliminate Mission Creep,* (Fort Leavenworth, KS: School for Advanced Military Science, 18 December 1997), 22.

[22]Ibid., 24.

[23]Rand Corporation, *Getting the Musicians of Mars on the Same Sheet of Music – Army Joint, Multinational, and Interagency C4ISR Interoperability*, 01 January 2001, available from Center for Army Lessons Learned Restricted Database, document RWP-03-188564, 7.

> available on the patterns of the warring faction, and their equipment was not known. This caused the commander to have an unclear picture of the enemy situation.[24]

Shortfall 2

The AIC failed to describe the refugee/displaced persons and international NGOs/PVO disposition with sufficient accuracy, completeness, precision, or reliability to support initial operations. Given the humanitarian relief mission, this was a fundamental element of the mission analysis and had a direct impact throughout the operation, to include force tailoring, deployment operations, and force flow decisions.

> The IPB failed to identify 49 humanitarian relief and NGOs already operating in the country. This resulted in confusion as to what the NGOs capabilities were and where they had been operating. The lack of information about the warring clans, terrain, and NGOs combined to give the deploying commander a fuzzy picture of the AO. This, in turn, affected both the selection of forces deployed and the order in which they arrived. Additionally, arriving units were not trained or equipped to accomplish the missions required.[25]

Shortfall 3

The AIC failed to describe the population, demographics, culture, and religion with sufficient accuracy, completeness, usability, precision, or reliability to meet operational requirements. In this case, this failure arguably led to the fatal escalation of the operation, resulting in the 3-4 October 1993 Ranger tragedy in Mogadishu.

> Our inability to adequately sense and analyze the [social, cultural, and political] (SCP) factors in Somalia led to a lack of understanding of how US and UN military force size, composition, and actions would be interpreted and acted on by the Somali's. A more detailed understanding of SCP factors in Somalia might have driven operational level decision makers to either choose alternative COAs or make operational level changes in intelligence, protection or other areas to compensate for the consequences of embarking on the mission to capture Aidid.[26]

---

[24]Wood, 24.

[25]Wood, 24.

[26]Kirk, 5.

Performance Analysis

This poor level of intelligence support to initial operations is the result of the lack of pre-crisis attention. Given the overwhelming uncertainty and the resulting national security concerns in the immediate aftermath of the Soviet Union's collapse, a backwater area like Somalia was deservedly low on the intelligence collection priority list. The databases simply did not exist in any meaningful manner.

Moreover, the type of intelligence required – cultural, political, social, and paramilitary – would only have been available from a deliberate and expensive HUMINT collection and analysis effort. What little intelligence that was collectable with the existing collection systems (IMINT and SIGINT) was never analyzed in detail (if at all), until the crisis developed. Thus, with no malice of intent, the intelligence community deliberately did not develop and sustain the pre-crisis intelligence baselines in an area that did not appear to have strategic importance.

Once the crisis matured and the potential for US operations crystallized, the AIC and operational force went into overdrive trying to fill information gaps. From the author's own experience, the 10th Mountain Division's best pre-deployment cultural and clan intelligence came from an ad hoc briefing by a pair of academics from Syracuse University. These researchers had recently completed six months of study in Somalia and were compiling their research for publication. Through the luck of timing and a personal relationship with a member of the Division staff, they provided a half-day's worth of briefings to the intelligence staff. The rest of the intelligence baseline matched the quotes above.

As the Rand Corporation neatly summarized, arriving in a truly austere theater, the commanders realized that the first priority was to make up for the AIC's inability to provide meaningful intelligence support: "Army units must realize that jumpstarting ISR operations may be an essential first task when entering a theater. "[27]

[27]Rand, 25.

TASK FORCE EAGLE

The name, "TASK FORCE EAGLE" is used in the context of this paper to include the intelligence support experiences throughout the US involvement in the Balkans over the past ten years. U.S. and NATO operations in the Balkans covered more of the operational spectrum than did OPERATION RESTORE HOPE, to include elements of conventional force-on-force combat.

Performance Assessment

Given the greater range of operational requirements, it again is not surprising that the intelligence community was unable to meet the operational and tactical requirements during the initial phases.

Shortfall 1

The AIC failed to describe the physical and information infrastructure with sufficient timeliness, completeness, and precision. As with Somalia, many of the forces did not have access to the critical intelligence necessary for initial planning and execution.

> [S]tanding databases for the area were sparse in the areas considered critical for early entry and road marches (e.g.: ports and throughput capacities and capabilities, road and rail trafficability, bridge classifications, and tunnel clearances).[28]

While there is some anecdotal evidence that this information was available, but not provided due to bureaucratic or policy reasons, [29] the official after action review is clear that the deploying forces were not adequately served, with resulting affects on entry into the theater.

[28]Center for Army Lessons Learned, *"Lessons Learned Report: Bosnia Contingency Planning and Training,"* (Fort Leavenworth, KS: US Army Training and Doctrine Command, December 1995), 54-5.

[29]Robert F. Scruggs, Staff Action Officer, AI-TCP Liaison, U.S. Army Intelligence and Security Command, Personal interview with author, 4 March 2003.

Shortfall 2

The AIC failed to describe the order of battle (conventional, unconventional, and political), the population, demographics, culture, and religion, and the economic structure with sufficient accuracy, timeliness, and completeness.

> Factional order of battle was ten times that normally confronted in conventional operations and in a constant state of flux…The nature of the environment in which IFOR found itself required intelligence personnel to deal with a myriad of information requirements that were not specifically military in nature.[30]

> Much of this [social, political, and economic] information is now overcome by events or restructuring, or is just plain wrong.[31]

Again, as with Somalia, understanding the local political and cultural issues in regions where Army forces would be deployed was critical during the initial planning and execution. Some units entered their area of operation with little understanding of the threat (or opportunities) in that area.

> In short, the intelligence-operating environment within MND-N was one of tremendous complexity and ambiguity…the threat environment was a 360° battlefield shaped by a tangled web of nationalist, regional, and global policy objectives. Threats covered a spectrum of former factional militaries, land mines, snipers, nationalist extremists, international terrorists, civil disturbances and riots, organized crime, hostile attitudes shaped by local media and factional propaganda, IFOR local national employees exploited by factional intelligence services and local power brokers, and extraordinarily rugged terrain and harsh weather conditions.[32]

The risk of catastrophic failure was high.

Shortfall 3

Once planning began for operations, the AIC was challenged to surge to develop information sufficiency:

> Theater intelligence support elements (e.g. the JAC, the EUCOM JIC, and the USAREUR Combat Intelligence Readiness Facility UCIRF), only at initial operational capacity, were

---

[30]Melissa E. Patrick, Intelligence *in Support of Peace Operations: The Story of Task Force Eagle and Operation Joint Endeavor*, (Carlisle Barracks, PA: Army War College, 10 April 2000), DTIC ADA378285, 6.

[31]John C. Hammond, Colonel, Stabilization Force-CJ2. *"Enclosure 1: Intelligence Support to SFOR" to "Memorandum for the COMSFOR: SFOR Tour Repo*rt, 4 DEC 96 to 26 SEP 97," 23 SEP 1997.

[32]Patrick, 14.

> faulted in various degrees at all levels….It is imperative that these elements be brought to full operational capability to allow proper training and maturation.[33]

Moreover, once operations were on-going, it was a great challenge to sustain the effort.

> More than one intelligence staff was strained under the requirements by their commanders to develop their own intelligence products because of very short planning times for each iteration of various mission branches and sequels.[34]

The AIC had to draw on augmentees and work on a surge-basis to continue to meet the operational requirement. This necessarily drained additional resources away from lower-priority intelligence missions, setting the conditions for another crisis-response cycle down the road.

Performance Analysis

Unlike OPERATION RESTORE HOPE, the operations and intelligence community did not enter the Balkans completely blind and unprepared. Yugoslavia's break-up and the subsequent conflicts among the constituent states and groups had been of strategic interest for several years. The intelligence collection focused at the strategic and operational level, from political intelligence to tracking the formal orders of battle of the post-Yugoslavian armed forces. Existing collection and analytic capabilities were sufficient to support policy-making and diplomacy.

However, this intelligence was insufficient in detail or depth to support stability and support operations at the tactical level. Specifically, the lack of key personality, group, economic, and paramilitary information had a tremendous operational impact early on. As with Somalia, this level of information required a sustained presence and collection effort (especially HUMINT) throughout the towns, villages, and key cities. Clearly, this was beyond the capability (or intention) of the strategic-intelligence-focused NIC and MIC. Thus, as with Somalia, deliberate and rational resource-constrained prioritization decisions had an immediate operational impact. It

[33]Center for Army Lessons Learned. *"Lessons Learned Report: Bosnia Contingency Planning and Training,"* 53.

[34]Ibid.

was not until deployed forces fielded the necessary collection capabilities that the requisite fidelity developed.

OPERATION DESERT SHIELD

As the first units deployed into theater in response to Iraq's invasion of Kuwait, the AIC's support to Operation DESERT SHIELD was on shaky grounds. Expectedly, intelligence support improved as the operations matured and responsibility and capability transferred into theater, supported with national assets. However, it took time to achieve this.[35]

Performance Assessment

During the early phases, there were two general assessments by the operational commanders about the AIC's ability to accomplish its tasks. The initial intelligence was not sufficiently focused to support tactical operations; and there was almost no usable terrain or environmental data. These shortfalls are amplified below:

Shortfall 1

The AIC failed to describe the order of battle (conventional, unconventional, and political) in sufficient completeness and usability. Much of the intelligence available at the start was at the strategic or operational level. There was little to support tactical planning at the division or corps level until the theater intelligence structure matured:

> [Commanders'] most common complaint was the products lacked details needed to plan and conduct tactical operations….They charged the products were appropriate for policy makers but not relevant to a combat commander.[36]

> [As] in the cases of Grenada and the Gulf, we had thin intelligence databases and few people who worked the area. We virtually had to build intelligence from scratch.[37]

---

[35]John F. Stewart, BG(P), G-2, 3rd United States Army, *Operation Desert Storm: The Military Intelligence Story: A View From the G-, 3d U.S. Army*, (Fort McPherson, GA: Headquarters, 3rd U.S. Army, April 1991), 9.

[36]Stephen J. Bond, Strategic *Intelligence for Tactical Operations: Intelligence Requirements for Force Projection,* (Carlisle Barracks, PA: Army War College,. 04 April 1998), DTIC. ADA343395, 20-21.

> We need a broader base of intelligence on many areas of high political and economic interest to the United States instead of deep data concentrated in a few areas.[38]

Shortfall 2

The AIC failed to describe the physical and information infrastructure with sufficient accuracy, completeness, and precision:

> The first order of intelligence business was terrain, for if the ground in the west could not support our armor forces, we could not conduct a main attack from there. **Knowledge of precisely the kind of desert we faced was sketchy**. In the years in which we had official relationships with Iraq, not one military attaché had apparently walked the terrain south of the Euphrates River to the Saudi Arabian border. If he had, someone had lost his reports. This speaks volumes about the importance of the basic kind of intelligence collection our Defense Attaché system should carry out. [Emphasis in original][39]

The impact of this shortfall is immediate and readily apparent. Basic tactical planning cannot occur without an understanding of the physical environment. What little information there was available did not make it to the commander.

Performance Analysis

The character of the pre-crisis intelligence collection and analysis was very similar to that described for the Balkans. The NIC and MIC focused upon strategic political/diplomatic intelligence and on sustaining a gross order of battle and disposition database. There was little call to develop and sustain tactical-level intelligence on the order of battle or terrain, and the AIC fell short in these areas. Since the conflict was far more conventional than either the Balkans or Somalia, local and regional civilian politics, culture and society were less critical to mission success. However, the AIC was unable to discern intent or future capabilities until operations were well underway. As before, this was the result of deliberate decisions to balance the perceived lack of a requirement against the limited assets and resources available.

---

[37]Stewart, 27.

[38]Ibid., 28.

[39]Ibid., 24.

Moreover, Operation DESERT SHIELD effectively illustrates the challenges and turmoil involved in attempting to surge to make up for long-term collection and analysis gaps:

> The appropriate Unified and Specified Command did not have the staff capability to manage suddenly myriad, urgent wartime requirements.[40]

> [T]his crisis once again pointed up shortcomings in human and technical intelligence about even major developing world military powers….Many aspects of the US Intelligence Community require rethinking – its structure and focus, priorities among the type of analysis done (counting equipment and units versus judging intentions), the regional, cultural, and language competencies pursued, and so on…the Gulf War showed this to be a significant shortcoming among those organizations supporting our air, ground, and naval forces.[41]

> The war reinforced the need for reforms in the US intelligence process. Earlier we noted that intelligence was not timely enough during the war, but it also remains too heavily focused on the Soviet threat….In this connection, in the Middle East and other regions, the lack of human intelligence is a well-known deficiency.[42]

While the intelligence community has come a long way in improving its capabilities since 1991, the dynamics and challenges here resonate through more recent operations, to include, anecdotally, Operation ENDURING FREEDOM. Much of the standing knowledge pool focuses at the strategic and operational level, with the implicit decision to wait until imminent operations to develop the necessary tactical fidelity.

Common Themes and Analysis

A common theme running through the after action reviews is the tremendous emphasis on human intelligence (HUMINT) and open source intelligence (OSINT) to collect the truly critical information. From Somalia to the Balkans to Southwest Asia, the requisite detail, depth, and

[40]Ibid., 27.

[41]Center for Strategic and International Studies, The *Gulf War: Military Lessons Learned (Interim Report of the CSIS Study Group on the Lessons Learned from the Gulf War)*, (Washington, DC: Center for Strategic and International Studies, July 1991), 31.

[42]Ibid., 43.

breadth could only be gained by sustained, interpersonal contact with the populace and environment. Closely following the open-source reporting from the area augments this presence.[43]

In all three case studies, the US Government had some minor presence in the AOR – typically a defense attaché or diplomatic mission. Additionally, with the exception of the Kuwaiti desert, all regions had a long history of NGO/PVO operations. These sources were eventually identified as critical, but missed, opportunities. Many were not harnessed until operations were already underway, if ever at all.

The three case studies seem to indicate that lead time (as a crisis evolved) appeared to have some impact on the ability to shift resources and surge prior to operational employment, but not decisively so. However, as noted above, the type, depth, and breath of information requires a sustained presence in the area of operations.[44]

The obvious solution is to have a long-term, focused presence in the region. However, this is prohibitive within the conventional intelligence architecture. This is a result of resource constraints and the resulting prioritization of efforts. Understanding these structural constraints hints at a solution that side steps these perennial resource constraints.

Organizational Dynamics of Intelligence Support

In prioritizing resources to meet the greatest needs, the NIC leadership inadvertently set in motion a cycle of crisis-response that eventually affects long-term readiness. In the words of the

[43]Kathleen A. Gavle, *Division Intelligence Requirements for Sustained Peace Enforcement Operations,* (Fort Leavenworth, KS: Army Command and General Staff College), 01 May 2000., DTIC ADA381780, 25; and Robert D. Steele, *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats*, (Carlisle, PA: Strategic Studies Institute, 2002), 17.

[44]OPERATION JUST CAUSE is an excellent example of the quality, quantity, and detail of information that becomes available once collection begins with forces on the ground. Despite a permanent garrison in Panama for several decades, it was not until ground forces were actively operating within and among the population that the tactical intelligence finally achieved the level necessary to support reaching situational understanding. Indeed, the intelligence structure was initially ill-prepared to process the reporting. – Conclusions drawn from Timothy D. Bloechl, *Mission Complete? Tactical Intelligence During the Transition from War to Peace*. (Fort Leavenworth, KS: School of Advanced Military Studies, 01 April 1993), DTIC. ADA 262609.

House Permanent Select Committee on Intelligence on the impact of prioritizing intelligence efforts:

> PDD-35[45] is designed to present the Administration's highest national security priorities, thereby providing the IC guidance for resource allocations, by establishing a "tier" structure. Unfortunately, but predictably, the IC is using PDD-35 to ensure that resources are being placed on the highest-tier issues, **in many cases having little or no resources left for lower-tier issues**…. [Emphasis added][46]

This focusing of resources has a series of unintended consequences for the AIC and the military commander:

> Other non-military requirements for these lower-tier countries, however, such as a country's political climate, economic structure, and internal stability, are of much lower priority or not reflected as having priority. Moreover, the growing number of Support to Military Operations (SMO) requirements threaten to consume resources that could be used to address non-military requirements….As a result, the Community may spend more time gathering intelligence for potential SMO than for monitoring other developments that might aid in supporting diplomatic efforts to prevent a situation where deployment of forces would be necessary. **Ironically, several of the CINCs expressed the desire to have the type of non-military information that was traditionally important only to civilian policy makers**. [Emphasis added][47]

Thus, the DODIPP's process for developing and sustaining the baseline is undercut by management decisions to meet the most critical requirements. The effect is exacerbated as analysts and resources bounce from crisis to crisis.

---

[45]"Presidential Decision Directive 35 (PDD-35) defines intelligence requirements from tier 0 to tier 4. Tier 0 is warning and crisis management. Tier 4 is countries that are virtually of no interest to the United States. The PDD specifically identifies targets that the US intelligence community will not collect against.

"Under PDD-35 highest priority is assigned to intelligence Support to [on-going] Military Operations [SMO]. The second priority is providing political, economic, and military intelligence on countries hostile to the United States to help to stop crises and conflicts before they start. Third priority is assigned to protecting American citizens from new trans-national threats such as drug traffickers, terrorists, organized criminals, and weapons of mass destruction. High priority is also assigned to Intelligence support to activities addressing counter-proliferation, as well as international terrorism, crime and drugs.

"This Directive established the Intelligence Priorities Interagency Working Group [IWG] as the forum for identifying foreign policy issues that are of sufficiently critical nature as to require amplified attention from the intelligence community. In addition, agencies represented in this interagency working group have established intelligence requirements groups to collect, analyze and rank strategic intelligence requirements and to represent these agency-level requirements at periodic meetings with the intelligence community to set intelligence requirements." Summary by Federation of Atomic Scientists. "*Presidential Decision Directive 35, 2 March 1995*," not dated, URL: http://www.fas.org/irp/offdocs/pdd35.htm, accessed 3 JAN 03.

[46]House Permanent Select Committee on Intelligence House of Representatives, *"IC21: The Intelligence Community in the 21st Century,"* 104th Congress, 1996, URL: http://www.fas.org/irp /congress/1996_rpt/ic21/ic21011.htm, accessed 2 January 2003, 7.

[47]Ibid.

This sets up a cycle of response that is the root of the AIC's challenges for the future: The Search Phase, The Surge Phase, and the Sustain Phase**.** Figure 4 illustrates the general pattern of information lag in the crisis sequence:

- **The Surge Phase**: The AIC gathers everything of military significance concerning the crisis region as soon as there are indications of future employment. Typically, the AIC discovers that existing databases and analysis are insufficient or insufficiently detailed. Most significantly, the AIC is unable to answer critical questions at precisely the time decision-makers must make the most critical decisions - during the dynamic and frantic pre-deployment planning phase. [48]

- **The Build Phase:** The AIC marshals extraordinary resources and begins to discover where the requisite information exists and starts building a usable knowledge base. The information comes from previous collection, non-traditional existing knowledge centers, and/or new collection. Again, the JTF are typically engaged in operations by the time the AIC achieves critical mass and crosses the "Required Intelligence" threshold.

- **The Sustain Phase:** The AIC has established a mature and sustainable collection, analysis, and reporting process tailored to meet the operational requirements. At this point, intelligence is well established and developed to the depth and breadth the decision-makers require to conduct sustained operations. Resources are gradually released as operations become routine.

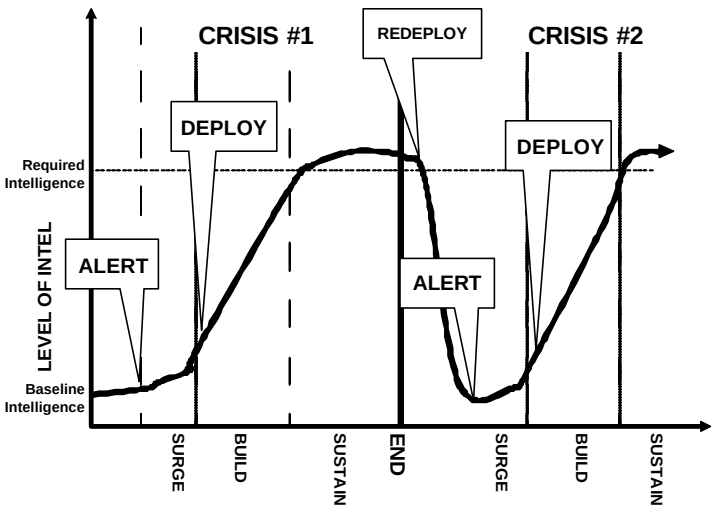


Figure 4: Intelligence Crisis-Response Cycle

Casual observation leads to an obvious strategy to mitigate this cycle: shorten the Surge and Build phases. These are the most time-sensitive elements of a crisis lifecycle, where the operational need and level of uncertainty is the highest while the resources and background at the lowest available level. As the case studies illustrated, the deployed forces are eventually able to gain and sustain information sufficiency, but suffered challenges during the planning and initial deployment/employment phases.

[48]Patrick, 6.

Conclusion

The survey of the three case studies provides ample evidence that the AIC remains challenged in supporting the early phases of contingency military operations. In each case, the leadership later opined that force structure, operational planning, tactics, and mission profiles would have been significantly altered if the initial intelligence had been sufficient. Several specifically commented on the shortcomings of the intelligence databases and the AIC to provide the critical intelligence at the necessary detail, precision, accuracy, and timeliness. While outside the scope of this study, initial open source and anecdotal reporting indicates these conditions existed in the recent operations in Afghanistan. That these trends have continued beyond Cold War deployments through the past decade are a testament to their intractability.

A fundamental cause for this inadequate intelligence support is the AIC's inability to achieve and sustain situational understanding in contingency areas. As directed by PDD-35, the NIC concentrates its limited resources on the most pressing national security issues. The resulting lower-tier issues remain un/under-serviced until they become the subject of a crisis-action drill.

Were the AIC able to sustain collection and analysis prior to the crisis response, planning and execution would be far more effective. There is a long trail of studies and after action reviews with recommendations on how to do this, to include harnessing sympathetic institutions. However, none provides a recommended structure to systematize this relationship into the AIC. [49] As the following chapter demonstrates, even the ATCP and AI-TCP, the blueprints for future intelligence transformation, pay passing notice to this problem but do not establish and execute a solution.

[49]Steele, 21.

CHAPTER 4:

Does Army Intelligence Transformation Meet the Challenge?

Army Intelligence Transformation is part of the greater Army Transformation effort. The Army Transformation Campaign Plan (ATCP) describes the overall transformation effort, vision, and goals.[50] The Army Intelligence Transformation Campaign Plan (AI-TCP) nests within the ATCP, "lay[ing] out a *vision for Army Intelligence Transformation in support of Army Transformation* [emphasis in original]."[51] In doing so, it provides a large-scale roadmap for the orderly, systematic transformation process.[52] These are the two venues for evaluating how the AIC plans to transform.

Given this scope and purpose, it is both fitting and necessary to assess the ATCP and AI-TCP. Do they identify and address the fundamental challenge described in the previous chapter? If inadequate, this failure would critically affect the future Army's viability. However, even if they do identify the challenge, is the Army implementing a viable solution? A review of the implementation plan, assigned responsibilities, and dedication of resources will hint at future success.

[50]Department of the Army, "*Transformation Campaign Plan*," (For Official Use Only), (Washington, DC: GPO, 10 April 2001), ii.

[51]U.S. Department of the Army, *Army Intelligence Transformation Campaign Plan (AI-TCP)* (UNCLASSIFIED), (Washington, DC: Deputy Chief of Staff for Intelligence, August 2001), 2.

[52]Ibid.

Intelligence Transformation in the ATCP

The ATCP is the Department of the Army's Transformation Synchronization tool.[53] The Army Transformation actions are structured and managed through fifteen Lines of Operation (LO). These LOs link related transformation efforts and provide the structure to synchronize efforts across the Army. Each LO has a designated MACOM or HQDA Staff Directorate as a proponent, as well as Army Secretariat oversight.[54]

The majority of Army Intelligence transformation efforts fall under *LO #8: C4 and ISR*, with the Army G-2 and G-6 as co-lead.[55] Whereas the AI-TCP outlines the vision and strategy, the ATCP LO #8 is the vehicle to track and synchronize implementation at the Department of the Army level. Specifically, the ATCP LO #8's purpose is to:

> Synchronize, coordinate, and integrate Joint and Army concepts, capabilities and implementation of Intelligence Surveillance, Reconnaissance Operations; information Management; and Space Operations to enable the transformation of the Operation and Institutional Army into a decision superior, decisive Network Centric force.[56]

Thus, the ATCP LO#8 is one place to look for efforts to implement the AI-TCP vision and strategy. The second place is with the implementation of the AI-TCP itself.

---

[53]Department of the Army, "*Transformation Campaign Plan*," (For Official Use Only), i.

[54]Department of the Army, "Army Transformation Campaign Plan Line of Operation #15: C4ISR, VTC #4," briefing provided to the Vice Chief of Staff of the Army, 27 August 2002, Online posting, Army Knowledge Online Collaboration Site. 6 August 2002. URL: <https://www.us.army.mil/portal/jhtml/dc/index.jhtml?_DARGS=%2Fportal%2Fjhtml%2Fcustomization%2Fheader_homepage.jhtml.4_A&_DAV=-1>, accessed 11 December 2002.

[55]Formerly known as LO #15 – Brad T. Andrew, Staff Action Officer, Army Intelligence Master Plan, U.S. Army G-2, E-mail interview with author, 18 February 2003. Relatedly, AIC transformation will also be covered in the Intelligence, Surveillance, and Reconnaissance (ISR) Annex to the US Army Transformation Campaign Plan (Pre-Decisional Draft), 19 February 2003. While not yet released, a review of the draft document indicates that conclusions drawn about the LO #8 should remain valid for the ISR Annex – it does not directly address establishing an Integration Center or CRIP as stated in the AI-TCP.

[56]Ibid.

AIC Transformation: The AI-TCP

As noted, the AI-TCP lays out a vision for the future of Army Intelligence. It then provides a grand strategy for achieving this end state. The core of the strategy is six long-range planning objectives that, when reached, ought to achieve the vision. While not a formal tasking document, the strategy assigns general responsibilities and intermediate objectives for each of the long-term objectives. If not a roadmap, it at least is a strip-map for Army Intelligence transformation. A more detailed description of the AI-TCP follows:

AI-TCP – The Vision

> Army Intelligence vision is A TRANSFORMED ARMY INTELLIGENCE TEAM PROJECTING KNOWLEDGE AT THE POINT OF DECISION EMPOWERING THE OBJECTIVE FORCE TO… SEE FIRST … UNDERSTAND FIRST … ACT FIRST … and FINISH DECISIVELY! [emphasis in original][57]

The AI-TCP describes the vision for Army Intelligence after it has successfully transformed in parallel with the Army's transformation to the Objective Force. The Army G-2, LTG Robert Noonan, elaborates the vision and includes several key themes, to include: "knowledge-based," "collaborative," "high-technology," and harnessing the complex national intelligence community.[58]

LTG Noonan goes on to more fully explain how a collaborative intelligence community will gather and apply relevant knowledge to meet the warfighting decision-maker's requirements. He introduces the concept of knowledge centers (equated to the DIPCs described in Chapter 2) and distributive operations:

> This vision requires distributed intelligence operations….Expert personnel will harness the capabilities of knowledge centers to support warfighters. Intelligence units organic to units of action and employment will not likely possess the equipment and expertise to satisfy all of the commander's intelligence requirements in all situations. The Army enterprise

[57]Ibid., 17.

[58]Robert W. Noonan, Jr., LTG, and Brad T. Andrew, LTC (RET). "Army Intelligence Provides the Knowledge Edge," Army Magazine, April 2002, URL: http://www.ausa.org/www/armymag.nsf, accessed 21 December 2002, not paginated.

> strategy envisions seamless linking knowledge centers in a collaborative environment to harness the power of knowledge management to support the warfighter. These knowledge centers include the national intelligence agencies, as well as academic and think-tank institutions, that Army intelligence organizations leverage to provide enabling intelligence to units of action and employment.[59]

With this amplification, LTG Noonan explicitly identifies that the AIC does not – and will not – possess the requisite expertise at the right place and time to support any given contingency.

Thus, the AI-TCP Vision *does* identify elements of the shortfall that leads to the crisis-response cycle. It remains in the strategy and execution to determine if it develops the key concepts, places the appropriate priorities, and sets the conditions for success.

AI-TCP - The Strategy

The AI-TCP establishes six long-range planning objectives to accomplish intelligence transformation. They cross the entire Doctrine, Training, Leaders, Organization, Material, and Soldiers spectrum.[60] Planning Objective #5, "*Transform EAC to ensure vertical collaboration, integration, and synchronization of national, joint, and civilian Knowledge Center-expertise to project the right knowledge at the Point of Decision*," focuses on integration and collaboration in general. If the AI-TCP is to address any collaboration initiatives, it would be here.

---

[59] Ibid.

[60] U.S. Department of the Army, *Army Intelligence Transformation Campaign Plan (AI-TCP) (UNCLASSIFIED)*, 55-60. They are:

- Long-Range Planning Objective #1: Establish a balanced, globally responsive, integrated, "Knowledge Projection Force," focused on the needs of tactical commanders, but capable of anticipating the needs of policy makers.
- Long-Range Planning Objective #2: Equip the future intelligence force to ensure responsive, deployable, agile, versatile, lethal, survivable, and sustainable capabilities in a non-linear battlespace. These characteristics are fundamental to achieving "Dominant Knowledge" and mission success across the spectrum of conflict.
- Long-Range Planning Objective #3: Train and educate the future intelligence force to thrive in the information dimension of the battlespace.
- Long-Range Planning Objective #4: Develop intelligence doctrine and policy to support joint intelligence operations in the information domain.
- Long-Range Planning Objective #5: Transform EAC to ensure vertical collaboration, integration, and synchronization of national, joint, and civilian Knowledge Center-expertise to project the right knowledge at the Point of Decision.
- Long-Range Planning Objective #6: Produce ground forces intelligence that supports ground component force development on a full time basis and warfighting in a complex, international environment.

The AI-TCP elsewhere describes a suggested means to improve its collaboration capability: "The Integration Center is charged with getting "the right knowledge, to the right person, at the right time," linking the knowledge centers:[61]

> Expert capabilities resident in Knowledge Centers are leveraged in support of commanders forward. Effective leveraging of Knowledge Centers will be achieved by a combination of reorienting a subset of Army personnel already assigned to these organizations, and assigning additional personnel specifically to create a tactically focused capability.[62]

With only cursory detail, the AI-TCP implies that this Integration Center will be the heart and brain enabling the distributive intelligence vision described above.[63] However, it does not specifically envision non-governmental knowledge centers as a core resource.

Although not a formal tasking document, the AI-TCP then gives the Intelligence and Security Command (INSCOM) responsibility for developing Planning Objective #5, to include the Integration Center.[64] The specific enabling objectives are:

- Designate an EAC Integration Center to orchestrate and focus the efforts of the various Knowledge Centers on projecting the right knowledge to the right person at the right time to ensure decision makers "see first, understand first, act first, and finish decisively."
- Ensure integration of I&W Centers, Multi-Component Support Brigades, and commercial and academic Knowledge Centers as appropriate (requires establishment of new TTP to leverage the civilian sector).
- Codify in partnering agreements, TTP, organizational development, and equipment acquisition and resourcing plans EAC operations in direct support of Units of Action and Employment (i.e. rapidly performing signal survey functions; deploying adaptively tailored special purpose systems to conduct niche and gap collection; employing Information Warfare capabilities; providing dedicated and surge analytical support, etc).
- Create transport layer to seamlessly link Knowledge Centers and EAC Integration Center with Interim Brigade Combat Teams (IBCT), divisions and corps (i.e. TROJAN Backbone linked to various classified and unclassified LANs / communications rings).[65]

Thus, the AI-TCP does, at least indirectly, identify and address the shortfalls noted in Chapter 3. Unfortunately, it proposes more tightly weaving together the AIC and MIC as the means to achieve

---

[61]Ibid., 23-4.

[62]Ibid., 23.

[63]Ibid.

[64]Ibid., 35.

[65]Ibid.,59.

better performance. It only tangentially addresses the concept of leveraging the non-governmental knowledge centers and does nothing to use this method to expand the baseline of information available to the AIC.

Will the AIC Meet the Challenge?

Despite the limited applicability of the ATCP and AI-TCP's solutions, it is still prudent to assess if they would (or could) address the base problem. There are two means to do so: through the ATCP LO #8 and through the AI-TCP Long Range Planning Objective #5, as executed by INSCOM.

ATCP LO #8 Execution

LO #8 does not directly or indirectly address establishing an Integration Center as envisioned by the AI-TCP. Specifically, in the early development of LO #8, the AIC identified 57 separate actions and efforts that must be accomplished in order to affect AIC Transformation. Of these, only one action approaches the Integration Center concept even remotely.[66] But, this action focuses on other requirements. It does not provide adequate visibility or guidance for developing a routine means to access non-governmental knowledge centers. As such, the ATCP LO #8 does not indicate that there is any formal effort at the Department of the Army level to tap these information sources.

AI-TCP Execution

The AI-TCP's reference to collaboration has not been implemented as envisioned either. The terrorist attacks of 11 September 2001 overcame INSCOM's initial response to the AI-TCP.

[66] "#56: Functional Architecture: Required by Congressional Mandate to define operational requirements of the Interim and Objective Force in determining materiel requirements to enable the warfighter, while insuring [sic] cross-functional, cross-Service, Joint and National ISR interoperability. Required for AROC (Army Resource Oversight Council) and JROC (Joint Resource Oversight Council) validation." - Ibid.,

Faced with the requirement to support the global war on terrorism, initial efforts were tabled as INSCOM's resources were refocused to the higher priority operations. There has been no action to develop a means of systemically tapping non-governmental knowledge centers. Moreover, INSCOM cannot estimate when that initiative will resume, if at all.[67]

Those familiar with INSCOM's operations may point to the AIC's accomplishments in collaborative intelligence operations as proof that the collaborative concept is alive and well.[68] Through the Information Dominance Center (IDC), INSCOM has weaved together an impressive capability; incorporating INSCOM's other organic knowledge centers and many of the MIC and NIC's complimentary organizations. To review INSCOM's current efforts:

> Currently INSCOM has used the Information Dominance Center (IDC) as the structure or place to develop a predictive I&W effort against Counter-Terrorism targets. This effort uses streaming data from various sources, access to databases for data mining, and tagging incoming data, reports, etc. into databases. Then using advanced analytic and display tools to show relationships in the data and information to aid the analytic process and make the job of the analysts easier. In addition to the IDC at INSCOM HQ, Mini-IDCs or IDC extensions have been placed in the Theater Intelligence Brigades and Groups (TIB/TIGs)….These are theater focused and link back into the IDC at INSCOM in a collaborative way. …This…gets to the issue of the vertical collaboration, as well as horizontal collaboration among knowledge centers.[69]

These efforts mark a quantum leap in collaborative analytic capabilities and have played critical roles in on-going operations.

However, it is important to note that the IDC's operations do not directly address the shortfall identified previously. The IDC initiative enables collaborative intelligence production between knowledge centers from within the intelligence community and *that are already in the Sustain Phase*. The IDC was not assigned the pre-crisis responsibility to coordinate, integrate, and exercise the building of a team of Army-requirements-focused experts in global terrorism. As such, the networks, procedures, and connectivity to non-governmental experts were not already

[67]Robert F. Scruggs, Staff Action Officer, AI-TCP Liaison, U.S. Army Intelligence and Security Command, E-mail interview with author, 6 February 2003.

[68]Robert F. Scruggs, Staff Action Officer, AI-TCP Liaison, U.S. Army Intelligence and Security Command, Personal interview with author, 4 March 2003.

[69]Ibid.

established. Moreover, the IDC did not monitor and track the respective knowledge centers' current status and capabilities to meet the intelligence requirements prior to the crisis. Rather, the integration and collaboration procedures and capabilities were built on the fly through the hard work and tremendous efforts of dedicated intelligence professionals.

Additionally, the collaborative team did not systemically include academia and the private sector. Their presence and contribution is typically solicited and incorporated in an ad hoc manner as predicted in the crisis response cycle. While the IDC may have shortened the Surge and Build Phases through technology and connectivity, it does not mark the quantum change in operating practices implied by the AI-TCP and it does not expand the base of knowledge in those areas where the AIC has historically failed.

Conclusion

The AI-TCP provides a wide-ranging and comprehensive vision and strategy for transforming Army Intelligence, within the context of the ATCP. Moreover, it implicitly recognizes the challenge military intelligence has in meeting global contingency and crisis operations – having the requisite expertise at the right time and place. In doing so, it validates the conclusions drawn in the previous chapter.

However, neither the ATCP nor the AI-TCP substantively addresses this problem. The ATCP does not indicate any initiatives. The AI-TCP somewhat addresses this shortfall through the proposed Integration Center; but, it only tangentially includes non-governmental knowledge centers as a means to fill the gaps within the AIC. Rather the AIC has focused on improving the linkages and collaborative capabilities *within* the AIC and MIC. The Information Dominance Center is the most visible example of this effort. While a necessary investment in modernizing the AIC's infrastructure and capabilities, it still fails to tap the vast pools of knowledge available outside of the NIC.

Moreover, without a plan to fundamentally address the problem, resources and energy that might have been available have been diverted. In executing this current mission, the AIC is forgoing the investment necessary to achieve a long-term solution. This is, ironically, yet another example of the crisis-response cycle in action. The focus on the immediate requirements may be leading the AIC to miss an opportunity to achieve a long-term solution – a solution that may well reduce the overall strain and provide a quantum leap in performance when and where it really counts.

Fortunately, there is a potential solution that is relatively low-cost, generally fits within the existing AIC structure, and can be implemented in parallel with the on-going intelligence operations. What follows is a program that would integrate smoothly into to the on-going transformation effort. It taps a massive national resource of information and intelligence and, if aggressively executed, would vastly improve support to combat operations. Moreover, it could break – or at least flatten - the crisis-response cycle.

CHAPTER 5:

A Better Strategy

INSCOM's work with the IDC is critical and necessary, but insufficient. The investment in the collaborative infrastructure and procedures is excellent. It improves the process of building knowledge and sustaining distributive intelligence support operations. However, it does not address the fundamental challenge within the intelligence community: sustaining a sufficiently broad and deep intelligence baseline in support of contingency response timelines. In short, it does not fill in the gaps in the baseline.

The AIC must explicitly change a basic assumption. Rather than solely improving internal processes, the AIC must accept that the organically developed intelligence baseline will *always* be inadequate. Given this, the main effort should be to build, optimize, and sustain *the process of building the information superiority in a timely basis* – again, filling the gaps in the Surge and Build phases. More importantly, the net must be cast more widely to draw on the non-governmental organizations that can fill in these gaps.

As previously noted, the intelligence community routinely draws on these information sources in an ad hoc and inefficient manner. However, an organization designed to identify, build, and sustain formal relationships based upon validated intelligence requirements could standardize this process. Moreover, given a robust exercise program (tied to existing military exercises and operations), this organization would be well placed to develop and mature all elements of the process (train the organizations on the nature of military requirements, exercise with the supported Army unit, exercise the collaboration systems and tools, *etcetera*). The Army would turn an ad hoc process into a robust and responsive operational system.

Why this Approach?

Establishing and rehearsing a system for building knowledge teams prior to a crisis is not just an initiative that falls in the "nice to do" category. It is supported by research and doctrine and should be one of the primary imperatives for the AIC's transformation. Joint Doctrine and Army policy explicitly support establishing this approach. Specifically, Joint Publication 2.0 directs intelligence organizations to

> "Establish and maintain a comprehensive directory of intelligence reach resources before deployment and throughout operations. The value of intelligence reach will greatly increase as the staff develops and maintains ready access to rich information resources. These resources are numerous and may include, for example, Army, Joint, DOD, non-DOD, national, commercial, foreign, and university research programs."[70]

However, it falls short by failing to direct building and sustaining a strong relationship with these resources.

Army policy also supports this approach. The Army Knowledge Management Plan, developed by the Army G-6 and approved by the Chief of Staff of the Army, establishes two objectives that specifically apply:

- **Objective 2.1 Develop new knowledge centers and cultivate existing ones**: This objective leverages existing knowledge centers and fosters their continued development (IDC evolution is consistent with this process). It also supports the creation of new knowledge centers at DOD, HQDA, and MACOM levels that facilitate the transfer of knowledge for superior decision-making.[71]

- **Objective 2.2 Pursue relationships with academia, professional societies, and industry.** This objective seeks KM partners to serve as successful models for the Army. This ensures a quality KM program. Partners include the best in business, academia, and professional societies.[72]

These demonstrate an Army-wide acknowledgement of the requirement to formalize and mature the collaborative team-building process both within and outside of the Army.

---

[70]Joint Chiefs of Staff, Joint *Publication 2-0. Doctrine for Intelligence Support to Joint Operations (DRAFT),* (Washington, DC), paragraph 2-59.

[71]U.S. Department of the Army, *"Army Knowledge Management: A Strategic Plan for an Agile Force,"* (Washington, DC: GPO, 8 August 2001), not paginated.

[72]Ibid.

Additionally, public research supports establishing coordinating procedures and organizations prior to the crisis. Specifically, disaster relief operations share many of the same characteristics as contingency operations: unknown timing, unknown requirements, and a rapidly changing situation well outside of the control of any one organization. Rather than trying to sustain all of the potentially necessary capabilities organically, the disaster relief community establishes procedures and organizations to rapidly build a tailored and immediately effective crisis-response team.[73] The applicability to intelligence support for crisis operations is immediate and obvious.

Not a Technology Solution

> "It has been assumed that knowledge management tools will unproblematically enable managers to manage knowledge with reasonable ease…Because the very nature of knowledge (and, therefore, of knowledge work) is obscured…pertinent organizational issues…tend to be inadequately considered."[74]

Integrating non-government knowledge centers into the intelligence effort requires an organizational and procedural response, *supported by technology that already exists and is mostly in place*. The solution is not technology-centric. A technology focus would be duplicative of other initiatives, ineffective in actually building and sustaining a distributive knowledge base, and the wrong road to go down.[75]

> In the last 20 years, US industry has invested more than $1 trillion in technology, but industry-wide analysis of IT investments shows no relationship between IT expenditures and company performance. This disconnect between IT expenditures and the organizational performance may be attributed to managerial ignorance of ways in which knowledge workers communicate and operate through the social process of collaborating, sharing knowledge, and building on each other's ideas.[76]

Thus, the evidence suggests that a technology-centric approach alone is of little value in achieving quantum improvements in performance and business practices.

---

[73]Jintae Lee and Tung Bui., "A Template-Based Methodology for Disaster Management Information Systems," Proceedings of the 33rd Hawaii International Conference on Systems Sciences – 2000, (Honolulu, Hawaii: University of Hawaii at Manoa, 2000), abstract.

[74]Ibid., 43.

[75]Ibid., 45.

[76]Ibid.

Modeling the Solution on Successful Program

The DoD has a model for establishing relationships and procedures for leveraging the private sector to meet operational and tactical military requirements – the Civilian Reserve Air Fleet (CRAF).[77] The CRAF program meets an analogous requirement for the US Air Force and the US Transportation Command (USTRANSCOM) – it satisfies permanent, structural shortfalls of in-house capacity through a formal, contractual relationship with non-government organizations that have the requisite capacity and a stake in sustaining that capacity for their own purposes. Specifically, CRAF:

- Identifies specific shortfalls in strategic lift capacity against projected requirements
- Identifies organizations that have organic capabilities to meet these shortfalls
- Establishes a contractual relationship with the organizations; providing two-way benefits (guaranteed business-levels in exchange for access to lift capacity for contingency/crisis operations)
- Establishes specific standards of support expected and required
- Establishes a pre-crisis monitoring and coordination regime to ensure ready implementation
- Exercises the relationships with the contracted organizations during peacetime and in support of military exercises
- Execute mobilization as required[78]

[77]CRAF is a unique and significant part of the nation's mobility resources. Selected civil aircraft from U.S. airlines, contractually committed to CRAF, support Department of Defense airlift requirements in emergencies when the airlift need exceeds the capability of military aircraft.

The airlines contractually pledge aircraft to the various segments of CRAF, ready for activation when needed. To provide incentives for civil carriers to commit aircraft to the CRAF program and to assure the United States of adequate airlift reserves, the government makes peacetime airlift business available to civilian airlines that offer aircraft to the CRAF. The DOD offers business through the International Airlift Services, which is the largest contract. For Fiscal Year 2003, the guaranteed portion of the contract is $394 million. AMC estimates that throughout Fiscal Year 2003 it will also award over $224 million in additional business that is not guaranteed.

To join CRAF, carriers must maintain minimum Long-Range International fleet commitment levels (30 percent for passenger and 15 percent for cargo). Aircraft committed must be U.S.-registered aircraft capable of over water operations, at least 3,500 nautical mile range, and 10 hours per day utilization rate. Carriers must also commit and maintain at least four complete cockpit crews for each aircraft. - U.S. Department of the Air Force, "USAF Fact Sheet: Civil Reserve Air Fleet," January 2003, URL: <http://www.af.mil/news/factsheets/Civil_Reserve_Air_Fleet.html>, accessed 15 December 2002.

[78]Ibid.

If "strategic lift," were substituted with "information/intelligence," then CRAF would describe a program designed to meet the systemic shortfalls in the intelligence baseline.

The AIC's "CRAF" - The Civilian Reserve Intelligence Program

The AIC must establish a functionally equivalent program with an assigned management organization. A Civilian Reserve Intelligence Program (CRIP), modeled after CRAF in form and function, meets this requirement. Again, for the reasons noted in Chapter 1, CRIP is deliberately restricted to an Army-only solution, at least initially. An Integration Center, as generally envisioned by the AI-TCP, would serve as the CRIP's executive organization. CRIP's elements and functions are described in more detail below.

Identify Shortfalls

The Integration Center's initial role is to monitor current, and more importantly, *projected* intelligence requirements and assess shortfalls in capacity. More specifically, it must establish the procedures for the DIPC's currently operating within the DoDIPP to report their known and projected shortfalls in information and analytic expertise as they apply to Army-specific requirements. Thus, the Integration Center's initial purpose would be to catalogue and monitor the systemic gaps within the AIC and MIC.

Identify Available Resources/Organizations

Joint Publication 2.0 identifies government and government-associated organizations that participate in distributive intelligence operations.[79] It further describes several non-government organizations, specifically media corporations, as potential partners for distributive intelligence operations. The Integration Center will identify additional non-governmental organizations that

[79]Joint Chiefs of Staff, *Joint Publication 2-0 (DRAFT)*, paragraph 2-58.

meet the expected intelligence requirements. These include, but are not limited to:

Organization	**Information/Intelligence**
Non-Government Organizations / Private Volunteer Organizations:	– cultural awareness – social/ethnic demographics – secondary infrastructure (outlying areas) – unconventional threat forces – local leadership / power structure – informal economic structure
Academia	– cultural awareness – social/ethnic demographics – government structure / political patterns – leadership – formal economic structure – trip reports from sabbaticals / on-site research
Multinational Corporations – Petrochemical/energy – Information/telecommunications – Engineering/Construction – Financial Institutions/Investment banking – International Media	– energy infrastructure – road infrastructure – terrain data – telecommunications infrastructure – formal economic structure – key economic/financial leadership – economic projections/assessments

Table 1: Non –Government Reach Resources

The organizations listed in Table 1 have vested interests in maintaining the types of information suggested. This information is critical to their fundamental business model. In order to be effective and competitive, they must apply resources and assets to develop and sustain the information, albeit in formats and the level of detail required for their internal uses. In short, they routinely provide the sustained, human interaction within the targeted environment that the case studies indicated were lacking.

Moreover, they represent the functional equivalent to the civilian air fleet – self-sustaining capacity that is relatively appropriate to military use, with minor modifications. Their information could become militarily valuable intelligence if analyzed, integrated, and packaged appropriately.

Establish Contractual Relationships

Leveraging these organizations and their information is not a new concept. These types of organizations are tapped routinely in an ad hoc and inefficient manner for current operations. Unfortunately, this is inefficient and provides wildly varying results. Using the appropriate contracting or other formal procedures, they should be 'put on retainer' for 'call-up' when required in a systematic manner. The challenge is finding appropriate mechanisms to establish this relationship.

Again, CRAF provides a model for this mechanism. The US Government, in some form or fashion, has standing business relationships with corporations from many of these industries and activities. As with CRAF, CRIP would integrate into these existing government contracts via "rider" sections. These riders establish the requirement for the contracting organization to make available information and expertise that they would reasonably be expected to maintain as part of their normal business practice.[80] More specifically, the riders establish the requirement that the collected information be maintained in a format and context immediately useable to the AIC for intelligence operations. The following section outlines these proposed requirements in more detail.

Naturally, the contract price should reflect the cost (plus an incentive profit) for maintaining the information in the format required by the AIC. Reimbursement would be for handling the information to meet Army requirements, not for the original collection. That would have been part of the institution's standing business practice and not a unique from the Army. Of course, additional reimbursement would be appropriate for any unique information specifically collected or analyzed in conjunction with organic operations.

Even more challenging than establishing the contractual relationship with corporations is demonstrating a mutual benefit with many NGO/PVOs. These organizations historically have

[80]While outside the scope of this document, establishing contractual riders may require legislative support from Congress. Additionally, it implies coordination/visibility of the corporations contracting with the US Government.

resisted associating with the United States military.[81] However, the military has numerous capabilities that can be tempting incentives (many of which are already provided on an ad hoc basis which belies effective planning for either organization). These incentives could include:

- guarantees of strategic and intra-theater lift support,
- communications support,
- medical support, life support (food/water, etc.), and
- dedicated security while in certain high-risk environments.

While not all NGO/PVOs would accept these incentives, many assuredly would, particularly if the information requirements levied are ethically neutral. Thus, CRIP would enable both the NGO/PVOs and the military to better plan requirements and capabilities for contingency operations *and* allow the AIC to routinely leverage their knowledge base.

Establish Specific Standards of Support

CRIP's standards of support are broken into three basic categories: unprocessed information; processed information; and expert analytic support. Each contracted organization would provide support in one or more of these areas. The key Integration Center task is to describe adequately the type, quality, and format of this support. It must be tailored to match the requirements established by the consuming organization within the Army.

The following are examples of how these categories might be established:

Unprocessed Information

This category generally applies to basic infrastructure and terrain description information requirements. Minimum information requirements can be established by applying a standardized worksheet for the organizations to complete and update in the course of their business in the targeted region. The worksheets may include physical descriptions, digital photographs, and minor

[81]Guy C., Swan, III. *Strengthening Military Relationships with NGOs During Complex Humanitarian Emergencies*. Carlisle Barracks, PA: Army War College, 26 March 1996), DTIC. ADA310858, abstract.

measurements (particularly if the contracted organization is technical in nature and would be gathering that information to begin with; e.g. an engineering/construction corporation).

Processed Information

This category generally applies to information that must be analyzed to be useable. For example, describing political or economic structures, assessing infrastructure capabilities, or providing general cultural or ethnic demographic information. Requirements can be described and satisfied via questionnaires and region/topic specific surveys that must be completed periodically. CRIP would host periodic conferences among the contracted organizations and the primary consumer units to encourage the integration of information and clarification of specific Army intelligence requirements. Moreover, this would provide the critical inter-personal interface so necessary to knowledge management.[82]

Expert Analytic Integration

This category applies to immediate crisis-response operations. Similar to CRAF drawing civilian aircraft into military service, contracting organizations would be committed to mobilizing their in-house experts to the appropriate DIPC (to include a JIC or possibly even a deployed JTF J-2 or ARFOR G-2). The nature and duration of their mobilization would be subject to contractual negotiations. Mobilizing experts with experience and some level of understanding of Army intelligence requirements, and familiarity with key organizations and personalities, would greatly facilitate building and executing distributed intelligence support operations.

---

[82]"Knowledge work is dominated by communication – discussion, deliberation, argumentation, debate, and negotiation….People usually talk in person, on the telephone, and via e-mail and groupware to share expertise and solve problems together. Knowledge circulates within the community….Much of that circulation occurs in informal, unwritten routine practices, mores, stories, and folkways.
When we look at our experience, the heart of knowledge is not the great body of stuff we learn, not even what the individual thinks, but a community in discourse, sharing ideas. Since the heart of knowledge resides within a community in discourse, to leverage knowledge, knowledge management must begin with identifying the natural community that owns/cares about a topic and the people who use it, not the knowledge itself." - Josephine Chinying Lang,. "Managerial Concerns in Knowledge Management," Journal *of Knowledge Management* 5, no. 1 (2001):,54.

Establish a Monitoring Regime

A key element to CRAF's successful implementation is the constant monitoring of the civilian air fleet to ensure compliance with the stated requirements. The same holds true for CRIP. The Integration Center is responsible for monitoring the contracted organizations' compliance with the information requirements levied. This includes monitoring the AIC's satisfaction with the quality and quantity of information provided within the bounds of the contract. Performance would necessarily affect contract recertification.

Exercise and "Mobilize"

Exercising the integration of contracted expertise into the AIC's intelligence operations is the heart of success and the key to shortening the Surge and Build phases of the crisis cycle. All of the previous elements of CRIP are merely enablers for this final, critical step. The Integration Center coordinates the mobilization of all three elements of intelligence support in conjunction with selected major exercises. The exercise support program is an integral element of the strategy and provides several benefits:

- Establishes/sustains personal relationships between the contracted organizations and the AIC
- Establishes, refines, and validates the process of building collaborative expert teams
- Familiarizes the contracted expert with specific Army requirements, and the context within which their intelligence will be used
- Familiarizes the AIC with the strengths and weaknesses of the contracted experts
- Identifies additional requirements
- Validates the program

Moreover, the exercise program validates the parallel investment in collaborative technology that the Army continues to make.

Recommended Organizational Placement

Given the Army-wide responsibilities and the requirement to interface with the MIC, NIC, and private sector, INSCOM is the logical executive agent for CRIP. INSCOM is the major command assigned responsibility for "echelon above corps" intelligence. Within INSCOM, the National Ground Intelligence Center (NGIC) is the most obvious implementing organization. The NGIC is fully integrated into the DoDIPP, understands Army-specific intelligence requirements, and already enjoys numerous relationships with academia and commercial institutions. Moreover, it routinely interacts with the rest of the MIC/NIC and is familiar with the process and procedures necessary to incorporate civilian information into military intelligence. Of course, the NGIC is not currently staffed or organized to conduct all of the functions identified above, and would require additional manpower and funding to be effective.

Comments on Resourcing

An important caveat is that CRIP requires a clear, sufficient, and sustained resource commitment in order to be viable. The NGIC (or whatever organization that eventually receives/develops the mission) is already operating under the severe resource constraints that drove the crisis response cycle to begin with. Adding additional mission without the requisite resources will only exacerbate the existing problem while inadequately developing a long-term solution. A detailed analysis between the expected improvements and the resource requirements is necessary before formal implementation. Arguably, the study would reveal that CRIP would provide far better intelligence more cheaply than if the AIC tried to develop and sustain the collection and execution internally. Presumably, INSCOM's pursuit of the AI-TCP LRPO #5 would have developed this analysis and recommendation, if it were continued.

Conclusion

CRIP clearly meets a long-standing deficiency in the AIC's structure and procedures. By establishing a formal program and responsible agency, CRIP would provide accountability, standardization, and the ability to track programmatically the AIC's efforts to leverage the private sector. All of this will go far in establishing the necessary metrics to evaluate effectiveness. Moreover, the program builds on an existing and effective DOD program, which can serve as a model for implementation.

CHAPTER 6:

Conclusion

This work attempts to address a critical shortfall in the way Army Intelligence supports Army operations under very specific conditions – a response to a crisis contingency operation. Army operations into contingency areas are unique for several reasons:

- the regions were typically low on the list of national priorities prior to employment;
- planning and preparation time is, by definition, short;
- the ability to bring overwhelming combat power to bear early is constrained by strategic lift capacity;
- **Army intelligence requirements are unique to the military in that they require a much higher degree of fidelity for both physical (terrain and environment) and social (politics, culture, economics, etc.) intelligence.**

These conditions mean that Army planners (and the supporting intelligence) come to the planning/execution "as they are." It places a premium on the depth and breadth of pre-crisis preparation in order to meet the timelines and requirements.

Within these parameters, the study seeks to rectify the crisis-response cycle within the Army Intelligence Community. While this pattern extends to the entire Joint community, this work remains limited to an Army-centric solution for two main reasons:

- **Army Special Interest:** the Army requirements are unique, and uniquely unsatisfied by the current system; and
- **Feasibility:** it is easier to develop a single-Service capability that later expands to into a Joint operation than to try and start out as a joint organization.

Implementing CRIP clearly has implications to the MIC and NIC. Moreover, it may well develop into a Joint program in the future. However, that initiative is outside of the scope of this work.

This recommendation to develop a Civilian Reserve Intelligence Program addresses a fundamental shortfall: the Army Intelligence Community, in concert with the military and national

intelligence community, is incapable of building and sustaining a sufficiently deep and broad intelligence baseline for the non-TIER 0/1 regions where military forces are likely to be employed. Rather than a failure of effort, this shortfall is the result of deliberate, pragmatic, and proper decisions based upon resource constraints and naturally shifting national and military priorities. As noted, on-going efforts to transform the Army to the Objective Force will only exacerbate the potential risks induced by the resulting intelligence crisis-response cycle.

As a given, Army Intelligence is in a constant process of modernization and evolution. Many of the current efforts focus on improving connectivity and virtual collaborative capabilities, both within the AIC and with the greater MIC and NIC. These improvements are both necessary and appropriate in leveraging the analytic and collection capabilities *already existent* in the AIC.

However, while necessary, these improvements are not sufficient. These efforts do not address the structural shortfall in baseline collection and analysis. Of course, simply providing more resources to increase the organic analysts and collection capability would help, to a degree; but would not address the structural flaws and dynamics that exist today. Arguably, a good part of any additional capability and analysts would be drawn into the same crisis-response pattern. They would help to provide even more detail and support for the crisis de jour, while not coloring in the black (or at least gray) intelligence holes that exist today.

Tragically, the formal Army Intelligence Transformation Plan (the AI-TCP and LO #8 of the ATCP) *does* recognize this shortfall. Moreover, it hints at a strategy to address the problem. However, due to ever-pressing contingency operations and resource and personnel constraints, this vision and strategy is at risk of abandonment. CRIP, as an adjunct program to the AIC Transformation, offers a viable and feasible low-cost solution that meets the intelligence requirements while avoiding the pitfalls of adding to the organic AIC structure.

Recommended Actions

Developing the CRIP requires a deliberate and relatively long-term commitment by the Army and AIC. Formally developing the CRIP to the maturity and capability envisioned would be a multi-year investment in time, personnel, money, and effort. For example, this research suggests that INSCOM is the proper major command to host this capability, with the National Ground Intelligence Center a logical starting point. However, these suggestions are simply that – suggestions designed to spark a more formal development of the concept. Prior to embarking down any path, more legwork must be done.

In order to establish an effective CRIP program, several actions must take place. These actions will confirm if the CRIP is feasible, acceptable, and sustainable for the AIC, as outline in this recommendation. As the preponderance of issues fall within the Echelon Above Corps (EAC) realm, INSCOM and/or Army G-2 should take lead.

Suggesting CRIP immediately generates numerous questions about its size, scope, structure, and operating procedures. These must be identified before there are any changes made to the AIC. Thus, the following studies must be completed before any programmatic options are offered:

- Identify the Specific AIC Intelligence Shortfalls
    - Task: Review known and projected *long-term* shortfalls in collection and analysis in support of Army intelligence requirements (particularly in non-TIER 0/1 areas)
    - Purpose: Establish the scope, depth, and breadth of the requirement
- Identify the Potential Commercial/Private Institutions to Join CRIP
    - Task: Review relevant commercial and NGO/PVO operations to determine the scope, depth, and breadth of the civilian information available and pertinent to Army requirements.
    - Purpose: Specifically determine the viability of meeting extensive Army intelligence requirements from the commercial/NGO/PVO sector.

- Identify the legal, fiscal, and policy implications of CRIP
    - Task: Conduct legal review and feasibility/acceptability review of CRIP contractual relationship elements
    - Purpose: Determine if CRIP requires policy or legislative changes
- Identify a structure for CRIP
    - Task: Review DTLOMS issues
    - Purpose: Identify the proper organizational, funding, personnel, and related requirements to implement CRIP
- Identify a recommended host agency to execute CRIP
    - Task: Review pool of potential organizations appropriate for participation in CRIP
    - Purpose: Determine if there is sufficient expertise and focus in potential organizations to meet AIC requirements

The Army G-2 and Commander, INSCOM should initiate these recommended actions and develop the process to build the CRIP into a functioning program. The results of these actions would inform and guide the necessary DA and INSCOM-level staff actions necessary to implement the CRIP. Doing so quickly would go far to alleviate one of the perennial challenges to intelligence crisis-action support.

CRIP is a relatively low-cost solution to the AIC's – and ultimately the MIC and NIC's - structural challenges. The AIC can leverage private sector organizations to meet known and projected knowledge shortfalls. The private sector represents self-sustaining, self-motivating 'excess capacity.' It collectively maintains situational awareness of much of the world that is beyond our nation's current capabilities and/or interest. This excess capacity can be harnessed to meet AIC requirements. These organizations sustain the regional presence that the intelligence communities cannot. Quite simply, they are a national treasure of untapped capability that must be harnessed to meet national security requirements. Their sustained presence and focused analysis fills a gaping void in the official intelligence architecture. Arguably, given a robust and mature relationship with private-sector knowledge centers, CRIP would have greatly improved many of the intelligence support challenges noted in the case studies.

Bringing civilian resources to bear on building baseline intelligence and meeting crisis intelligence requirements is clearly a win-win solution. By establishing and exercising formal relationships with these organizations, the AIC can make great strides in reducing the Surge and Build phases of the crisis-response cycle. For the associated organizations, the program offers a variety of incentives to enhance and augment their business model with minimal effort. Bottom line, CRIP would satisfy a requirement that no other Army Transformation Program addresses.

On a cautionary note, for CRIP to be effective and lasting for the Army, an AIC organization must receive and accept full ownership and responsibility for success. The program must be executed by an organization with the necessary scope, authorities, and resources to establish and sustain the linkage between the private sector and the field Army.

Providing sufficient knowledge to support planning and execution of contingency operations is a fundamental mission for Army Intelligence. With the transition to the lighter, more agile Objective Force, the imperative for getting it right the first time is that much greater. The collaborative infrastructure must continue to develop, but so must the pool of expertise that it draws from, integrates, and brings to the fight. The CRIP is a sound, cost-effective means to achieve this necessary goal by fundamentally expanding how the AIC builds, maintains, and sustains its intelligence baseline.

BIBLIOGRAPHY

10th Mountain Division (Light). *U.S. Army Forces, Somalia After Action Report for Operation RESTORE HOPE*. Fort Drum, NY: 10th Mountain Division (Light), 1993.

Ackerman, Robert K. "Army Intelligence Deals with two Transformations." *Signal Magazine* 56, no. 5 (January 2002): 41-44.

Adelman, Howard, Astri Suhrke, and Bruce Jones. *Early Warning and Conflict Management: Genocide in Rwanda*. Fantoft-Bergen, Norway: Chr. Michelsen Institute, September 1995.

Andrew, Brad T., LTC (retired). Staff Action Officer, Army Intelligence Master Plan, U.S. Army G-2 (DAMO-IF). Series of e-mail interviews with author. 10 August 2002 to 31 March 2003.

Ash, Lawrence N. *Wilderness Guide. Providing Intelligence for the Commander in Bosnia.* Newport, RI: Naval War College. 06 March 1996. DTIC. ADA307494.

Bates, Troy R. "Internet Support to expeditionary Forces: Filling the Intelligence Gap." *Marine Corps Gazette* 81, no. 6 (June 1997): 41-44.

Berthiaume, Christiane. "NGOs: Our Right Arm." *Refugees* 97 (1994): 3-7.

Best, Richard A., Jr. "Peacekeeping: Intelligence Requirements." *CRS Report for Congress 94-394F*. Washington, DC: Congressional Research Service, Library of Congress, 6 May 1994.

Betts, Richard K. *Surprise Attack: Lessons for Defense Planning*. Washington, DC: Brookings Institution, 1982.

Binnendijk, Hans, and Patrick Clawson, eds. *Strategic Assessment 1995: U.S. Security Challenges in Transition*. Washington, DC: Institute for National Strategic Studies, National Defense University, 1995.

Bloechl, Timothy D. *Mission Complete? Tactical Intelligence During the Transition from War to Peace*. Fort Leavenworth, KS: School of Advanced Military Studies, 01 April 1993. DTIC. ADA262609.

Bond, Stephen J. *Strategic Intelligence for Tactical Operations: Intelligence Requirements for Force Projection*. Carlisle Barracks, PA: Army War College, 04 April 1998. DTIC. ADA343395.

Brady, Christopher, and Sam Daws. "UN Operations: The Political-Military Interface." *International Peacekeeping* 1, no. 1 (Spring 1994): 59-79.

Brei, William S., Capt, USAF. *Assessing Intelligence by Principles of Quality: The Case Study of Imagery Intelligence Support to Operation PROVIDE COMFORT*. MSSI Thesis. Washington, DC: Defense Intelligence College, July 1993.

Burlas, Joe. "Noonan: Transforming the Intelligence Force." Armylink News. 14 August 2000. <http://www.dtic.mil/armylink/news/Aug2001/a20010814noon0814.html>. Accessed 15 October 2002.

Cabeen, Jules P. and Brian R. Dunmire. "Alternative Change in the Force XXI GS MI (General Support Military Intelligence) Company." *Military Intelligence* 22, no. 3 (July-September 1996): 25-28.

Cavanaugh, John P., LTC, USA. *Operation PROVIDE COMFORT: A Model for Future NATO Operations*. Monograph. Fort Leavenworth, KS: School of Advanced Military Studies, 1992.

Center for Army Lessons Learned (CALL) Pamphlet 92-6. *Humanitarian Assistance, Volume 1, Operations other than War*. Fort Leavenworth, KS: CALL, 1992.

_____ *Bosnia Contingency Planning and Training*. Fort Leavenworth, KS: CALL, December 1992.

_____ *Joint Contingency Force Advanced Warfighting Experiment: Final Report*. Fort Leavenworth, KS: CALL, 2000. Available from Center for Army Lessons Learned Restricted Database, document ID RWP-12-422427.

_____ *Refugee/Migrant Support Operations Training Support Package, S2/Intelligence*. Fort Leavenworth, KS: CALL, n.d.

_____ *USMC NEO Lessons Learned*. Fort Leavenworth, KS: CALL, 1989. Available from Center for Army Lessons Learned Restricted Database, document ID RWP-03-157469.

_____"*Operation Restore Hope: Lessons Learned Report*." Fort Leavenworth, KS: Center for Army Lessons Learned, 3 DEC 1992 – 4 MAY 1993.

Center for Strategic and International Studies. *The Gulf War: Military Lessons Learned (Interim Report of the CSIS Study Group on the Lessons Learned from the Gulf War)*. Washington, DC: Center for Strategic and International Studies, July 1991.

Cici, Emin. "Knowledge Management as a Competitive Asset: A Review." *Marketing Intelligence and Planning* 18, no. 4 (2000): 166-170.

Commission on the Roles and Capabilities of the United States Intelligence Community. *Preparing for the 21st Century: An Appraisal of United States Intelligence* – a.k.a. "The Aspin-Brown Commission." (Washington, DC: GPO. 1 March 1996).

Costa, Christopher P., CPT, USA. "Changing Gears: Special Operations Intelligence Support to Operation PROVIDE COMFORT." *Military Intelligence* 18, no. 4 (October-December 1992): 24-28.

Defense Intelligence Agency. "Agency Operations and Training Assessment System." presented to the World Wide Joint Training Conference, 2002 by Paul Gregory. URL: http://www.dtic.mil/ doctrine/jel/training_pubs/19_dia.pdf. Accessed on 20 September 2002.

Eden, Steven J. "Knowledge-based Warfare Implications." *Military Review* 77, no. 2 (March-April 1997): 49-51.

Faint, Donald R. "Contingency Intelligence." *Military Review* 74, no. 7 (July 1994): 59-64.

Fast, Barbara G. "Building Situational Awareness in Force XXI." *Military Intelligence* 23, no. 4 (October-December 1997): 8-14.

Gavle, Kathleen A. *Division Intelligence Requirements for Sustained Peace Enforcement Operations*. Fort Leavenworth, KS: Army Command and General Staff College, 01 May 2000. DTIC. ADA381780.

Green, Gus E., Sr. *Distributive Collaborative Analysis: A New Approach for Intelligence Analysis.* Carlisle Barracks, PA: Army War College, 10 April 2001. DTIC. ADA390568.

Gregory, Paul. See *Defense Intelligence Agency*. "Agency Operations and Training Assessment System."

Harthcock, Clyde T. *Peace Operations from an Intelligence Perspective*. Carlisle Barracks, PA: Army War College, 30 April 1999. DTIC. ADA364597.

Hayden, Michael V., Brig Gen, USAF. "Warfighters and Intelligence: One Team—One Fight." *Defense intelligence Journal* 4, no. 2 (Fall 1995): 17-30.

Institute for Defense Analysis. *Enablers for an Effective Joint Rapid-Response Operations Force (JROF)*. By P.C. Albright. 01 February 2000. DTIC. ADA384838.

Johns, Sonja., Michael Shalak, Marc Luoma, and Donna Fore. *Knowledge Warrior for the 21st Century – Catalysts for Cultural Change*. Carlisle Barracks, PA: Army War College, 11 May 2000. DTIC. ADA380132.

Joint Chiefs of Staff. "Fact Sheet: Intelligence (J-2) Crisis Operations." 4 September 2002. <http://www.dtic.mil/jcs/core/crisisops.html.>. Accessed 15 November 2002.

_____ *Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3500.04B. Universal Joint Task List*. Washington, DC: GPO, 1 October 1999.

_____ *Joint Publication 1-02. DOD Dictionary of Military and Associated Term.* Washington, DC: GPO, 12 April 2001.

_____ *Joint Publication 2-0 (DRAFT). Doctrine for Intelligence Support to Joint Operations*. Washington, DC: not published.

_____ *Joint Publication 2-0. Doctrine for Intelligence Support to Joint Operations*. Washington, DC: GPO, 9 March 2000.

_____ *Joint Publication 2-01. Joint and National Intelligence Support to Military Operations (First Draft).* Washington, DC: GPO, 19 July 2002.

_____ *Joint Publication 2-02. National Intelligence Support to Joint Operations.* Washington, DC: GPO, 28 September 1998.

_____ *Joint Publication 3-0. Doctrine for Joint Operations*. Washington, DC: GPO, 10 September 2000.

_____ *Joint Publication 3-07. Joint Doctrine for Military Operations Other Than War*. Washington, DC: GPO, 16 June 1995.

Kellar, Charles S., MAJ, US Army. *Organizing Anarchy: Planning for Refugee Support Operations*. Monograph. Fort Leavenworth, KS: School of Advanced Military Studies, 1995.

Kirk, James A. *Putting Social, Cultural, and Political Factors into the Joint Doctrine Playbook.* Newport, RI: Naval War College, 04 February 2002. DTIC. ADA401839.

Landers, Daniel F. "The Defense Warning System." *Defense Intelligence Journal* 3 (1994): 21-32.

Lang, Josephine Chinying. "Managerial Concerns in Knowledge Management." *Journal of Knowledge Management* 5, no. 1 (2001): 43-57.

Lawlor, Maryann. "Eliminating the Fog of War." *Signal* 55, no. 2 (October 2000): 21-24.

Lee, Jintae, and Tung Bui. "A Template-Based Methodology for Disaster Management Information Systems." Proceedings of the 33rd Hawaii International Conference on Systems Sciences – 2000. Honolulu, Hawaii: University of Hawaii at Manoa, 2000.

Lilland, Jon B. *United Nations Peace Operations and the Brahimi Report*. MS thesis., Carlisle Barracks, PA: Army War College, 10 April 2001. DTIC. ADA 391135

Masback, Keith. "Transforming Army Intelligence." *Armed Forces Journal International: The Intelligence, Surveillance, and Reconnaissance Journal* 1 (January 2002): 30-35.

McCarthy, Mary. "The National Warning System: Striving for an Elusive Goal." *Defense Intelligence Journal* 3 (1994): 5-19.

McGuiness, Matthew P. *United States Special Forces – the 21st Century Urban Challenge*. Army War College, Carlisle Barracks, PA. 01 May 2000. DTIC. ADA380140.

Mitchell, Jeffrey F. "The Multicomponent Contingency Support Brigade: A Force Multiplier." *Military Intelligence Professional Bulletin* 28, no. 2 (April-June 2002): 34-37.

National Defense Research Institute, Arroyo Center. *Army Experiences with Deployment Planning in Operations Desert Shield.* 01 September 1990. Available from Center for Army Lessons Learned Restricted Database, document ID number RWP-13-447005.

Noonan, Robert W., Jr. "The Transformation of Army Intelligence." *Military Intelligence Professional Bulletin* 26, no. 4 (October-December 2000): 9-11.

Noonan, Robert W., Jr., LTG and Brad T. Andrew LTC (RET). "Army Intelligence Provides the Knowledge Edge." Army Magazine. April 2002. URL: <http://www.ausa.org/www/armymag.nsf/ (all)/5D28B37ED6F27A2 285256B83006E03F3?OpenDocument>. Accessed 20 December 2002.

Pacher, Leo R. *Redefining Military intelligence Leadership Skills for the Future*. Fort Leavenworth, KS: School of Advanced Military Studies, 15 May 2000.

Patrick, Melissa E. *Intelligence in Support of Peace Operations: The Story of Task Force Eagle and Operation Joint Endeavor*. Carlisle Barracks, PA: Army War College, 10 April 2000. DTIC ADA378285.

Peavie, Barrett K. *Intelligence Sharing in Bosnia*. Fort Leavenworth, KS: School of Advanced Military Studies, 01 January 2001. DTIC. ADA387143.

Potkovic, Troy M., 1LT, USA. "Operation CONTINUE HOPE: Maintaining Intelligence Credibility." *Military Intelligence* 21, no. 3 (July-September 1995): 18-20.

Rababy, David A., Capt, USMC. "Intelligence Support During a Humanitarian Mission." *Marine Corps Gazette* 79, no. 2 (February 1995): 40-42.

Rand Corporation. *Getting the Musicians of Mars on the Same Sheet of Music – Army Joint, Multinational, and Interagency C4ISR Interoperability*. 01 January 2001. Available from Center for Army Lessons Learned Restricted Database, document ID number RWP-03-188564.

Rapp, Jeffrey N. *Intelligence Requirements for Military Operations Other Than War: A Low Technology Business*. Carlisle Barracks, PA: Army War College, 26 March 1998. DTIC. ADA342276.

Resch, David T. "Predictive Analysis: The Gap Between Academia and Practitioners." *Military Intelligence* 21, no. 2 (April-June1995): 26-29.

Riggs, John M., LTG (US Army), Director, Objective Force Task Force. "Transforming the Army to the Objective Force." 22 July 2002. <http://www.objectiveforce.army.mil>. Accessed 11 November 2002.

Scott, Karren E. *Paradigm Shift: US Strategic Intelligence in the 1990's*. Carlisle Barracks, PA: Army War College, 06 April 1993. DTIC. ADA263584.

Scruggs, Robert F. Staff Action Officer, AI-TCP Liaison, U.S. Army Intelligence and Security Command. Interviewed by author, 4 March 2003. Frontier Conference Center, Fort Leavenworth, KS.

_____ E-mail interview by author, 6 February 2003.

Shelton, David L., MAJ, USMC. "Intelligence Lessons Known and Revealed during Operation RESTORE HOPE Somalia." *Marine Corps Gazette* 79, no. 2 (February 1995): 37-40.

Shelton, Paul A. "Frontline Intelligence for the 21st Century." *Marine Corps Gazette* 80, no. 9 (September 1996): 30.

Steele, Robert D. *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats*. Carlisle, PA: Strategic Studies Institute, 2002.

Steetin, Robert E. *The Media, Intelligence, and Information Proliferations: Managing and Leveraging the Chaos*. Carlisle Barracks, PA: Army War College, 16 January 1999. DTIC. ADA361151.

Stewart, John F., BG(P), G-2, 3rd United States Army. *Operation Desert Storm: The Military Intelligence Story: A View From the G-, 3d U.S. Army*. Fort McPherson, GA: Headquarters, 3rd United States Army, April 1991.

Story, Ann E., and Aryea Gottlieb. "Beyond the Range of Military Operations." *Joint Force Quarterly* 9 (Autumn 1995): 99-104.

Swan, Guy C., III. *Strengthening Military Relationships with NGOs During Complex Humanitarian Emergencies*. Carlisle Barracks, PA: Army War College, 26 March 1996. DTIC. ADA310858.

Thomas, John D. "MI Is Out Front in Army Transformation." *Military Intelligence Professional Bulletin* 26, no. 4 (October-December 2000): 2-4.

U.S. Congress. House. Permanent Select Committee on Intelligence. *IC21: Intelligence Community in the 21st Century*. 104th Congress, March 4, 1996. Committee Print.

U.S. Department of the Air Force. "USAF Fact Sheet: Civil Reserve Air Fleet." January 2003. URL: <http://www.af.mil/news/ factsheets/Civil_Reserve_Air_Fleet.html>. Accessed 20 January 2003.

U.S. Department of the Army. "Army Intelligence Transformation: Report to the CS/CSS Working Group." 14 December 2000. URL: <http://www.hqda.army.mil/logweb /directorates/pl/ Transofrmation%20LO9/LO9_main.htm>. Accessed 11 December 2002.

_____ Army Intelligence Transformation Campaign Plan (AI-TCP) (UNCLASSIFIED). Washington, DC: Deputy Chief of Staff for Intelligence, August 2001.

_____ "Army Transformation Campaign Plan Line of Operation #15: C4ISR, VTC #4." Online posting, Army Knowledge Online Collaboration Site. 6 August 2002. URL: <https://www.us.army.mil/portal/jhtml/dc/index.jhtml?_DARGS=%2Fportal%2Fjhtml%2Fcustomization%2Fheader_homepage.jhtml.4_A&_DAV=-1>. Accessed 11 December 2002.

_____ "Army Transformation Campaign Plan Line of Operation #15: C4ISR, VTC #5." Online posting, Army Knowledge Online Collaboration Site. 20 August 2002. URL: <https://www.us.army.mil/portal/jhtml/dc /index.jhtml?_DARGS=%2Fportal%2Fjhtml%2Fcustomization%2Fheader_homepage.jhtml .4_A&_DAV=-1>. Accessed 11 December 2002.

_____ *Field Manual 2-0. Intelligence* (Initial Coordinating Draft), Fort Huachuca, Arizona:. US Army Intelligence Center and Fort Huachuca. 25 October 2002

_____ *Field Manual 3-0. Operations.* Washington, D.C.: GPO. June 2001

_____ *Field Manual 34-3. Intelligence Analysis.* Washington, DC: Department of the Army, March 1993.

_____ *Field Manual 34-37. Strategic, Departmental, and Operational IEW Operations (Preliminary Draft)*. 15 August 2002. URL: <http://www.fas.org /irp/dodir/army/fm34-37_97>. Accessed 15 November 2002.

_____ *Field Manual 100-23. Peace Operations*. Washington, DC: Department of the Army, December 1994.

_____ The 2002 Army Modernization Plan. 15 August 2002. URL: <http://www.army.mil/features/ MODPlan/2002/default.htm>. Accessed 15 December 2002.

_____ *Training and Doctrine Command Pamphlet 525-75, Intel XXI – A Concept for Force XXI Intelligence Operations*. Fort Monroe, VA: Training and Doctrine Command, 1 November 1996.

_____ *Training and Doctrine Command Pamphlet 525-3-90. The United States Army Objective Force Operational and Organizational Plan for Maneuver Unit of Action*. Fort Monroe, VA: Training and Doctrine Command, 22 July 2002.

_____ *Training and Doctrine Command Pamphlet 525-3-93 (or 100 – pending final titling). Objective Force Unit of Employment Concept (Final Coordinating Draft).* Fort Monroe, VA: Training and Doctrine Command, 7 August 2002.

_____ Transformation Campaign Plan (For Official Use Only). Washington, DC.: GPO, 10 April 2001.

_____ Transformation Campaign Plan, Intelligence, Surveillance and Reconnaissance (ISR) Annex (DRAFT, Pre-decisional) (For Official Use Only). Washington, DC: Headquarters, Department of the Army. 19 February 2003.

_____ "U.S. Army White Paper: Concepts for the Objective Force." not dated. Accessed on 21 August 2002. URL: <http://www.objectiveforce.army.mil/ pages/objectiveforcewhitepaper.pdf.>. Accessed 12 November 2002

U.S. European Command (USEUCOM). *After Action Review Operation SUPPORT HOPE 1994*. Heidelberg, Germany: USEUCOM, 1994.

_____ *Operation PROVIDE COMFORT After Action Report*. Heidelberg, Germany: USEUCOM, 29 January 1992.

Wood, Todd R. *Can IPB Eliminate Mission Creep?* Fort Leavenworth, KS: School of Advanced Military Studies, 18 December 1997. DTIC. ADA340770.

Appendix A:

Evaluation Criteria

Army Intelligence "provide[s] commanders with the intelligence required to visualize the battlefield, assess the situation, and direct military actions."[83] The simple question in evaluating past (and predicting future) AIC performance in meeting this mission is clear – "historically, has the AIC provide sufficient intelligence to support the first 96 hours of combat operations? Will it be able to do so in the future?" This chapter sets the criteria for answering these questions.

The tasks comprising the AIC's mission are specified in a variety of complementary, hierarchical Joint and Army doctrine. A set of common tasks can be distilled from these sources and serves as the task list for evaluation. Once the tasks are identified, the second step is to detail the standards. Again, doctrine provides these standards. The final step is to establish the baseline conditions under which these tasks must be performed. While many of the conditions are specified or implied in approved doctrine, the assessment will include several inferred conditions to account for projected OF operational concepts. Only in doing so, will the assessment of future performance be of value.

Intelligence Requirements – Specifying the AIC's Tasks

Joint and Army doctrine provides nested, complementary guidance on intelligence support tasks for the DOD and AIC. These tasks were vetted against contemporary operational concepts and represent the requirements drawn from the standing force. There are four sources that capture the bulk of the Joint and Army intelligence doctrinal requirements – The Universal Joint Task List, Joint Publication 2.0, Army Field Manual 3.0, and Army Field Manual 2.0. The detailed and

[83]U.S. Department of the Army, *Field Manual 2-0, Intelligence* (Initial Coordinating Draft), (Fort Huachuca, AZ:. US Army Intelligence Center and Fort Huachuca, 25 October 2002), 1-8.

specific requirements can be distilled to a usable list by reviewing the nesting of the requirements from Joint down to Army doctrine. The result is the short task list that will serve as the evaluation categories.

The Chairman of the Joint Chiefs of Staff Manual 3500.04B, *The Universal Joint Task List (UJTL)*

Since the future Army operations are envisioned almost exclusively within a Joint force, Joint doctrine is particularly applicable as a starting point. The Chairman of the Joint Chiefs of Staff Manual 3500.04B, *The Universal Joint Task List* (UJTL) establishes the requirements for the Joint Force and subordinate units, including specific intelligence support tasks. While the UJTL's list of intelligence tasks is exhaustive, the key task, "OP 2.4.2.3: Provide General Military Intelligence (GMI) for the Joint Operations Area" covers most of the categories of detailed intelligence required for the deployed force. GMI is further defined in Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations (First Draft),* below.

However, OP 2.4.2.3 only provides the *categories of intelligence* necessary to support operations. The following tasks describe the requirements for operationalizing intelligence support, from pre-deployment preparation to supporting on-going operations – the *how* of providing the GMI. Reviewing these will help to describe the operating conditions and standards that apply to the intelligence community:[84]

TASK	DESCRIPTION
OP 2.2.1 "Collect Information on Operational Situation."	This fundamental task sets the baseline requirements for joint operations in the *pre-crisis phase*. It requires collection and analysis of significant information on enemy (and friendly) force strengths and vulnerabilities, threat operational doctrine, and forces. Additionally, it expands the intelligence requirement to include an entire battlespace characterization threat allies, insurgents, terrorists, illegal drug traffickers, belligerents in peace

[84] Joint Chiefs of Staff. *Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3500.04B. Universal Joint Task List*, 2-324 to 2-327.

TASK	DESCRIPTION
	support or peace enforcement situations, other opponents, the nature and characteristics of the area of interest, battlefield damage assessment, munitions effects, medical assessments, NBC contamination, political, economic, industrial, geospatial, demographic, climatic, cultural, and psychological profiles.
OP 2.4 "Produce Operational Intelligence and Prepare Intelligence Products"	Essentially, turning information into intelligence. Of note is that the *criteria for evaluation is measured in hours, not days or weeks.* [emphasis added]
OP 2.4.1 "Evaluate, Integrate, Analyze, and Interpret Operational Information"	Essentially, turning intelligence into Situational Understanding. This task captures the entire process of developing and maintaining situation understanding based upon collection and analysis.
OP 2.4.1.1 "Identify Operational Issues and Threats"	This task additionally specifies that the analysis must determine the impact of social, political, economic, and health environment on …campaign plans and joint operations.
OP 2.4.2.2 "Provide Current Intelligence for the Joint Operations Area"	Provide intelligence collected and produced IAW previous tasks, particularly GMI and targeting information
OP 2.4.2.4 "Provide Target Intelligence for the Joint Operations Area"	Provide detailed targeting information for lethal and non-lethal fires, as well as maneuver.
OP 2.5.3 "Provide Near Real Time Intelligence for the Joint Operations Area Planners and Decision Makers"	Near real time defined as within 5 seconds to 5 minutes of occurrence.

To summarize, the IC must prepare detailed descriptions and assessments of the area of operations in all areas of GMI (described below) prior to crisis action planning; provide continuously updated and predictive assessments of the AOR during deployment and employment; and provide targeting data to support lethal and non-lethal operations throughout. The support must be timely and detailed, with requirements measured in minutes to hours, rather than days and weeks.

The Joint Publications 2-x Series

The Joint Publications 2-x Series provides additional guidance and detail on how the Joint and Component Intelligence organizations will meet the UJTL requirements. JP 2-0, *Doctrine for*

Intelligence Support to Joint Operations, establishes the framework for the deliberate and crisis action planning phases of Joint and Component operations:

> Intelligence planning for rapid response to possible theater crises occurs well ahead of time as part of a command's overall, integrated deliberate planning process….When a particular crisis situation unfolds, crisis action planners develop an actual operation plan using deliberate planning as the basis. Intelligence input to the operation plan includes an adjusted and updated threat scenario and an intelligence annex that tailors intelligence support to the geographical area, nature of the threat, scope of operations, and assigned forces.[85]

Of particular note is the requirement to conduct intelligence planning and collection well before a crisis evolves.

JP 2-01, *Joint and National Intelligence Support to Military Operations (First Draft)*, expands OP 2.4.2.2, "General Military Intelligence Requirements," to include:[86]

- Adversary training, doctrine, leadership, experience, morale of forces, state of readiness, and will to fight
- Adversary's strengths and weaknesses, force composition, location, and disposition, including command, control, communications, computers, and intelligence, logistics and sustainment, force readiness and mobilization capabilities
- Basic infrastructure (power, resources, health, population centers and public institutions)
- Hydrographic and geographic intelligence, including urban areas, coasts and landing beaches, troop landing zones, and geological intelligence
- Capability and availability of all transportation modes in the operational area
- Military materiel production and support industries
- Military economics, including foreign military assistance
- Insurgency and terrorism
- Military-political and/or sociological intelligence
- Location, identification, and description of military-related installations
- Survival, escape, resistance, and evasion from government control

It lists an additional 32 pages of specific intelligence requirements.[87]

---

[85]Joint Chiefs of Staff, *Joint Publication 2-0*, p. II-2.

[86]Joint Chiefs of Staff, *Joint Publication 2-01. Joint and National Intelligence Support to Military Operations (First Draft)* (Washington, DC: GPO, 19 July 2002), III-72

[87]Ibid., Annex C (p. c-1 to c-32).

JP 2-01 further establishes the requirement for anticipatory intelligence focused upon the specific requirements of the CJTF and subordinate units and commanders.[88] It goes on to set a time standard for support to the joint commander: "Proper situation development demands that staffs be able to provide immediate advice (within approximately 12 hours) to commanders based on deliberate planning."[89]

Army Intelligence Support Requirements – Field Manual 3-0 *Operations*

Army Field Manual 3-0, *Operations* establishes intelligence support as the foundation for effective planning and execution of military operations: "Intelligence provides critical support to all operations, including Information operations. It supports planning, decision making, target development, targeting, and protecting the force."[90] This establishes the formal linkage to operations. As noted below, it goes on to set the standards for intelligence support that will be used to support the assessment of the AIC.

Army Intelligence Support Requirements – Field Manual 2-0, Intelligence

FM 2.0, *Intelligence*, establishes the basic framework for intelligence support within the Army. Moreover, it provides additional detail as to the GMI required to support Army requirements.

Intelligence Preparation of the Battlefield (IPB) is the doctrinal process for describing the environment for the commander in support of mission analysis and execution. FM 2.0 categorizes the aspects of the operating environment as such:

[88]Ibid., p. IV-1.

[89]Ibid., IV-9.

[90]U.S. Department of the Army, *Field Manual 3-0. Operations,* (Washington, D.C.: GPO. June 2001), 11-8.

CRITICAL VARIABLES OF THE OPERATIONAL ENVIRONMENT[91]	
• Nature and Stability of the State • Regional and Global Relationships • Economics • Demographics • Information • Physical Environment	• Technology • External Organizations • National Will • Time • Military Capabilities

These clearly encompass the categories of GMI established in JP 2.01 above and show the linkage between Joint and Army requirements.

Within this framework, the variables can be further distilled into specific categories of information. While all not exhaustive, the following composite tasks provide the basics necessary for the conduct of operations, with the possible exception of targeting.

TASK	Standard
Describe the Order of Battle: - Conventional - Unconventional - Political	Ability to develop composition & disposition of: - key forces and weapons systems, to include precision fires and WMD systems, to company-level resolution.[92] - key unconventional forces and weapons systems, to include WMD systems. Emphasis is on identifying terrorists, guerillas, and other militarily significant threats that can affect the disposition or employment of forces within 96 hours of force entry.[93] - national, regional, and local political environment, to include: key formal and informal leaders, security force leadership, pertinent local and regional policy issues, expected level of cooperation/resistance, and interactions within and between different government organizations, political parties, and informal leadership/groups.

[91]U.S. Department of the Army, *Field Manual 2-0,,* 1-8.

[92]Assuming a brigade-sized OF will not be available until 96 hours, platoon-level enemy composition/disposition is the minimum requirement to support the initial battalion-sized deployment.

[93]The 96 hour threshold is when the OF will achieve minimum self- sustaining combat power and should presumably be capable of detecting and mitigating the unconventional threats.

TASK	Standard
Describe the Physical and Information Infrastructure	Ability to characterize and classify key physical infrastructure systems, capabilities, and capacities; to describe the formal and informal communications network, to include the physical communications infrastructure, key media outlets and their respective markets, key opinion-leaders and their respective markets, and local-to-international information interaction. Includes the ability to predict the effects of direct attack and to manage BDA and secondary/tertiary affects of operations against the infrastructure.
Describe the Population, Demographics, Culture, and Religion	Ability to identify, locate, and characterize the ethnic, religious, and clan/tribal structures in the area of operations, to include: leaders (who and where), policies/attitudes towards US policies and involvement, expected level of cooperation/resistance, and interactions within/between different groups. Specifically identify those groups that directly and immediately oppose US operations in the AOR and have the capability to affect action. Additionally, describe the cultural and social environment, to include mores, values, customs, and practices that may affect inter-personal contact and policy development for commanders and soldiers on the ground.[94]
Describe the Refugee/Displace Persons & International NGOs/PVOs	Ability to identify current and projected displaced civilians within the AOR, to include: size, political and social relationship with the adversary and towards the US, medical and humanitarian aid requirements, and original homeland. Additionally, to identify which NGOs/PVOs are operating within the AOR capabilities, requirements, limitations, policies towards the population with the AOR, policies towards US military operations, key local leadership, and locations.
Describe the Economic Structure	Ability to describe local and then regional economic patterns and requirements, to include: key industries, sources of wealth and economic influence, daily economic patterns (e.g.: marketing times, sources of goods, services, and basic food items), black market structure (including leadership, controlling groups, and locations).

[94]Kirk, 2-4.

Intelligence Support Standards

Given these tasks, Army Field Manual 3.0, *Operations*, provides the evaluation criteria, or conditions and standards, for the AIC support[95] As intelligence supports the commander's planning and execution of operations, it is appropriate to draw the definition of success – the standards – from an operational manual of the operational community.[96]

- **Accuracy**. The information conveys the actual situation; in short, it is fact.
- **Timeliness**. The information has not been overtaken by events.[97] Intelligence must be available when the commander requires it. Late intelligence is of no value in informing current and future operations.
- **Usability**. The information is easily understood or displayed in a format that immediately conveys the meaning. Additionally, it must be relevant and tailored to the specific needs of the commander. This necessitates that the producer must understand the command's requirements and operating environment.
- **Completeness**. The information contains all required components *to sustain operations for 96 hours.*[98] It must answer the stated and most likely future questions to the fullest degree possible. It must be predictive and anticipatory of both the friendly and adversary actions.
- **Precision**. The information has the required level of detail, no more and no less.
- **Reliability.** The information is trustworthy, uncorrupted, and undistorted**.** Intelligence must be free from political or other constraints, preconceptions, or policy directives.

Each standard is situation-specific and difficult to quantify. Commanders' assessments and after action reviews will serve to determine whether the conduct of these five tasks met these requirements.

---

[95]U.S. Department of the Army, *Field Manual 3-0*, 11-13.

[96]Expanded definitions drawn from: Barrett Peavie, Major, *Intelligence Sharing in Bosnia*, (Fort Leavenworth, KS: School for Advanced Military Science, 4 September 2001), 34-38.

[97]If the timeliness requirement of the case study is tighter than the OF's projected timeline, then a 48-hour requirement will be applied. This will be done because, arguably, given that intelligence is necessary *before* deployment to better package the force and prepare the soldiers, the requirement for adequate intelligence is shorter than the 96-hour employment requirement cited in the Objective Force White Paper. The more stringent condition attempts to enable the commanders to plan effectively operations and force structure in a timely manner.

[98]The standard must be modified to reflect OF requirements. The AIC must be able to provide the requisite information to support uninterrupted OF operations for 96 hours. This period conforms to the closure of the initial employment package - the period of maximum risk and least flexibility. Moreover, the initial force will develop information in support of the larger OF employment, beginning the process of achieving AOR-wide SU. Once follow-on forces enter the AOR, there is generally enough flexibility to adjust the force flow, structure, and scheme of maneuver to correct to any lingering intelligence shortfalls.

Intelligence Support Conditions

The Joint and Army Doctrine provides some guidance on the general conditions that apply to the AIC's task for intelligence support. These are summarized as:

- Maintain a baseline intelligence *prior to* crisis action planning
- Provide operational-level intelligence in support of planning within twelve hours of crisis action planning initiation[99]
- Once deployed/employed, provide near-real time intelligence for the AOR, within 5 minutes of occurrence.

However, in addition to these general conditions, the Objective Force Concept of Operations presents a significantly different operating environment:

> "The Army goal is to deploy a brigade combat team anywhere in the world in 96 hours after liftoff, a division on the ground in 120 hours, and five divisions in theater in 30 days. This will drive system and capability parameters."[100]

> ….The situational understanding required to support operational maneuver from strategic distances begins at home stations and continues throughout deployment, including during operations required to establish assure access. *The goal is to establish entry conditions and sufficient knowledge base to insure that strategic maneuver is not executed as a strategic meeting engagement, but as a deliberate introduction of force packages tailored and ready for immediate operations*. [emphasis added][101]

Executing immediate ground combat operations as an integral element of initial deployment generates intelligence requirements that are far more detailed and complex than in traditional operations.

This CONOP leads to two additional basic conditions that are unique for OF intelligence support: time and lack of access. While some elements of the legacy force frequently work within these same constraints (Special Forces and elements of the 18th Airborne Corps, for example), they may be considered unique to OF because they will apply to the entire OF.

---

[99]The specific twelve-hour standard for OP 2.4, Produce Operational Intelligence and Prepare Intelligence Products is drawn from Joint Chiefs of Staff, *Joint Publication 2-01*, p. IV-9.

[100]U.S. Department of the Army, *"U.S. Army White Paper: Concepts for the Objective Force*," 9; reconfirmed in *Training and Doctrine Command, Pamphlet 525-3-93 (or 100 – pending final titling),* p. 22.

[101]U.S. Army Training and Doctrine Command, *Pamphlet 525-3-93* , 23-24.

- **Strategic Responsiveness**: Gain situational understanding in less than H-48 hours.[102] In crisis operations, time and space initially favor the aggressor. Rapid strategic response allows the Joint Force Commander to neutralize this advantage early, allowing the force to seize the initiative and transition from the defense to the offensive quickly. This requires sufficient information to build and employ force packages precisely from the beginning of operations to seize the initiative from the enemy. It imposes a strict time constraint on the tasks assigned to the AIC to provide the CDR the requisite SU.[103]

- **Limited AOR Access**. Aside from certain, limited national, strategic capabilities, the OF must be capable of entering an area of responsibility without a significant advance force to develop situation awareness. The Joint Commander must be able to conduct operations upon arrival, with no gaps or operational pauses between early entry and follow-on forces.[104] Therefore, the AIC must develop SU without an operational pause for deploying (operational and tactical level) collection capabilities into the AOR prior to initial force employment.[105]

Thus, the OF modifies the conditions that will be applied to the AIC in Chapter 3 to the following:

- Maintain a baseline intelligence *prior to* crisis action planning, *without a surge in collection and analytic capabilities in the prospective AOR*
- Provide operational-level intelligence in support of planning within twelve hours of crisis action planning initiation[106] *and tactical-level intelligence for planning and operations within 48 hours.*
- Once deployed/employed, provide near-real time intelligence for the AOR, within 5 minutes of occurrence.

Summary

As criteria for evaluating performance, the assessment mechanism is clear – historically, has the AIC provide sufficient intelligence to support the first 96 hours of combat operations? Will it be able to do so in the future? Doctrine provides the tools for answering these questions.

---

[102] As noted previously, given that intelligence is necessary *before* deployment to better package the force and prepare the soldiers, the requirement for adequate intelligence is shorter than the 96-hour employment requirement cited in the Objective Force White Paper. The more stringent condition attempts to enable the commanders to plan effectively operations and force structure in a timely manner.

[103] U.S. Department of the Army, *"U.S. Army White Paper: Concepts for the Objective Force*," 9; reconfirmed in U.S. Army Training and Doctrine Command, *Pamphlet 525-3-93 (or 100 – pending final titling),* 17.

[104] U.S. Department of the Army, Training and Doctrine Command, Pamphlet *525-3-93 (or 100 – pending final titling),* 17.

[105] This is a particular challenge given that the most critical information can frequently only be gained by a sustained HUMINT presence in the AOR.

[106] The specific twelve-hour standard for OP 2.4, Produce Operational Intelligence and Prepare Intelligence Products is an interpolation of requirements based upon the planning cycle and operational experience. The UJTL does not provide specific criteria.

All of the components and elements of the AIC's mission to provide intelligence can be distilled down to the five specific tasks. Their value – the standards of success – are rightly drawn from the Operations Community in FM 3.0, rather than the Intelligence Community in the FM 2.x series, as the commander and the deployed forces are the critical consumer. Finally, the conditions imposed for providing the intelligence to standard are also drawn from operational requirements. The result is a simple structure to determine if the AIC has been successful in meeting its mission – were the ground commanders able to effectively conduct offensive, defensive, stability, and support operations upon initial deployment into theater. If not, which task(s) were not completed to standard and required a substantial change to operations, the operational tempo, and/or force structure to make up for the intelligence shortfall?

However, the assessment that follows in Chapter 3 is only a tool to identifying where and why the AIC has shortfalls. In drawing the conclusions that follow, the intent is to show a pattern that leads to identifying structural and doctrinal shortcomings in how the AIC prepares for contingency operations. The ultimate goal is to identify these systemic causes and recommend solutions.

Appendix B:

National Intelligence Community

There are many organizations within the intelligence community that support military operations by providing specific intelligence products and services. The J2/G2/S2 and his staff must be familiar with these organizations and the methods of obtaining information from them as necessary. The following is a detailed review of the organizations identified in Figure 1: National Intelligence Community, noted on page 11. All information is drawn from Joint Publication 2.02, *National Intelligence Support to Joint Operations.*[107]

DOD Agencies

- **Defense Intelligence Agency (DIA).** DIA is a combat support agency and a major collector and producer in the defense intelligence community. The DIA's support flows across full spectrum operations to include counterterrorism, counterdrug, medical intelligence, WMD and proliferation, UN peacekeeping and coalition support, missile and space intelligence, noncombatant evacuation operations (NEOs), targeting, and BDA.

- **National Security Agency (NSA).** NSA ensures cryptologic planning and support for joint operations. Working with the tactical cryptologic units of a command, NSA provides SIGINT and information security (INFOSEC), encompassing communications security (COMSEC) and computer security, as well as telecommunications support and OPSEC. The people and equipment providing SIGINT, INFOSEC, and OPSEC constitute the United States

- **Cryptologic System (USCS).** The NSA, through the USCS, fulfills cryptologic command and/or management, readiness, and operational responsibilities in support of military operations according to the Secretary of Defense tasking, priorities, and standards of timeliness.

- **National Imagery and Mapping Agency (NIMA).** NIMA's mission is to provide timely, relevant, and accurate intelligence and geospatial information in support of national security objectives of the United States. The Director of NIMA advises the Secretary of Defense, Director Central Intelligence (DCI), Chairman of the Joint Chiefs of Staff (JCS), and the combatant commanders on imagery, IMINT, and geospatial information. The Operations Directorate, Customer Support Office, is the focal point for interface with external customers, including the JCS, combatant commands, services, and national and defense agencies.

- **National Reconnaissance Office (NRO).** The mission of the NRO is to enhance US government and military information superiority across full spectrum operations. NRO

[107] Joint Chiefs of Staff, *Joint Publication 2-02, National Intelligence Support to Joint Operations.* (Washington, DC: GPO, 28 September 1998), II-3 to V-1.

responsibilities include supporting I&W, monitoring arms control agreements, and performing crisis support to the planning and conduct of military operations. The NRO accomplishes its mission by building and operating IMINT and SIGINT reconnaissance satellites and associated communications systems.

- **US Navy (USN).** Naval intelligence products and services support the operating forces, the Department of the Navy, and the maritime intelligence requirements of national level agencies. Naval intelligence responsibilities include maritime intelligence on global merchant affairs, counter-narcotics, fishing issues, ocean dumping of radioactive waste, technology transfer, counter-proliferation, cryptologic related functions, criminal investigations and CI, I&W support, management of Coast Guard collection, and development of new weapons systems and countermeasures.

- **US Marine Corps (USMC).** USMC intelligence provides pre-deployment training and force contingency planning for requirements that are not satisfied by theater, other service, or national capabilities. The Marine Corps Intelligence Agency (MCIA) handles the integration, development, and application of general military intelligence (GMI), technical information, all-source production, and open-source materials.

- **US Air Force (USAF).** USAF ISR fill a variety of roles to meet US national security requirements. The USAF operates worldwide ground sites and an array of airborne R&S platforms to meet national level intelligence requirements. To support day-to-day USAF operations and to meet specific USAF requirements, intelligence professionals at the wing and squadron levels use suites of interoperable analysis tools and dissemination systems to tailor information received from all levels and agencies in the Intelligence Community. USAF responsibilities include all-source information on aerospace systems and potential adversaries' capabilities and intentions, cryptologic operations, I&W, IO, and criminal investigative and CI services.

Non-DOD Agencies

The primary focus of non-DOD members of the Intelligence Community is strategic intelligence and support to the President and the Secretary of Defense. This responsibility includes assessing potential issues and situations that could impact US national security interests and objectives. These agencies identify global and regional issues and threats. Some of the intelligence products and services these agencies provide are essential to accurate assessment of the threat and environment, particularly during stability operations and support operations.

- **Central Intelligence Agency (CIA).** The CIA's primary areas of expertise are in HUMINT collection, imagery, all-source analysis, and the production of political and economic intelligence. CIA and military personnel staff the CIA's Office of Military Affairs (OMA). As the CIA's single point of contact for military support, OMA negotiates, coordinates, manages, and monitors all aspects of agency support for military operations. This support is a continuous process that the agency enhances or modifies to respond to a crisis or developing operation. Interaction between OMA and the DCI representatives to the Office of the Secretary of Defense (OSD), the

Joint Staff, and the combatant commands facilitates providing national level intelligence in support of joint operations, contingency and operation planning, and exercises.

- **Department of State, Bureau of Intelligence and Research.** The Bureau of Intelligence and Research coordinates programs for intelligence, analysis, and research and produces intelligence studies and current intelligence analyses essential to foreign policy determination and execution. Its Bureau of International Narcotics Matters develops, coordinates, and implements international narcotics control assistance activities. It is the principal point of contact and provides policy advice on international narcotics control matters for the Office of Management and Budget, the NSC, and the White House Office of National Drug Control Policy (ONDCP). The Bureau also oversees and coordinates the international narcotics control policies, programs, and activities of US agencies.

- **Department of Energy, Office of Nonproliferation and National Security**. The Office of Nonproliferation and National Security directs the development of the State Department's policy, plans, and procedures relating to arms control, nonproliferation, export controls, and safeguard activities. Additionally, this office is responsible for—

  - Managing the department's R&D program.
  - Verifying and monitoring arms implementation and compliance activities.
  - Providing threat assessments and support to headquarters and field offices.

- **Department of the Treasury.** The US Treasury Department's intelligence-related missions include producing and disseminating foreign intelligence relating to US economic policy and participating with the Department of State in the overt collection of general foreign economic information.

- **Federal Bureau of Investigation (FBI).** The FBI is the principal investigative arm of the Department of Justice (DOJ) and has primary responsibility for CI and counterterrorism operations conducted in the United States. CI operations contemplated by any other organizations in the United States must be coordinated with the FBI. Any overseas CI operation conducted by the FBI must be coordinated with the CIA.

Other Government Agencies

US Coast Guard (USCG). The USCG, subordinate to the Department of Transportation, has unique missions and responsibilities as both an armed force and a law enforcement agency (LEA), which makes it a significant player in several national security issues. The USCG intelligence program supports counterdrug operations, mass seaborne migration operations, alien migration interdiction operations, living marine resource enforcement, maritime intercept operations, port status and/or safety, counterterrorism, coastal and harbor defense operations, and marine safety and/or environmental protection.

Miscellaneous Agencies. There are a number of US Government agencies and organizations, not members of the Intelligence Community, that are responsible for gathering and maintaining information and statistics related to foreign governments and international affairs. Organizations such as the Library of Congress, the Departments of Agriculture and Commerce, the National Technical Information Center, US Information Agency, US Information Service, and the US Patent Office are potential sources of specialized information on political, economic, and military-related topics. The Intelligence Community may draw on these organizations to support and enhance research and analysis and for relevant, peripheral data and background information for planners and decision-makers. Many other US Government agencies may become directly involved in supporting DOD especially during stability operations and support operations. (See JP 2-02 for a description of agency support to joint operations and intelligence.) These organizations include—

- Department of Transportation.
- Disaster Assistance Response Team within the Office of Foreign Disaster.
- US Agency for International Development.
- Immigration and Naturalization Service.
- US Border Patrol
- Federal Emergency Management Agency (FEMA).