Intelligence Sharing in Bosnia

A Monograph
by
Major Barrett K. Peavie
United States Army

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

First Term AY 00-01

REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-01-2001	Monograph	xx-xx-2000 to xx-xx-2001

4. TITLE AND SUBTITLE Intelligence Sharing in Bosnia Unclassified	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Peavie, Barrett K. ;	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME AND ADDRESS USA Command & General Staff College School of Advanced Military Studies 1 Reynolds Ave. Fort Leavenworth , KS 66048	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS ,	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

A
PUBLIC RELEASE

,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

US participation in expeditionary operations after the end of the cold war, 1991,is indicative of a shift in national security strategy from containment to engagement. Participation is at best multinational, at its most challenging, coalition. Sharing intelligence in a coalition environment, especially a stability and support operation was a challenge by design. The intelligence systems used in Bosnia from 1995-1997 were developed for a different kind of conflict, for exploitation in a conventional war. The implementation of inoperable, stovepiped, technology was indicative of a mindset that prepared for unilateral operations as oppose to multinational stability operations. The NATO led Implementation Force IFOR, eventually became a 60,000 person, thirty-six- nation coalition force. The implementation force consisted of both Partnership for Peace nations as well as non-NATO countries. US intelligence sharing doctrine did not reflect the adjustments that professionals made on the ground to embrace the multinational composition of the division. This monograph examines intelligence sharing doctrine, practices, and challenges during Operation Joint Endeavor, the first out of area employment of NATO, particularly for the operational commander. The monograph shows how intelligence systems developed for the cold war are inadequate for the stability and support environment. Using intelligence principles for multinational operations it explores how effective the employment of intelligence sharing was in Bosnia from December 1995 to 1997. Sharing intelligence in a SASO environment is so inherently complex that cold war policies and systems adversely affect the quality of intelligence. This environment requires primacy of intelligence disciplines that were not the cold war focus. Bosnian conflict demanded synthesis of political, cultural, economic, ethnic, information, human intelligence (HUMINT), an intelligence discipline that the US Army arguably neglected during the cold war. Moreover, synchronization of intelligence efforts from nations that have different national agendas, capabilities, and procedures on intelligence sharing became the concern of operational level officers in the multinational divisions. Adding complication is an allied intelligence architecture where the US is not in charge, which shared intelligence based on a cold war mentality of need to know, as oppose to a tailored push methodology that use broadcast dissemination for visualizing the situation. Finally, the challenge of technical system interoperability increases with the demands of near real time accurate intelligence for operational decision-making. Given this environment, intelligence-sharing requirements across an ad hoc coalition still demand operational and foreign disclosure security. The dynamic tension between the intelligence battlefield operating system providing actionable near-real-time intelligence to commanders for coalition synchronization and the requirement to protect national sources and methods is untenable in stability and support operations. Operational commanders at the division level must resolve the tension that normally occurs at higher levels in conventional operations. Using the intelligence principles in current doctrine, the monograph makes recommendations for the resolution of this tension in the form of a mental model for intelligence sharing in stability operations. The principles and

model presented in the monograph together establish a point of departure for adapting to the demands of intelligence sharing in a coalition environment.

15. SUBJECT TERMS
Operation Joint Endeavor; intelligence sharing; Bosnia; doctrine; IFOR; multinational operations

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
			Same as Report (SAR)	54	Burgess, Ed burgesse@leavenworth.army.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 913 758-3171 DSN 585-3171

Abstract

INTELLIGENCE SHARING IN BOSNIA by MAJ Barrett K. Peavie, US Army, 50 pages.

US participation in expeditionary operations after the end of the cold war, 1991,is indicative of a shift in national security strategy from containment to engagement. Participation is at best multinational, at its most challenging, coalition. Sharing intelligence in a coalition environment, especially a stability and support operation was a challenge by design. The intelligence systems used in Bosnia from 1995-1997 were developed for a different kind of conflict, for exploitation in a conventional war. The implementation of inoperable, stovepiped, technology was indicative of a mindset that prepared for unilateral operations as oppose to multinational stability operations.

The NATO led Implementation Force IFOR, eventually became a 60,000 person, thirty-six-nation coalition force. The implementation force consisted of both Partnership for Peace nations as well as non-NATO countries. US intelligence sharing doctrine did not reflect the adjustments that professionals made on the ground to embrace the multinational composition of the division.

This monograph examines intelligence sharing doctrine, practices, and challenges during *Operation Joint Endeavor*, the first out of area employment of NATO, particularly for the operational commander. The monograph shows how intelligence systems developed for the cold war are inadequate for the stability and support environment. Using intelligence principles for multinational operations it explores how effective the employment of intelligence sharing was in Bosnia from December 1995 to 1997. Sharing intelligence in a SASO environment is so inherently complex that cold war policies and systems adversely affect the quality of intelligence. This environment requires primacy of intelligence disciplines that were not the cold war focus. Bosnian conflict demanded synthesis of political, cultural, economic, ethnic, information, human intelligence (HUMINT), an intelligence discipline that the US Army arguably neglected during the cold war. Moreover, synchronization of intelligence efforts from nations that have different national agendas, capabilities, and procedures on intelligence sharing became the concern of operational level officers in the multinational divisions. Adding complication is an allied intelligence architecture where the US is not in charge, which shared intelligence based on a cold war mentality of need to know, as oppose to a tailored push methodology that use broadcast dissemination for visualizing the situation. Finally, the challenge of technical system interoperability increases with the demands of near real time accurate intelligence for operational decision-making. Given this environment, intelligence-sharing requirements across an ad hoc coalition still demand operational and foreign disclosure security.

The dynamic tension between the intelligence battlefield operating system providing actionable near-real-time intelligence to commanders for coalition synchronization and the requirement to protect national sources and methods is untenable in stability and support operations. Operational commanders at the division level must resolve the tension that normally occurs at higher levels in conventional operations. Using the intelligence principles in current doctrine, the monograph makes recommendations for the resolution of this tension in the form of a mental model for intelligence sharing in stability operations.

The principles and model presented in the monograph together establish a point of departure for adapting to the demands of intelligence sharing in a coalition environment.

TABLE OF CONTENTS

CHAPTER ONE

I. INTRODUCTION

With the collapse of the Soviet Union in 1991 and the shift in US national security strategy from one of containment to engagement and enlargement, the US military participates in expeditionary operations around the world. In 1995, the North Atlantic Treaty Organization (NATO) and allied coalition partners established the NATO Implementation Force (IFOR) in Bosnia. IFOR was a 60,000-person, 36-nation coalition force. IFOR's operation, *Joint Endeavor*, represented the first time NATO has lead a coalition in a peace support operation with Partnership for Peace partners and other non-NATO countries. The coalition consisted of three multinational divisions with a corps headquarters represented by NATO's Allied Rapid Reaction Corps (ARRC). The US Army's 1st Armored Division formed the core of Multinational Division (North), MND(N), which is commonly known as Task Force Eagle in US historical documents. Understanding that intelligence is the oil that lubricates the operational engine, the paper examines flow of information in a multinational environment. This paper highlights why sharing intelligence in any multination stability and support operation (SASO) having U.S. participation is an operational problem.

This monograph examines intelligence sharing doctrine, practices, and challenges during *Operation Joint Endeavor*, the first out of area employment of NATO, particularly for the operational commander. In a broader sense, the monograph shows how intelligence systems developed for the cold war are inadequate for the stability and support environment. Using intelligence principles for multinational operations it explores how effective the employment of intelligence sharing was in Bosnia from December 1995 to December 1997.

The thesis presented here is that sharing intelligence in a stability and support coalition operation is so inherently complex that cold war policies and stovepipe systems; non-interoperable systems, adversely affect the quality of intelligence, which has a direct impact on

operational mission success. The dynamic tension between the intelligence battlefield operating system providing actionable near- real-time intelligence to commanders for coalition synchronization and the requirement to protect national sources and methods is untenable in stability and support operations. Operational commanders at the division level must resolve the dynamic tension that normally occurs at higher levels in conventional operations. The ability to perform this function requires a paradigm shift, based upon doctrine. Currently there is no single source doctrine for intelligence sharing. However, history indicates that coalition operations conducted in the SASO environment are both a present reality and a likely future probability.

This monograph validates the relevancy of intelligence principles concerning coalition dissemination practices. This chapter outlines the genesis of guidance for the operational intelligence officer and briefly examines the plethora of doctrinal sources that complicate intelligence sharing. Chapter II describes the Bosnian threat environment and exposes the inadequacy of stovepipe intelligence systems hardware for coalition sharing. Additionally this chapter describes the mental paradigm shift that must occur in doctrine and most importantly within the mind of the operational commander. Chapter III examines the ten principles used to test intelligence quality in the context of the US Army's latest international stability operation, the implementation, and stabilization forces in Bosnia Herzegovina 1995-1997. Using the principles, chapter IV makes recommendations for the resolution of dynamic tension in the form of a mental model for intelligence sharing in stability operations. It is beyond the scope of this paper to discuss the reasons why the United States might deploy military forces to resolve non-US social conflicts. The assumption is that the army will continue to be engaged in world affairs and coalition stability operations are apart of full spectrum operations. According to Force XX1 operations manuals, "The main imperative guiding future operations, from full war to domestic support operations, will be to gain information and continue accurate and timely shared

perceptions for the battles-pace."[1] However, the monograph explains why the dynamic tension is more pronounced in internal US stovepipe systems rather than external coalition sharing in terms of the US Army's intelligence battlefield operating systems ability to share information effectively in a stability and support environment.

Impact of Doctrine

US Army *Field Manual 100-5: Operations*, defines doctrine as "the fundamental principles by which the military forces guide their actions in support of national objectives."[2] As early as 1994 the US Army doctrine on intelligence sharing indicated that it might be inadequate for the types of operations post cold war. Superseding the 1990 manual, the *US Army FM 34-2, Collection Management and Synchronization Planning* published in 1994, provides the doctrinal framework for synchronizing the Intelligence System of Systems (ISOS). ISOS was architecture of procedures, organizations, and equipment that was designed to focus the intelligence effort, and to gain dissemination of intelligence for the right place and time for key decisions. Imbedded in ISOS was an understanding that collection and dissemination technologies provide commanders with an unprecedented capability to satisfy the command's intelligence requirements within timelines that support operational decisions. In spite of the published potential of ISOS, the doctrine acknowledges, "US units subordinated to non-US headquarters may face unique problems in disseminating intelligence."[3] The US Army's *Peace Operations FM 100-23* states "when conducting multinational operations, sharing information with allies may in itself become an issue."[4] The following year,

---

[1] Headquarters, U.S. Army Training and Doctrine Command, *Force XXI Operations*, TRADOC PAM 525-5 (Fort Monroe, VA: TRADOC), 1 August 1994, Chapter 3.
[2] U.S. Department of the Army *Field Manual 100-5: Operations* (Washington D.C., 1993), Glossary-3.

[3] U.S. Department of the Army *Field Manual 34-2, Collection Management and Synchronization Planning* (Washington D.C., 1994), 5-2.
[4] U.S. Department of the Army , *Peace Operations, Field Manual 100-23*; (Washington, DC, 30 December

1995, a year before U.S. implementation forces in Bosnia, the publication of joint doctrine for Intelligence Support to Operations, reveals a more complex challenge for the operational commander with the statement that, "There is no single intelligence doctrine for multinational operations. Each coalition or alliance must develop its own doctrine."[5] Recognizing as early as 1996 that a change needed to occur with policy, the director of the CIA, William Perry, issued a directive that changed basic security practices from a cold war model to coalition warfare in a stability and support operation.

> I am focusing on the needs of commanders at all levels in the armed forces. Coalition warfare is the future model for US military conflicts, and I want the Intelligence Community to rededicate itself to the concept of releasable tailored intelligence—intelligence produced at the lowest security level commensurate with the protection of sources and methods or produced in a format that allows for timely disclosure to US customers or foreign governments. From this point forward we must write for the consumer.[6]

Although this represents a major step towards change, during initial Bosnian operations in 1995 execution of intelligence sharing was not in accord with the new mandate. Methods to permit coalition sharing quickly like sanitation; the process of editing intelligence before dissemination and tear line procedures were not as common as restrictive control markings. The most restrictive intelligence control marking, ORCON, defined as information controlled by originator; hindered coalition sharing because dissemination beyond the initiating headquarters required advanced permission from the originator.

As of 1996, it was the operational commander's responsibility to establish a framework for the dissemination of intelligence information. This task is not without references.

> Among the multitude of references that either require the operational commander to accomplish intelligence disclosure or which tell him how to accomplish it are

---

1994), 45

[5] Joint Chiefs of Staff, *Joint Doctrine for Intelligence Support to Operations, Joint Pub 2-0,* (Washington, D.C.: 5 May 1995), VIII-1.

[6] Central Intelligence Agency, Director of Central Intelligence Directive 1/7, *Security Controls on the Dissemination of Intelligence Information* (Washington: 1996), www.fas.org/irp/offdocs/dcid17m.htm

> DCID 1/7, DCID 5/6, CJCS Instruction 5221.01, Executive Order 12968, Joint Warfighting Center Joint Task Force Commander's Handbook for Peace Operations, DoD Directive 5230-11, NDP-1, Joint Pub 2-0, Joint Pub 2-01, Joint Pub 3-07.1, Joint Pub 3-07.3, Joint Pub 3-16, Joint Pub 5-00.2, Field Manual 100-7, Field Manual 100-8, Field Manual 100-20, Field Manual 100-23, and Field Manual 34-2.[7]

This plethora of doctrinal guidance and policy, sometimes contradictory or at least confusing, regulates intelligence dissemination. Key among the policies are Director of Central Intelligence Directive (DCID) 5/6 and National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (also known as National Disclosure Policy or NDP-1).[8] The Collection Management and Synchronization Planning manual, FM 34-2, published in 1994, dedicates approximately a page to intelligence operations in a combined environment and states simply "a combined unit commander must establish a system that optimizes each nation's contributions and provides all units a high quality intelligence picture."[9] This concept is consistent with the intelligence sharing tenet of broadcast dissemination and shared situational awareness, which pushes intelligence products.

At the operational level of war, the joint and multinational intelligence system does not concentrate just on the collection, identification, location, and analysis of the center of gravity and operational objectives. It also must focus its production effort downward and concentrate

---

[7] George K. Gramer, Jr., "Optimizing Intelligence Sharing in a Coalition Environment", *Naval War College*, 1999. Author states that Joint Pub 5-00.2 identifies dissemination as a major challenge (VI-6). DODD 5230.11 enclosure 6 has an extensive security classification guide for the National Disclosure Policy that delineates subject matter and classification of over 17 subjects related to operational dissemination. Keeping in mind of the very ad hoc nature of coalitions: Joint Pub 2-0 referring to multinational operations states the "methodology for exchanging intelligence should be conceived and exercised well before operations begin" (VIII-4). Joint Pub 3.07.1 states that the "sharing of US intelligence is a sensitive area that must be evaluated based on the circumstances of each situation" (IV-21). Although not doctrine, the Joint Task Force Commander's Handbook for Peace Operations is a well-written concise companion for quick reference to doctrinal guidance on intelligence dissemination (with CD-ROM). The complete publication data on each is in the bibliography.

[8] National Disclosure Policy –1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*, according to DOD directive 5230.11, June 16, 1992, NDP-1 is provided to designated disclosure authorities on a need-to-know basis from the Office of the Director for International Security Programs, Office of the Deputy Under Secretary of Defense for Security Policy (ODUSD(SP).

[9] U.S. Department of the Army, *Collection Management and Synchronization Planning, Field Manual 34-2*; (Washington, DC, 8 March 1994), 5-2

efforts on war fighting priority intelligence requirements.[10] To add complexity to this focus FM 34-2, cautions the operator to make sure that compartmented information is not disseminated to users who are only authorized collateral information. Legal restrictions may also prohibit the dissemination of information to allied or coalition forces. This is especially true during operations other than war where political considerations may dominate collection operations.[11] The Task Force Eagle After Action Report summarizes the relevance of current doctrine: "None of the key field manuals (FM-3, FM 34-7, FM 34-130, or FM 100-23) addressed how to verify treaty compliance issues such as those laid out in the General Framework for the Agreement of Peace (GFAP)."[12]According to the division intelligence officer, G2, at the beginning of *Operation Joint Endeavor*, "Doctrine such as intelligence preparation of the battlefield (IPB) and indications and warning (I&W) were completely inadequate to the task at hand, and had to be modified and retailored by the forces in the field. Doctrine also failed to address adequately the multi-service, multi-agency, and multi-national nature of operations in a coalition environment."[13]

A finding from the Defense Science Board that was tasked to review intelligence in Bosnia claims that " the doctrine with respect to unit hierarchy in a coalition environment needs to be defined for the corps, division, and brigade levels."[14] Offering a different opinion, the chief of intelligence for the stabilization forces, COMSFOR, J2, in the second paragraph of his tour report states, "The peacekeeping mission does not require a radical change in the way we carry our intelligence support."[15] The research indicates that there is a difference of opinion regarding this issue. US joint doctrine calls for two categories of shared intelligence: Level 1, which can be

---

[10] U.S. Department of the Army, *Decisive Force: The Army in Theater Operations, Field Manual 100-7*, (Washington, DC, 31 May 1995), 5-17.

[11] *Collection Management and Synchronization Planning, Field Manual 34-2*;p. 3-22.
[12] Task Force Eagle, *Task Force Eagle, 28 Dec 95-10 Nov 96: After Action Report*. (Unpublished manuscript dated 1 June 1997 in the U.S. Army War College Library, Carlisle Barracks, PA), III-20.
[13] Melissa E Patrick,. *Intelligence in Support of Peace Operations*, 2.
[14] Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield: May-July 1996*," Office of the Under Secretary of Defense for Acquisition and Technology, Washington, D.C. p 16.
[15] Hammond, John C., MEMORANDUM FOR THE COMSFOR: SFOR Tour Report, 4 December 1996-26 September 1997. Article located on LTC Rich Holden's "Standard Intel Data Dump" CD as of 16

shown to but not retained by coalition and United Nations forces and level 2, which has been properly cleared for release to coalition and U.N. forces.[16] It further states, "The methodology for exchanging intelligence should be conceived and exercised well before operations begin."[17] Obviously, by the defining coalitions as an ad hoc operation brought together for a temporary mission; complying with joint doctrine is unrealistic. The following example illustrates. LTC Colin Agee, former military intelligence officer in USAREUR, comments on the complexity of on the foreign release of Joint Surveillance Target Attack Radar System, JSTARS,-produced intelligence (electronic intelligence information at the Secret level). Early verbal guidance from the JSTARS Squadron to the Ground Support Module crews was consistent with Level 1: they could permit their NATO partners to view data on their screens, but were prohibited from providing hard copies, which reduced the utility of the product. The original written guidance in December 1995, promulgated by the U.S. Air Fore's Disclosure Policy Branch, was ambiguous. EUCOM did not publish definitive guidance until mid-February, a month and a half after initial operating capability was declared. In the absence of such guidance, elements at British, French, and multinational headquarters had to make their own, localized decisions on releasability.[18] These differences fracture unity of effort, synchronization of intelligence capability and optimization of limited resources.

For the scope of this paper, it is important to clarify common terms relating to operational intelligence dissemination. According to doctrine, operational intelligence is that intelligence required for the planning and conduct of major operations within a theater of operations. Disclosure is showing or revealing classified intelligence, whether orally, in writing or any other medium, without providing the recipient with a copy of such information for retention. Release provides the recipient of classified information with a copy, whether in writing or any other

---

March 2000
[16] Joint Chiefs of Staff, *Joint Doctrine for Intelligence Support to Operations (Joint Pub 2-0)*, VIII-1
[17] Ibid., VIII-4.
[18] Agee, Collin A., "Joint STARS in Bosnia: Too Much Data Too Little Intel?," *Military Intelligence*

medium, of such information for retention. Sharing defines activities involving the disclosure or release of intelligence.[19]

The Army's premier field manual on operational art in 1995 states that "the timely dissemination of usable and pertinent intelligence is the most important intelligence problem that must be solved on the battlefield."[20] The author contends that, LTC Melissa Patrick, former G2 for MND (N) characterized the impact of operational intelligence doctrine in Bosnia best; "Task Force Eagle analysts succeeded largely by setting aside the doctrine and applying innovative approaches that they dreamed up."[21]Perhaps that is the best that doctrine can provide, an initial foundation to approach operational challenges as oppose to a prescriptive litany of task list to solve problems in every environment.

In conclusion, the U.S. Army is a doctrine-driven institution. In Bosnia, U.S. Army doctrines were largely inadequate in an environment that forced American commanders to contend with the information, political, diplomatic, and military intelligence demands of stability operations. "Almost from the inception of the IFOR operation, U.S. commanders found themselves in uncharted territory. Describing this challenge, Major General William Nash[22] noted that this was an inner ear problem. Having trained thirty years to read a battlefield, Nash observed that the general officers were now asked to read a 'peace field."[23]

Chapter II examines this threat environment and highlights three major challenges, command and control/intelligence structure, the cold war mindset, and technological interoperability in Bosnia. It is key to understanding why doctrine failed and human ingenuity and flexibility

---

Professional Bulletin,(Fort Huachuca, AZ, October-December 1996), .8.

[19] Central Intelligence Agency, Director of Central Intelligence Directive 5/6, *Intelligence Disclosure Policy* (Washington D.C.: 1998), paragraph 5.

[20] *Decisive Force: The Army in Theater Operations*, *Field Manual 100-7*, 5-19.

[21] Melissa E Patrick., *Intelligence in Support of Peace Operations*, 23.

[22] Maj. Gen. William Nash was the first commanding general of Multi-National Division North/Task Force Eagle in Bosnia. This division was one of three divisions that comprised the NATO Implementation force that went into Bosnia in 1995 as part of the Dayton Peace Accords.

[23] Howard Olsen, and John Davis, "Training U.S. Army Officers for Peace Operations: Lessons from Bosnia", *United States Institute of Peace Special Report*, www.usip.org/oc/sr991029nb.html

attempted to circumvent its shortcomings. It highlights some of the U.S. Army's internal problems associated with cold war intelligence systems that hindered effective coalition sharing. The intelligence challenge is overcoming US stovepiped technology, beset by a unilateral mindset in a multinational environment

CHAPTER TWO

II. ENVIRONMENT AND OPERATIONAL CHALLENGES

This chapter analyzes the environment of intelligence in *Operation Joint Endeavor* and within a broader context provides the reader with an awareness of the complexity that is inherent with intelligence sharing in a SASO operation. The U.S. Army *FM 100-23* states, "Peace operations take place in environments less well-defined than war…the traditional elements of combat power may not apply…the needs of the commander involved in peace operations are in some ways more complex than those of the commander conducting combat operations."[24] Increasing complexity of the environment has led to increasing specialization that has led to increasing demands for information at all levels. This spawns new organizations and expands old ones to satisfy the demand for information, which in turn creates still more demand which in its turn creates more complexity and so on.[25] Subsequent chapters will use this environment to explore the effectiveness of intelligence sharing. Before this exploration, it is prudent to appreciate the demands that the recent ethnic history places on the intelligence system.

Background

Bosnia-Herzegovina has a long and turbulent history.[26] Originally part of the Roman

[24]*Peace Operations, Field Manual 100-23,* p. v.
[25]Martin L.Van Creveld, *Command in War,(*Cambridge, Harvard University Press, 1985), 258. See Frank Kitson, *Warfare as a Whole*, (London, Faber and Faber Limited, 1987), p 65 for more information on complexity and the expanded requirements of intelligence and risk incurred in the British Army during peace-keeping operations.
[26] Noel Malcolm, *Kosovo: A Short History*, (New York, Haper Collins) 1999. xvii compares and contrast the historical relevance of 'ethnic hatred' in Bosnia and Kosovo. Author argues that the conflict is more about differing views on national origin as oppose to religion and culture. For a regional discussion in a travel-guide style on ethnicity and cultural hatred see Robert Kaplan's *Balkan Ghosts: A Journey Through*

Empire, the area was conquered by the Ottoman Turks and administered by the Austro-Hungarian Empire. These historical events are largely responsible for the Bosnians, Serbs, and Croats adopting different religions and developing distinct cultural backgrounds. When Yugoslavia disintegrated in June 1991, Serb Republic president Slobodan Miloshevich tried to consolidate Serb territory. A civil war erupted. During the next four years, the warring factions committed numerous human rights violations. This included mass killings and murder, systematic rape, torture and other heinous crimes against humanity. In October 1995, the warring factions agreed to a ceasefire. Three months later, December 1995, the presidents of Bosnia, Croatia and Serbia signed the Dayton Peace Accords (DPA) in Paris, France.[27] The agreement was designed to stop the warring factions from fighting, return people to their pre-war homes, and rebuild Bosnia's infrastructure: in short, to create a self-sustaining peace in a multiethnic Bosnia. Although the fighting subsided, the former warring factions continued to mount aggressive information campaigns using disinformation, distorted or incomplete reporting, manipulation of national and international media, public statements and accusations, intimidation and orchestrated media events.[28] Former Secretary of Defense William J. Perry said, "Bosnia may very well be the toughest security policy issue we face today. Under Tito it was said that Yugoslavia consisted of seven neighbors, six republics, five nations, four languages, three religions, two alphabets and one country."[29] This assessment emphasizes the complexity of the environment. According to

---

History, (New York Saint Martin's Press) 1993, 22. See also Christopher Merrill, *Only the Nails Remain: Scenes from the Balkan Wars*,(New York, Rowman & Litttlefield) 1999, 105-353, for a vivid characterization of the regional culture and war atrocities from 1993-1996.

[27] For a detailed account into negotiations leading to the DPA and the force structure of IFOR see Richard Holbrooke, *To End a War*, (New York Random House) 1998, 310-324, 203. Critical commentary on the U.S diplomatic response to the conflict is in David Rieff, *Slaughterhouse: Bosnia and the Failure of the We*st, (New York, Simon & Schuster) 1995, 1-29 and Stjepan G. Mestrovic, *The Conceit of Innocence: Losing the Conscience of the West in the War against Bosnia* (Texas A&M University Press College Station) 1997. For a full discussion of the impact of the DPA since implementation see *Bosnia Peace Operation: Crime and Corruption Threaten successful Implementation of the Dayton Peace Agreement* (GAO/NSIAD-00-156, July 2000).

[28] , Stephen W. Shanahan, "Information Operations in Bosnia", *Military Review*, (November-December 1997), 55-57.

[29] U.S. Department of State. Bosnia Fact Sheet: *Human Rights Abuses in the Balkans*, updated and released by the Bureau of Public Affairs, 11 December 1995.

Steven L. Burg and Paul Shoup authors of one of the most detailed historical accounts of the conflict states:

> The conflict in Bosnia-Herzegovina was the first major test in the post-Cold War period of the ability of the international community to resolve ethnic conflicts. These efforts failed to prevent a catastrophic war or to establish the conditions for a stable peace once the war was ended. As a result, Bosnia remained haunted by the contradiction between integration and partition. [30]

Maj. Gen. Robert Grange, commander of MND-N during the initial stabilization phase and his intelligence officer, LTC John Roveno, describe the Bosnian environment in an unpublished article entitled "Shaping the Environment" as not one conflict but many that are linked to both the past and the present war. The authors continue to present the main threats to the people of Bosnia-Herzegovina as non-compliant military, paramilitary, corrupt police, criminal elements, extremist groups, and political hard-liners. In order to respond effectively:

> The military forces must shape the environment into one that favors the peaceful implementation of the General Framework Agreement for Peace (GFAP) by identifying and disrupting linkages between crime, terrorism black marketing, and disinformation currently used by those in power who prefer the status quo. Shaping such a complex environment requires a well orchestrated campaign using a wide range of collections systems, followed by synchronized operations with the right mix of military, political and informational {intelligence} assets.[31]

This is important for recognizing that in order to set conditions for the successful implementation of the Dayton Peace Accords (DPA), and protect forces, the intelligence preparation of the environment requires significant adjustment. Given this environment, the following paragraph explores the effectiveness of coalition intelligence sharing from military intelligence professionals in Bosnia during *Operation Joint Endeavor.*

A key finding from an *Operation Joint Endeavor* after action report supports the theory

---

[30] Steven L Burg and Paul S. Shoup, *The War in Bosnia Herzegovina, Ethnic Conflict and International Intervention*, (M.E. Sharpe Armonk, New York, 2000), 388. For more information on partition theory see Radha Kumar, *Divide and Fall?: Bosnia in the Annals of Partition*, (London, Verso) 1997, esp101-135.

[31] David L. Grange, and John S. Rovegno, "Shaping The Environment", unpublished article submitted to *Joint Forces Quarterly*, 1997.Article located on LTC Rich Holden's "Standard Intel Data Dump" CD as of 16 March 2000.

that intelligence is one of the hardest things to share in a coalition environment. Moreover, it asserts that "each partner, no matter how dedicated to the general cause, has a natural tendency to mask his intelligence capabilities and to retain control of what tasks he performs and how his products are disseminated".[32] "*Joint Endeavor* is remarkable in the degree to which the various coalition members were willing to cooperate. Even so, there was some confusion as to roles and responsibilities and some duplication of effort, and each nation chose to follow its own disclosure rules."[33] According to LTC Melissa Patrick, former MND (N) intelligence officer, "there were two imperatives for maximizing a multinational intelligence operating system; developing a fully integrated and interoperable intelligence architecture and resolving issues of releasibility."[34] The preponderance of the evidence in the following paragraphs highlight three areas that this monograph found that had a significant impact on sharing intelligence; command structure, a cold war mindset for intelligence and technological interoperability. Even the emerging operational doctrine acknowledges the intelligence challenge; "The complexity of the operational environment requires intelligence that is shared (pushed and pulled up and down) from the national level to the tactical level".[35] This is an important distinction because it reemphasizes the mandate that the director of the CIA, William Perry, issued in response to intelligence operations in Bosnia in 1995. The structure for intelligence operations is the framework for the integration, and synchronization of coalition information sharing. The following section explores the impact of both the command and intelligence structure on the operational intelligence task of dissemination.

---

[32] Wentz, Larry K. "Intelligence Operations," in *Lessons from Bosnia: The IFOR Experience*, 53.
[33] USAREUR Headquarters Operation Joint Endeavor After Action Report, Volume1 May 1997, xiv.
[34] Melissa E. Patrick. *Intelligence in Support of Peace Operations*, 24.
[35] U.S. Army Training and Doctrine Command, "*Operations (DRAG Edition) Field Manual 3-0*," Fort Leavenworth, 15 June 2000, 11-7.

Command & Control / Intelligence Structure

Historically, the most contentious aspect of coalition operations is command and control according to Colonel Anthony Rice of the United Kingdom.[36] Emphasizing this fault line, lessons learned editor, Larry Wentz, states "the coalition intelligence environment caused problems for U.S. forces when the U.S. was not in charge".[37] Allies often had a different scheme for utilization of intelligence, and have their own methods for it. On 20 December 1995, a NATO-led multinational forced called the Implementation Force (IFOR) started Operation Joint Endeavor. IFOR was mandated by the United Nations Security Council Resolution 1031 to help ensure compliance with the military provisions of the Dayton Peace Accords. "Eager to avoid the command problems that crippled the UN effort between 1991 and 1995, NATO insisted that IFOR have a unified command structure."[38] On 20 December 1995, most of the forces assigned to IFOR were placed under the operational control (OPCON) of Supreme Allied Command Europe (SACEUR), General George Joulwan, USA. The principle of unified command also applied to 17 of the 18 non-NATO countries (mostly members of the Partnership For Peace, PFP) who chose to participate in the IFOR operations. All non-NATO forces but Russia were incorporated into the unified command structure alongside NATO forces, under the command of the IFOR Commander and his multinational divisional commanders.

Background

The command and control arrangement, illustrated in appendix B, with multinational divisions subordinated directly to a NATO corps headquarters represented a departure from previous NATO doctrine and operating procedures. The ARRC was a relatively new

---

[36] Anthony J. Rice, "Command and Control: The Essence of Coalition Warfare," *Parameters*, (Spring 1997): 152-167. For more see Martha E Maurer, *Coalition Command and Control: Key Considerations*, Washington D.C. National Defense University Institute for National Strategic Studies 1996.

[37] Larry K Wentz, "Intelligence Operations", 117.

[38] Pascale Combelles Siege, *Target Bosnia, Integrating Information Activities in Peace Operations*, 26.

headquarters. Before its activation in 1993, divisions in NATO were national formations subordinated to corps of their own nation. Under that system, dissemination issues were not a factor at the division level and division staffs were not expected to deal with them, nor were they prepared to do so. Furthermore, NATO and US doctrine regarded intelligence as a national responsibility, with reporting chains going through national channels. The lowest level at which national intelligence pipes could be expected to terminate was at corps or even army level. Not surprising, "establishing trust and confidence, especially between the strategic level headquarters in Belgium and the operational level (IFOR HQ) was a challenge"[39] This challenge resulted despite the dual intelligence structure designed to circumvent friction imposed by multinational composition.

Intelligence support was shaped along two architectural lines: one NATO: the other for U.S. forces. "Well established alliances have tended to gravitate more toward one of the integrated command structures; for example, NATO's Allied Rapid Reaction Corps (ARRC) uses an integrated command structure with force integration."[40] For *Operation Joint Endeavor*, OJE, NATO tailored a multinational intelligence organization with shared responsibilities that included National Intelligence Centers (NICs) at the ARRC and integrated positions. The United States National Intelligence Center, USNIC, was collocated with ARRC headquarters at Sarajevo. The U.K. and France deployed NICs, and conducted intelligence operations under the direction of Commander Allied Rapid Reaction Corps, COMARRC. Other national contingents had intelligence representation at brigade level, with varying degrees of effectiveness. Each nation brought certain strengths and weaknesses to the table and its own national augmentation. National Intelligence Support Teams, NISTs, formed from the National Military Joint Intelligence Center (NMJIC) supported capabilities throughout the dual structures. Able to provide rapid answerers to the commander's priority intelligence requirements, NISTs were

[39] Ibid,.56.
[40] Brian Nichiporuk, *Forecasting the Effects of Army XXI Design Upon Multinational Force Compatibility*,

valued additions to the intelligence force. However, "there were no common procedures, responsibilities, and command relationships for integrating the NISTs, and as a result, the NISTs operated and supported differently."[41] Again, the differences tended to hinder coalition sharing. A center designed to address this dissemination challenge was the Linked Operations and Intelligence Center Europe.

The Linked Operations and Intelligence Center Europe (LOCE) was NATO's interoperable automation and information processor for *Operation Joint Endeavor*. LOCE connected the US Army's MND-N to the Allied Rapid Reaction Corps (ARRC), its national intelligence center (USNIC), to IFOR Chief of Intelligence (J2), to the US Army Europe Combat Intelligence Readiness Facility (UCIRF), and finally, to the Joint Analysis Center (JAC). USAREUR's UCIRF provided the authoritative ground order of battle and the force protection databases for the theater. Since NATO had no USEUCOM JAC equivalent, the JAC fell in as NATO's theater analysis center. The intelligence flowed neatly across channels, with U.S. support transparent to NATO. USAREUR elements provided U.S. technical information that was not otherwise available to NATO. According to most sources, the allies employed their long established human intelligence capabilities to great effect. Addressing the challenge via creating a framework is only part of a solution. The structure in this instance appears adequate, however some observations indicate that the intelligence planning and the US mindset towards its use was an obstacle for coalition sharing.

Intelligence Planning

Despite the dual intelligence structure the area that remained clouded was information sharing. Theater plans did not provide releasability and sanitization procedures for sensitive national information. U.S. intelligence elements used U.S. national procedures and released classified information to the partner nations. It was sometimes a one-way street. Differing

---

RAND Documented Briefing, Arroyo Center, 2000, 29

[41]USAREUR Headquarters, *Operation Joint Endeavor After Action Report*, Volume1 May 1997, 84.

philosophies affected responsive intelligence analysis and dissemination to US. Commanders. The ARRC G2, a U.K. officer, released information strictly on a "need to know" basis. This conflicted with U.S. doctrine of shared situational awareness and broadcast intelligence. U.K. and French reporting flowed directly into the ARRC, with little getting into U.S. hands.

The operational impact of the C2 structure on intelligence was twofold. Task Force Eagle has units from Russia, Sweden, and other countries that are members of the Implementation Force (IFOR), but are not members of NATO "Stability operations require modification of the intelligence process due to the operational environment, participants, and the number and types of assets assigned."[42] The procedures for requesting information from higher headquarters were also modified. Doctrine from Joint Pub 2-01, Joint Intelligence Support to Military Operations states that the Task Force requests information from its next higher HQ, in this case the Allied Rapid Reaction Corps (ARRC).[43] The ARRC is a NATO element and does not have direct tasking authority of U.S. systems. USEUCOM and the ARRC led an effort to assign responsibilities for intelligence production. The U.S. and NATO structures did not always work in harmony to de-conflict and align production efforts. "The importance of identifying the right products, accomplished by designated experts, and delivered to the right customer in a timely manner is the hallmark of good IPB. However, for NATO and IFOR this became a challenge due to the unknowns associated with the first-ever peace operation and the need to establish an IFOR peace-oriented IPB process and meld it with national approaches as the operation unfolded. The mix of uneven intelligence experiences and capabilities of the participating nations was a factor as well."[44] This situation creates an environment characterized by lack of equilibrium, where there is a great deal of happenstance, and residual conditions are very important. Warfighting as well

---

[42] Center for Army Lessons Learned. "*Initial Impressions Report: Task Force Eagle Initial Operations: Operation Joint ENDEAVOR*," Center for Army Lessons Learned, Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, May 1996, p65.
[43] U.S. Joint Chiefs of Staff, *Joint Intelligence Support to Military Operations* (Joint Pub 2-01) Washington, D.C.: 20 November 1996, p III-8.
[44] Larry K.Wentz, "Intelligence Operations," in *Lessons from Bosnia: The IFOR Experience*, p72.

as the Stability and Support Operations produce a great deal of pressure for adaptation. An environment tends to be on the edge of chaos because the elements are constantly adapting to each other and things are always in flux.[45] Task Force Eagle's task organization, appendix B, illustrates this complexity of differences in culture, national agendas, language, and military capability.

Dissemination architectures were very difficult to impose in *Operation Joint Endeavor*, as each nation followed its own information disclosure rules. In NATO, members declare what they will share and what they will keep. Releasability of U.S. classified information to coalition partners was guided by National Disclosure Policy-1 (NDP-1) which gives senior U.S. commander authority to determine the procedures and limits for sharing classified U.S. information in that environment. An astute observation from the US Army Europe lesson learned document states:

> Foreign disclosure of U.S. intelligence information to allied partners (NATO and non-NATO), and the techniques associated with it, worked well during OJE. However, releasibility and sanitization procedures for classified materials were not planned among the participating nations before the operation.[46]

These information-sharing procedures must be established early in the planning process of a multinational operation, a concept that magnifies in difficulty with coalitions due principally by its ad hoc nature. The next section explores the paradigm of change that is required to adapt the intelligence structure and the stovepiped systems that developed because of a cognitive disposition set during the cold war, which promoted unilateral thinking.

---

[45] Thomas K Adams, "The Real Military Revolution", *Parameters*, US Army War College Quarterly vol. XXX, No. 3, (Autumn 2000), p. 59.
[46] USAREUR Headquarters, *Operation Joint Endeavor After Action Report*, Volume1 May 1997,p 91.

Cold War Mentality

"There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in success, than to take the lead in the introduction of a new order of things."[47] Taking on the challenge of change in 1995, the Secretary of Defense and Director, Central Intelligence Agency agreed the time had come to break down some of the leftover Cold War security barriers and go from a "'System High' environment to a 'System Low' one. Their objective was to ensure that information was put into the hands of those who needed it in a timely fashion without revealing sources and methods, but stringently protecting highly sensitive information."[48]

Mental Model

Operation Joint Endeavor required strategic, operational, and tactical intelligence operating in joint, combined, and interagency roles. At the tactical level, functional units contributed to reconnaissance and surveillance plans, the intelligence reporting process, and the synthesis of information. The national and operational levels of the intelligence community gave priority attention to the intelligence gaps, stepped into the tactical arena with specially-equipped forward support teams, and purpose built collection systems to exploit the non-lethal OJE environment. The intelligence system was organized and resourced for sensor-to-shooter targeting with go-to war, mobile, tactical assets. Stove piped technology prevailed. Multi-service and multinational aspects of operating in a peace enforcement environment were missing from most intelligence doctrine, plans, and tactics, techniques, and procedures.

The Linked Operations-Intelligence Centers Europe (LOCE), a theater level intelligence sharing center, started as a U.S. system and was adopted by our allies because it was further along in development and offered better capability than what was available to them at the time. "While our coalition partners now are fully using LOCE and sharing information among themselves, the

[47] Machiavelli, Niccolo, "The Prince", translated by W.K. Marriott, J.M. Dent & Sons, London 1908, p29.
[48] Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield: May-July 1996,"* Office of the Under Secretary of Defense for Acquisition and Technology, Washington, D.C. p 19

Defense Science Board Task Force (DSB) noted many cases where U.S. forces are not taking full advantage of the information in LOCE. One reason is inadequate training. Another reason is the attitude 'I've got my own system; I don't need to use that one."[49] This attitude reflects a cold war mentality of over specialization and a unilateral approach to information sharing.

Despite attitude, there is a need to push intelligence capability by echelon lower. The intelligence architecture needs to move Corps capability down to the Division level and Division capability down to the Brigade level. To include fielding a Trojan Spirit system at brigade level. Other factors exacerbated the information need found by the DSB down at the battalion level. The DSB found many examples of reduced effectiveness due to the constraints of narrow bandwidth in communications systems and equipment that did not work.

> The DSB found a 15' AT&T antenna installed right outside a Battalion Headquarters providing 3 Mbps connectivity for telephone calls home from the troops, provided they had an AT&T credit card. We could have brought some of that bandwidth to get SECRET REL NATO operational data to the war fighters at the battalion level. But to do so in the future requires we reevaluate the doctrine of how we conduct operations other than war, OOTW, and other types of conflict.[50]

The vignette is another example of the U.S. mental inflexibility with the intelligence challenges of pushing capability lower. The model not only has to change in regards to quantity of information but also the nature or kind of intelligence is different in peace operations. A contrast in priority in conventional operations, political intelligence is primal in stability and support operations.

[49] Ibid.
[50] Ibid., 27.

Intelligence Focus

Within120 days of the Dayton Accord signing, the military mission geared towards combat is now primarily all sustainment. The research suggests that the implementation of the Dayton Accord would be better served if the division intelligence officer provided intelligence on political and military (POL/MIL) issues. This type of intelligence would be very useful to numerous units such as Civil Affairs, PSYOPs, and Public Affairs. Knowing who the real "Power Brokers" are whether political, religious, cultural, ethnic, or criminal is key to mission success. G2 should not forget about combat intelligence, but should shift resources to at least provide basic Political/Military information to subordinate units. With all the convoys operating in Bosnia and numerous eyes and ears in these convoys, the CA, PSYOP, CI, MP, and PAO elements can provide G2 a wealth of information that can be assembled into beneficial intelligence for the command. POL/Mil intelligence can help to identify potential trouble spots such as protest sites, grave visits, mass visits to home sites by former warring factions etc. "This intelligence will allow commanders to be better prepared with forces and courses of action. The lesson learned is intelligence for peacekeeping operation is considerably different from intelligence used during combat operations."[51] This opinion is collaborated by research conducted by the Defense Science Board, a Federal Advisory Committee established to provide independent advice to the Secretary of Defense.

Push versus Pull

The Defense Science Board conducted visits to the U.S. National Intelligence Centers (NICs) and our IFOR and NATO intelligence centers and found widely varying daily numbers of Requests for Information (RFI) and a sense that there needed to be a change in the current approach.

> Instead of having intelligence center staff sitting at the Centers and writing to be asked for information by operators who don't know what they can ask for, the

[51] Center for Army Lessons Learned, *Initial Impressions Report: Task Force Eagle Initial Operations: Operation JOINT ENDEAVOR.,* September 1996, C-43.

> Task Force believes we need to move to the anchor desk concept and learn to produce and distribute the right specific product sot support focused operational needs. This is a totally different role for the resources. By using common standards for metadata descriptors and ensuring data is geospatially referenced, time-tagged, and pedigreed, all providers can work more effectively, and integrated products will be possible. Rationalized databases can be specified and implemented.[52]

The intelligence community needs to get away form the current concept of the national intelligence centers (NICs) and other units waiting to be asked for information through the request for information (RFI) process, and then responding to the request. Instead, national and joint intelligence centers must use their knowledge of available products and ones that can be produced, i.e., custom products, as they anticipate what is needed at lower levels and do a smart push of it through the expanded communications pipes. The DSB Task Force found examples of this type behavior at the Joint Analysis Center (JAC). The informal system of personal relationships, 'back channels', and liaison staffing is inefficient, but shows that the information usually is there or can be produced if one knows how to go after it. The Task force is confident that a formal system can be as effective and achieve higher efficiency.

Collaborating this line of reasoning, a former Chief of Joint Intelligence in Bosnia, contends that the IFOR/SFOR divisions operate in the tactical realm, and IFOR/SFOR headquarters attempts to operate in the tactical-operational domain. Those headquarters above IFOR/SFOR should operate most generally in the operation-strategic sphere. When this is violated, the doctrinal basis of levels of command and their supporting intelligence elements is damaged. Higher levels should be separated not only in perspective, but also in time from lower levels. This applies to intelligence reporting and analysis as well as it does to other aspects of command and control.

> As an example, the fact that a single VRS brigade had an alert should not be a must-be-reported-now item to high levels of command; as it turns out most of these are nonevents. The action of a single brigade should be of little interest to a higher headquarters. If we are all analyzing the same information for the same

[52] Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield:* p 35

> objectives, then we have probably failed our commanders and wasted the resources provided to us.[53]

In the case of theater level intelligence analysis centers (like the JAC), it is possible that they may do intelligence analysis and reporting at all three levels, from the tactical to the strategic, to service their customers at all three levels. If this is so, then their support should be provided to the respective level commander, rather than broadcast across all spectrums of command. If they do no follow this general guideline, they risk contributing to the problem.[54]

The need to check facts and their analysis is obvious, but in the rush to publish, it is often forgotten. From the higher levels, it should be possible to check these facts and analysis with SFOR or other sources if necessary, before publication; we certainly possess the communications to do so. Much of what is rushed to publication would be improved by time, consideration, and research. Value would not be lost even if it waited 24 hours, much like the difference between news and intelligence.

> If the information is not crucial to the decision maker within your organization, then why must it immediately be published? Are we really in competition to publish first? We have spent considerable time perusing the traffic early in the morning for those erroneously reported items which we know will result in a phone call to COMSFOR (with varying degrees of success); we provide him information so he can say he knows about it and that it is not important or true. At present, we have to do this because of the way our systems works (or doesn't work); we all could spend this time better doing "intelligence" rather than "damage control".[55]

The ability to communicate is desperately vital to sharing intelligence. As technology moves towards written forms of communication, second language knowledge will increase in importance in coalitions.

[53] John C Hammond. MEMORANDUM FOR THE COMSFOR: SFOR Tour Report
[54] Ibid.
[55] Ibid.

Language Cognition

Much has been learned from working with IFOR allies in this ongoing mission. The most profound lesson is the importance of being adaptable to pull separate national units together as a brigade; and to do it communicating via a second language. US allies deserve credit for their superb command of English, the second language that made most of IFOR accomplishments possible. Proficiency in a foreign language should become a requirement for American military professional development. Not all multinational units will have command of the English language as many in the Nordic-Polish Brigade did. Even when working with allied soldiers fluent in English, displaying knowledge of their language and culture is greatly appreciated and encourages team building.[56] Brigadier General (Retired) Hall, former INSCOM commander, states that

> the way people think, sense, and perceive are constraints in future operations. This observation holds true for people we face in competitive endeavors and for people we work with in coalition operations…With the stated importance of multi-national and coalition operations, it's just as important to wargame the act, react, and counteract cycles of coalition partners as it is to wargame against the actions of foes.[57]

Stove piped thinking leads to hardware development and employment that adds perhaps the most daunting obstacle to coalition intelligence sharing.

Technological Interoperability

The role that intelligence technical systems had on sharing in Bosnia's multinational environment is address in this section. Several authors contend that technology advancement has both a negative and positive impact on intelligence sharing in a coalition environment.

> Technology is a two-edged sword in coalition operations. Global communications systems enhance connectivity among coalition members;

[56] , Harold Knudsen, "Fire Support for the Nordic-Polish Brigade: An Interoperability Lesson for the Future", *Field Artillery Journal*,(May-June 1997), p.11

[57] Wayne M Hall, *The Janus Paradox: The Army's Preparation for Conflicts of the 21st Century*, Paper, Interim Brigade Combat Team (IBCT) O&O Concept, Hall, 15 August 2000, p11.

> emerging military technology allows unprecedented surveillance. Moreover, information technologies have the potential to accelerate deployments and permit decisive operations. The downside is that rapid and costly changes in technology also create barriers to effective integration of coalition forces.[58]

It is beyond the scope of this paper to address the detailed merits of technology, however, the discussion of operational level intelligence capability that directly influences sharing, and foreign disclosure is addressed.

Intelligence Processors

There were numerous U.S. intelligence processors deployed for *Operation Joint Endeavor*. The TF Eagle Analysis and Control Element (ACE) alone had eleven systems. This enhanced the dissemination of finished intelligence and raw information. However, the lack of compatibility among systems and the differing levels of classified information they could process complicated dissemination. In addition, the classification of collection systems and the information from them, both U.S. and multinational caused modification of tasking and information dissemination.

Intelligence processing for *Operation Joint Endeavor* (OJE) was automated and joint. The Joint Deployable Intelligence Support system (JDISS), sponsored by the Defense Intelligence Agency (DIA) General Defense Intelligence Program, provided support. The JDISS is a strategic and operational system encased in a laptop computer that compartmentalizes highly classified intelligence information by intelligence discipline. Intelligence disciplines include counterintelligence (CI), signal intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), technical intelligence (TECHINT), and human intelligence (HUMINT). The system was the primary connectivity to national databases. There were more than 750 JDISSs deployed in USEUCOM, over half at the JAC. JDISS provided immediate access to theater and national databases. NISTs equipped with JDISS gave the IFOR, ARRC, and TF Eagle direct access to the latest national information. NISTs provided

[58] Robert H. Scales, Jr., "Trust, Not Technology, Sustains Coalitions", *Parameters*, US Army War College

JDISS training to TF Eagle and USAREUR (Forward) DISE operators. However, the JDISS could not be electronically connected for data exchanged to the processing systems at corps and division. "The lack of connectivity between echelon above corps EAC and echelon below corps EBC systems was caused by security access restrictions. Intelligence data was compartmentalized and communicated to users within their own stovepipe arrangements, a root cause of the proliferation of intelligence processing systems."[59] This problem is neither exclusive to a level of conflict and more importantly plagues the effective interoperability of systems in a coalition. More is not necessarily better.

Positive Impact

Not every intelligence processor system employed reflected the vestiges of the cold war. Several other automated systems were key to data basing information and delivering timely intelligence, especially during the deployment phase. The USAREUR Combat Intelligence Readiness Facility UCIRF created and maintained the theater force protection database, called Blackbird. Force protection teams interviewed the local populace and passed information, to include digitized images, to the Blackbird database with their TRRIP systems. New information was passed through the Secret Internet Protocol Router Network (SIPRNET) to the INTELLINK national database. In this way, the secret collateral database could be shared immediately from national to tactical.[60] Another example of effective employment of US intelligence sharing technology in this environment was the WARLORD.

"Ninety percent of the intelligence passed to the task force was via the WARLORD system. The WARLORD was the most effective intelligence processing system in TASK Force Eagle."[61] There were thirty WARLORD systems located with units in Task Force Eagle. The

---

Quarterly, vol. XXVIII, No. 4, (Winter 1998-99), 6.

[59]USAREUR Headquarters, *Operation Joint Endeavor After Action Report*, Volume1 May 1997, 82.

[60] Ibid.

[61]Center For Army Lessons Learned, *Initial Impressions Report: Task Force Eagle Initial Operations: Operation JOINT ENDEAVOR.* Center for Army Lessons Learned. Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, May 1996, 66.

WARLORD was placed at all brigade level headquarters of those participants in *Operation Joint Endeavor*. The level of classification of material available on the WARLORD caused the institution of special security requirements. The WARLORD gave the operator access to several different databases; much of it not normally releasable to NATO or non-NATO nations. To ensure that the nations working within the MND (N) had access to classified material they needed for operations, additional levels of access were developed. The information on the WARLORD system is divided into the categories of Secret NORFORN, no foreigners, Secret Releasable to NATO, Secret Releasable to Implementation Force (IFOR). To ensure that no compromise of classified material occurred, a three-step process was performed. First, a U.S. system operator reviewed the material for release to the host unit and then pulled the information off the WARLORD. Second, the U.S. operator gave the information to the Special Operations Command Liaison Control Element (SOCLCE) OIC, who reviewed the material to ensure releasabiltiy. The third step was to provide it to the unit they are supporting. At no time did the systems allow for the transfer of needed intelligence between all Operation Joint Endeavor participants without compromising U.S. or NATO security. As personnel rotate into the liaison element, the incoming personnel must know and understand the system to ensure that no lapses in security occur. WARLORD performance during Operation JOINT ENDEAVOR was invaluable.[62]

The ASAS, a corps and division processor, was the heart of TF Eagle ACE functionalities, and was not user-friendly. The division and brigade intelligence processor, the WARLORD (ASAS-W), was a better tool. The most effective processing system deployed was the Theater Rapid Response Intelligence Package (TRRIP). Used by force protection teams, the ACE, and USAREUR (Forward) Deployable Intelligence Support Element (DISE), the TRRIP could transmit digital imagery, pull still images from videotape, scan and transmit documents,

---

[62]Center For Army Lessons Learned, *Initial Impressions Report: Task Force Eagle Initial Operations:*

and create and transmit written reports. It was also linked to national databases, pushing and pulling intelligence. All this information required data storage before dissemination.

Sharing Intelligence databases

The JAC maintained the ultimate theater database, a fusion of air, ground, and maritime intelligence, which was culled and disseminated through JDISS. This all-source U.S. only processing system was available at all U.S. intelligence nodes. From USAREUR's point of view, the JDISS provided the primary link to the rest of the intelligence world, and intelligence operations could not function without it.[63]

A less understood and usually ignored portion of the intelligence architecture was the simultaneous reporting by the aerial surveillance platforms into the broadcast systems, i.e., Tactical Data Dissemination System (TDDS) and Tactical Information Broadcast System (TIBS). Both TDDS and TIBS were received in the CAOC and then fed into the RAP display that was maintained on a system call ADSI (Air Defense System Integrator). This caused some redundant reporting. One interesting but somewhat frustrating aspect of the surveillance operation was the fact that the air situation picture or RAP was a NATO product coming primarily for NATO sensors (NAEW) and managed by the NATO CAOC. The NATO commanders consistently refused to provide the air picture to U.S. theater headquarters based on the logic that they would then have to provide it to all NATO capitals. This greatly frustrated some U.S. commanders and DISA engineers who wanted to implement a Common Operation Picture (COP) on the U.S. Global command and Control System (GCCS) as part of the BC2A initiative.[64]

The DSB Task Force believes that not just the JIMC and JAC but other JICs and Theater NICs should be proactive providers using common geospatial reference time tags and pedigreed information. This will address the problems that prevent us now form pulling up data because we

---

Operation JOINT ENDEAVOR., 66.
[63] Ibid., 83.
[64] Ibid.,100.

can't find it and then, if it is found, not being able to use it fully because we can't get it overlaid on top of each other. Solving the problems that prevent us from retrieving data must be a high priority.

Multilevel Security

Intelligence units were unable to link automation systems together on a single local area network (LAN) because of security requirements. DIA must approve multi-level security before a system can be used for all functions (i.e., JDISS to ASAS, unclassified and classified information automated through one process and able to access each level). This created a complex automation environment and large amount of duplicative cabling to link systems together. Commercial systems existed, certified by DIA and NSA, to operate on a single LAN through a multi-level server. Army intelligence units at I Corps already use such devices. With the increasing amount of automation at the tactical level, the use of a multi-level secure LAN server would reduce the time, complexity and resources necessary to link systems together.[65] The Task Force found that DIA has several less than perfect, multilevel security solutions available now. The Task Force recommends that DIA pick one, install it at the Joint Analysis Center (JAC) as well as other locations operating to the same constraints and not wait for the 100% solution-that the benefits of doing so appear to outweigh the risk in this circumstance.[66]

Communications and information security issues had to be dealt with as well. Although the military communications and information systems operated SECRET system-high, other systems were not secure. The Internet, INMARSAT, cellular, and commercial telephone systems were not protected and were frequently used for command and control purposes. Configuration management and information protection measures; virus protection and intrusion detection and protection were slow in implementation. Diskettes were shared between classified and unclassified systems and there was a lack of discipline and standard operating procedures to

[65] USAREUR Headquarters, *Operation Joint Endeavor After Action Report*, Volume1 May 1997, 890
[66] Ibid., 45.

effectively control the situation. There was a lack of security devices such as secure telephone, safes, and shredders. Security was an ongoing responsibility for which improvements were continuously made over the duration of the operation.[67] However, at least one researcher contends that security was lacked and computer viruses were widespread.

> We have coalition partners shoving data back and forth at each other. We should take seriously the capabilities of other forces and discipline ourselves to make it harder for other forces to know or anticipate our intentions and plans and to attack our systems. At the very least, we should expedite the deployment of secure cell phones for our forces in the field.[68]

Addressing the security challenge is not limited to hardware; sometimes it is met by practicing operational security.

Operational Security (OPSEC) was particularly challenging for the IFOR operation. The operational environment was reasonably stable for Bosnia. However, the lack of an obvious threat bread a sense of complacency, which is a threat in and of itself. Other types of OPSEC risks had to be managed as well. There were numerous television and print journalists question soldiers, and the soldiers had to be briefed to ensure they did not release classified information to the media. Every day, hundreds of local national workers entered IFOR areas of operation. It was a challenge to keep a close eye on these daily visitors. OPSEC is an operations function, not a security function per se. Therefore, there must be integrated into the planning and execution of the operation. Given this operational environment, commanders demanded more communication capacity, which equates to bandwidth.

[67]Larry K Wentz, "Intelligence Operations," in *Lessons from Bosnia: The IFOR Experience*, 67.

[68] Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield:* 55.

Bandwidth

To move all this information required a large communications capacity. Trojan Spirit II, an intelligence-only communications pipeline, provided the throughput for the intelligence system and deployed with all the forward intelligence elements. A prototype Joint Broadcasting System (JBS) also deployed and was available to intelligence users, primarily for unmanned aerial vehicles (UAV) transmissions. It provided plenty of bandwidth, but technical and experimental restriction on its use required the dedicated communications switches of TROJAN Special Purpose Integrated Remote Intelligence Terminal, Spirit II. Another example of the stovepiped technology left over from the cold war.

While significant progress has been made in strengthening the LOCE system by extending the range of information that can be carried on it and encouraging allies and coalition partners to make their own contributions of information, the Task Force finds our forces are not exploiting LOCE as they should. Continuing limitations with the LOCE system that contribute to its underutilization by U.S. forces include: LOCE bandwidth is far too low at major nodes (only 19.2kbps and often is less than that depending on how a site is configured) and does not allow for effective information push to the brigade level; US forces cannot easily move between LOCE and U.S. databases; the ACE is reacting rather than pushing information; and there is no electronic connectivity between the Army's Warlord system and LOCE.[69] While the U.S. is prevented from giving Bosnia Command and Control Analysis (BC2A) equipment to other countries, one route to further coalition activities could be other countries buying receiver suites that would allow them to get the JBS broadcasts.[70]

The DSB Task Force finds that great improvements has been made in getting information processing, distribution, and dissemination down to the division, wing and battle group level through the use of JBS. It is so much better than last August that 'improvement' is not even the

[69] Ibid.
[70] Ibid., 24.

right work, but the dramatic change does not yet occur below those levels. Nineteen of the original 29 requested JBS sites have been fielded in support of Operation Joint Endeavor, but 51 locations are needed according to Commanders. JBS is providing great connectivity where it is deployed, but should be further deployed immediately to lower echelons where bandwidth is greatly limited. The Task Force believes it is important to continue the process of bringing JBS up to its full potential as a foundation for the Global Broadcast System (GBS) recommended by the DSB previously and endorsed in other studies. JBS should be seen as a low cost, low risk opportunity to explore technology and operational implications before making major GBS commitments.[71]

Imagery Sharing

New sources of imagery appropriate for ground commanders emerged from OJE. Specifically, gun cameras, UAVs, hand-held digital cameras, and video were highly productive. However, effective methods to catalogue and maintain registries of such images did not exist. Some images found their way to the imagery servers at the JAC, but much of the imagery form the Theater 'Rapid Reaction Intelligence Package (TRRIP) never found its way to a theater level server. The Predator ground station module did a good job of capturing still images from the motion sequences and did load these onto the imagery server at the JAC. One problem associated with this was that imagery from the Predator had to be manually manipulated to move it to the appropriate collateral server at the JAC. Automation capabilities were not networked. Elements using and developing low level imagery such as TRRIP and other hand-held sources, did not establish techniques and procedures for integration and distribution of their products.[72]The manned imagery system, ARL had dissemination problems as well.

Although the Arial Reconnaissance Low, ARL, was a workhorse aircraft for TF Eagle, it did have some shortfalls. The ARL downlink, called a remote vehicle terminal (RVT), did not

[71] Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield"*, 23.
[72] USAREUR Headquarters, *Operation Joint Endeavor After Action Report*, Volume1 May 1997,196.

always receive the video or selected images on the same day of the mission. Terrain masking limited the line-of-sight connection and it took two or three days to get the complete ARL video mailed or delivered to the TF Eagle ACE. Some of these problems are indicative of stovepiped technology development. However, the Defense Science Board recommended some changes.

The 1995 Task Force recommended immediate declassification of the Controlled Imagery Base (CIB) to provide gridded photo maps to our land forces. There was great evidence of a need for that on the ground. The Task Force believes that a sufficiently rich mixture of sources (National, Theater, Organic, commercial) is achievable to hide the ultimate capabilities of our systems while providing the highly current materials needed for effective use of tools such as PowerScene and Eagle Vision.[73]This kind of flexibility or dynamic reconfiguirbility is a paradigm shift.

Dynamic reconfiguribility.

Common information to/from lower force element levels is needed to make 'jointness' even more effective. The DSB has said before that the JTF Commander needs the right collection of tanks, ships, planes, and warriors to accomplish the OOTW mission objectives. In Bosnia, because the mission phases change, the requirements, and capabilities mix also changes over time. In the world of C4ISR, information capability is the ability to hook together the right hardware, software, information systems, databases, communications pipes, and sensors to support that ad hoc collection of shooters. This is what 'dynamic reconfigurability' means: the flexible reengineering of C4ISR systems and processes to be able to "plug and play.'[74] This is the opposite capability of stovepiped technology.

Conclusion

The Army needs to review doctrine in light of coalition control of the intelligence process in a non-U.S. pure environment. USAREUR, as a deploying force, must maintain dialog with

[73] Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield"*, 59
[74] Ibid., 23.

national intelligence agencies to identify systems for environment specific problems for collection, exploitation, and dissemination. The formal training system must re-emphasize basic Intelligence skills while finding a methodology for dealing with an accelerating technology base and widely divergent areas of operations. Finally, tailored response packages will eventually demand that only the essential is deployed forward with a correspondingly higher reliance on split-based support from sanctuary.[75]

These issues reflect the organization, doctrine, training, coalition, and equipment observations from *Operation Joint Endeavor* and represent how this operation is relying more on information-skilled soldiers and emerging technologies. The research emphasizes that this finding is not a criticism of any organization in particular, because this situation did not exist before. Pushing intelligence capability lower and expanding into political and cultural intelligence are representative of the required paradigm shift. These changes have resulted from communications and other technology/systems advances that permit more of this information to be disseminated at lower levels; thus, information management is the emerging challenge that is beyond the scope of the paper. However, chapter three evaluates Bosnia sharing vignettes against intelligence standards for the validation of relevancy.

CHAPTER THREE

III. SHARING VERSUS THE INTELLIGENCE STANDARDS

This chapter uses U.S. multinational operations in Bosnia as a case study for assessing relevance in operational intelligence practices. Monograph uses vignettes to measure the qualitative criterion against the policy and procedures used in *Operation Joint Endeavor.*

[75] USAREUR Headquarters, *Operation Joint Endeavor After Action Report*, Volume1 May 1997, 94.

The five tenets of intelligence quality from the Joint Doctrine for Intelligence Support to Operations, JP 2-0, and the multinational principles for implementing policy and procedures are evaluation criterion. These tenets and principles are qualitative standards against which the monograph evaluates intelligence activities and products. A failure to achieve any one of these fundamental attributes may contribute to a failure of operations. Brigadier General John Smith, former Director, Intelligence Directorate (J2) of SOUTHCOM contends that some argue that providing intelligence in a Bosnia-type scenario is unique, others argue that the principles of intelligence support are enduring; regardless of the operation and differ only in detail. Regardless there are certain aspects of planning for intelligence in stability and support operations, which deserve special emphasis if that support is to be effective.[76] The author acknowledges the limitation of conclusive findings due to the brevity of selected examples. However, there may be value in the exploration of trends and enduring qualitative principles.

Five Tenets of Intelligence Quality

Timeliness- *Intelligence must be available when the commander requires it. Late intelligence is as useless as no intelligence. Timely intelligence enables the commander to anticipate events in the operational area. This enables the commander to time operations for maximum effectiveness and to avoid being surprised.*

Current time requirements for the simultaneous fusion of real-time or near-real time (NRT) collection with other analysis and reporting stretch the boundaries of current intelligence architecture capabilities. For example, same-day imagery is no longer sufficient. The acceptable time scale for effective all-source fused intelligence support to the combat forces is now measured in minutes and hours.[77] According to COL George Gramer, former Intelligence director on the CJ2 staff, HQ IFOR, NATO releasable SIGINT reporting consistently was a day late and a

[76] , John W Smith. "Essential Stability and Support Operations Planning Factors*", Military Intelligence Professional Bulletin*, Fort Huachuca, Volume 22 No. 4,(October –December 1996), 2

[77] Hector M. Cuevas, Jr., "Collection Management and Imagery Support to Deep Operations in Kosovo, *Military Intelligence Professional Bulletin*, Volume 26, Number 1, The U.S. Army Intelligence Center and

dollar short. It often comprised only marginally useful information as much as three to four days old. SIGINT not releasable to all the NATO and IFOR partners existed in fairly large quantities; however, its limited distribution decreased its ultimate value to HQ IFOR significantly.[78] Other intelligence disciplines, particularly human intelligence, enabled the commander to make timely operation decisions in a stability and support operation. The US Army's lack of depth in this area is by design of systems and capabilities developed for the conventional operations during the cold war.

Objectivity- *To be accurate, intelligence must be objective. It must be free from any political or other constraints and must not be distorted by pressure to conform to the positions held by higher levels of command. Intelligence products must not be shaped to conform to any perceptions of the commander's preferences. While intelligence is a factor in determining policy, policy must not determine intelligence.*

Open source intelligence (OSINT) is a valuable resource particularly in a peacekeeping environment. Much of it, however, has the slant of the authors or sponsors, and may actually be designed to influence the readership, to include us. Coupled with the reality that one can often find an article somewhere to support almost any position or assessment, the user must be very careful of it utility as intelligence. As an example, an intelligence officer spent much of a day researching an item put in a high level intelligence summary that was based on a FBIS (Foreign Broadcast Information Service) item where a high level Federal Republic of Yugoslavia official commented on the movement of tanks from a location. No time frame was given or purpose for the move. The slant of the subsequent intelligence article published was that tanks had probably been moved without approval. The intelligence chief had to prove the negative; not tanks had indeed moved from this location since war's end; and the area was under surveillance and monitoring so it was very unlikely that anything had recently occurred. It is also possible the official was mistaken or referring to another movement elsewhere (of which there were many). A

Fort Huachuca, (January-March 2000), 16.

[78]George K Gramer, Jr. "Operations JOINT ENDEAVOR: Combined-Joint Intelligence in Peace Enforcement Operations," *Military Intelligence Professional Bulletin*,(October-December 1996), 13

single press article presented as intelligence, with no other corroborating indicators, caused an overreaction. What is "press" must be clearly labeled, and well-founded assessment based on other information must always accompany it.[79]

Due to the nonmilitary nature of many of the COMIFOR's intelligence requirements, HQ IFOR should have had the ability to impact more extensively on non-military collectors and receive releasable products in return. Further, NATO remains a political organization, and as such, sixteen national agendas must be satisfied. The correct political spin was needed, even on intelligence, a product that generally should be devoid of specific political consideration or bias.[80]Offering a different opinion is Carl Von Clausewitz: "War cannot be divorced from political life; and whenever this occurs in our thinking about war, the many links that connect the two elements are destroyed an we are left with something pointless and devoid of sense."[81]

Usability- *Intelligence must be tailored to the specific needs of the commander and provide in forms suitable for immediate comprehension. The commander must be able to quickly apply intelligence to the task at hand. Providing useful intelligence requires the producers to understand the circumstances under which their products are used.*

The impact of the ARRC intelligence summary (INTSUM) was considerable. It was clearly the premier releasable intelligence information in theater. There were other daily products of importance, notably the Joint Analysis Center Molesworth Balkan INTSUM and the ARRC Commander's Assessment Report and SITREP. HQ IFOR also received infrequent products from the national intelligence agencies of several NATO nations, including the U.S. Defense Intelligence Agency. Unfortunately, most releasable reporting subsequent to the ARRC INTSUM was a regurgitation of the ARRC INTSUM in a variety of other formats. This led to

[79] John C Hammond,. SFOR Tour Report, 4 December 1996-26 September 1997.

[80]George K Gramer, Jr., "Operations JOINT ENDEAVOR: Combined-Joint Intelligence in Peace Enforcement Operations," 14

[81] Carl von Clausewitz, *On War,* ed. and translated by Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 605.

redundant reporting of the same data by multiple reporters that can add an impression of multi-source validation. To add to this confusion, some theater and national intelligence agencies reported data as soon as possible, whether corroborated or not, often requiring retractions. There was relatively little analysis or assessment in most of the releasable intelligence products. As a result, the IFOR leadership extensively criticized some of these products and the intelligence centers producing them.[82]

Completeness-*Complete intelligence answers the commander's questions about the adversary to the fullest degree possible. It also tells the commander what remains unknown. To be complete, intelligence must identify all the adversary's capabilities. It must inform the commander of the possible courses of action that are available to the adversary commander. When justified by the available evidence, intelligence must forecast future adversary actions and intentions.*

U.S. deliberate and methodical planning contrasted with the casualness of other nations; the U.S. reliance on decentralized decision-making was in sharp contrast to the centralized execution of the Russians; and the timeliness and completeness of reporting and follow-up met a wide variety of standards. While U.S. units reported volumes of battlefield information based on troops in contact, French reporting was minimal, reflecting only significant activity and largely ignoring order of battle. One of the clearest differences was illustrated by the manner in which the multinational divisions analyzed and approved factional weapons declarations. After plotting all the declarations, the U.S. conducted an intelligence preparation of the battlefield (IPB), analyzing the road networks, distances to the zone of separation (ZOS), and terrain that afforded concealment, looking for likely weapons storage or hiding places that were not declared. Then, the G2 directed reconnaissance of the suspected sites to find violations. The result of theIPB produced hundreds of violations. In contrast, neither the British nor the French deliberately looked for declarations violations, resulting in a tremendous disparity within the ARRC between the U.S. sector and the other MNDs. After conceding that the U.S. methodology 'was brilliant',

[82] George K. Gramer, Jr., Operations JOINT ENDEAVOR, 12.

the ARRC G2 requested that it not be used for evaluating future declarations.[83]

Relevance- *Intelligence must be relevant to the planning and execution of the operation at hand. It must aid the commander in the accomplishment of the mission. Intelligence must contribute to the commander's understanding of the adversary. It must help the commander decide how to accomplish the assigned mission without being unduly hindered by the adversary.*

There are no countries in the NATO Alliance that share intelligence to the extent that the U.S. does. Either they do not have the capacity to collect in the region, to process the information they do have, the ability to disseminate it to SFOR, or the will to share in a deliberate manner. According to an American intelligence officer, information provided by both the Germans and the French has been inconsequential and incomplete, when provided at all. Even when there is agreement at the highest levels (such as the signals intelligence sharing required by the NATO Communications and Information System Agency, NACISA, agreements) there is often great resistance to sharing at the lower levels; this is even experienced with the U.S. SIGINT community whenever there is a unit change in Task Force Eagle.[84]

Validation

Of the five tenets of intelligence quality, *objectivity* did not validate as relevant in the stability and support operation. The primacy of political agendas manifested in national through local levels negated the viability of this tenet. Open source intelligence will increase with the proliferation of the World Wide Web, Internet, and globalization. Based on the intelligence requirements of the 21st Century and the likelihood of SASO coalitions it is this researcher's position that political and cultural naiveté is not a viable excuse for the exploitation of operational and strategic aims in a knowledge based organization. The tenet of *timeliness* and *relevancy* presents a duality that presents the next technological and analytical challenge. Getting the right intelligence quickly to the decision maker without overwhelming him/her with boundless data is knowledge management, the next step.

[83] Melissa E Patrick,. *Intelligence in Support of Peace Operations*, 35.
[84] John C Hammond, SFOR Tour Report; 4 December 1996 to 26 September 1997.

Five Principles of Multinational Intelligence

Intelligence in multinational operations has identified five general principles for implementing policy and procedures: (Joint Publication 2-0, appendix A). These principles are further developed in FM 100-8, as essential to the successful conduct of operations in a SASO environment. The following examples are not all inclusive yet they are indicators for the employment of the principles. For the scope of this monograph, they are characteristic of operational employment against the standards.

Maintain unity of effort - *Intelligence officers of each nation need to view the threat from multinational as well as national perspectives. A threat to one element of an alliance or coalition by the common adversary must be considered a threat to all alliance or coalition elements.*

The Task Force felt that the Russian Brigade was getting better intelligence down at the brigade level than we were because we had one of our sharpest U.S. Army Major S2's there with a group of twenty young people skilled in communications. The Task Force asked the Army Major,

> Do the Russians let you into their intelligence center the way you let them into yours? The Major replied, "I am their intelligence center". And the Task Force was very proud of what we heard. We saw young people who were overcoming the stovepipe systems that we still deploy by innovating. They did not ask for some acquisition manager in the Pentagon to approve it. They were just doing it. Better and interoperable systems eventually must replace the local efforts, but until then these efforts help get the job done for our war fighters.[85]

Make adjustments - *There will be differences in intelligence doctrine and procedures among the coalition partners. Major differences may include how intelligence is provided to the commander or procedures for showing information among intelligence agencies.*

Intelligence doctrine and methodology varied widely among nations with significant differences in how the non-U.S. units approached intelligence operations. While the Nord-Pol brigade S2 functioned in a manner similar to the U.S. paradigm, the Russian brigade S2 was

[85] Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield"*, 62.

primarily a chief of reconnaissance and did not conduct all-source reporting. Reporting by any element other than reconnaissance patrols went to the Russian Chief of Staff and was never passed to the S2. As a result, the Russian S2 did not provide all source reports, seemingly because he had no mechanism for all-source fusion or analysis. Indeed, the center of gravity for the brigade's intelligence appeared to be with the Russian Chief of Staff, who had no linkage to the MND intelligence system. Additionally, the Turkish brigade had no professional intelligence personnel and had an S2 in name only. For all practical proposes, the intelligence channels in the Turkish brigade were nonfunctional other than what was provided by the US liaison team.[86]

Plan early and plan concurrently- *This permits solutions to differences to be developed and tried before operations begin.*

The fast-paced IFOR and national planning efforts had some negative impacts of the orchestration of theater intelligence production. Several organizations, in their enthusiasm to provide useful products, ended up duplicating efforts. For instance, for the United States, both the Task Force Eagle and the UCIRF produced assessments on the links between NGOs and foreign forces; and both the JAC and the USAREUR Forward Deployable Intelligence Support Element (DISE) produced pieces on political-military analysis. Likewise, while some efforts were duplicated, other critical areas fell short. For *Operation Joint Endeavor*, the roles of all the intelligence producers could have been more clearly defined. A better division of effort could have been assigned among the IFOR, ARRC, and MND players.[87]

Share all necessary information- *Coalition members must share all relevant and pertinent intelligence about the situation and adversary.*

The DSB Task Force believes that a comprehensive, current, and shared Ground Order of Battle is needed to reduce the threat of fratricide as well as improve the executions of joint

[86]Melissa E Patrick, *Intelligence in Support of Peace Operations*, 26
[87]Larry K. Wentz, "Intelligence Operations," in *Lessons from Bosnia: The IFOR Experience*," p72

operations against mission objectives. ARRC policy restricts release to higher echelons. It is possible that allies are reluctant to contribute Blue data because of concerns that the data might go back to their countries through new or uncontrolled channels.[88]

Conduct complementary operations - *Intelligence efforts of the nations must be complementary, and all intelligence resources must be available for application to the whole of the intelligence problem.*

While the U.S. intelligence contribution to Joint Endeavor surpassed that of the other nations, one should not assume that intelligence sharing was a one-way street, with the U.S. serving as the sole contributor. Other nations brought capabilities that either augmented or enhanced what the U.S. provided, particularly in the field of human Intelligence (HUMINT). Within MND-N, the CI/HUMINT structure incorporated two multinational NATO units provided by the ARRC in direct support of MND-N. The Joint Forces Intelligence Team (JFIT) was a British HUMINT organization, which over time formed a partnership with the U.S. Defense HUMINT Service (DHS), adding several DHS officers to its roster. JFIT also integrated several Norwegians, former United Nations Military Observers (UNMOs) with experience among the VRS, and thereby gained access to traditionally closed areas. The other unit, the Allied Counterintelligence Unit (ACIU) was an UK-US counterintelligence unit, which developed a close working relationship with the U.S. Air Force Office of Special Investigations (OSI) and Army tactical counterintelligence teams. Both of these multinational organizations made significant contributions to MND-N's collection capabilities by broadening access to certain groups among the Bosnian factions, particularly among those who would not have been overly receptive to meeting with U.S. personnel. Furthermore, the two NATO units did not follow the more stringent U.S. force protection guidelines, enabling them to move more freely in the sector while maintaining a lower profile. Both organizations were full participants in the MND-N weekly HUMINT coordination meetings, accepting tasking from the G2 and fully sharing their reporting. The NATO units significantly enhanced the tactical CI and HUMINT collection

[88]Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield:* p31.

capability within MND-N and provide a sterling example that coalition intelligence operations, when properly integrated and based on mutual trust, can provide broader and more diverse intelligence than could be achieved through unilateral approaches. MND-N's CI/HUMINT architecture demonstrates that multinational intelligence can become something more than just a political expediency to be endured.[89]

Validation

In a true coalition environment, the principle of *plan early and concurrently* is not viable. Four of the five multinational principles are valid and relevant based on the initial coalition experience in Bosnia, 1995-97. The ad hoc nature of a coalition is simply counterfactual to the viability of exploiting this principle. The principle of *make adjustments* and *share all necessary information* will be the linchpin of successful intelligence sharing operations in the future.

CHAPTER FOUR

IV. CONCLUSION

Future operations for the United States Army according to Joint Vision documents will not only be joint but will include allies and coalition partners. Lessons Learned from Bosnia for sharing intelligence indicate that the present challenge is internal versus external.

> Our more technically advanced allies will have systems and equipment that are essentially compatible, enabling them to interface and share information in order to operate effectively with US forces at all levels. However, we must also be capable of operating with allies and coalition partners who may be technologically incompatible-especially at the tactical level.[90]

The author began this research with a belief that the main impediment to sharing operational intelligence was due to policy and doctrine. The research suggests that technological

[89] Melissa E Patrick. *Intelligence in Support of Peace Operations*, 27.
[90] Joint Vision 2020, Washington D.C. 2000.

interoperability within US channels was woefully inadequate due largely to stove-piped system development, for the increased demand for shared operational intelligence. Additionally, it was apparent from the outset that the implementing force would be challenged by the paradigm shift shown in figure 4, and that success in operational intelligence execution would be dependent on how well the force could analyze and absorb the shift. USAREUR made some discoveries along the way. It was necessary to rely on national agencies to provide technology and systems to respond to the operational environment. National agencies can design, procure, and field systems that deal with environments specific shortfalls more rapidly than they can be acquired and deployed in the military system. Sensor-to-Shooter intelligence did not provide a foundation for long-range analysis and did not accurately target the intentions of low-tech belligerents. The proliferation of new systems at the analytic nodes, without additional manning, often increased the load on available resources. There is a need to decrease the number of duplicative systems which are labor-intensive, require long lead times for training, and my not talk to other systems.

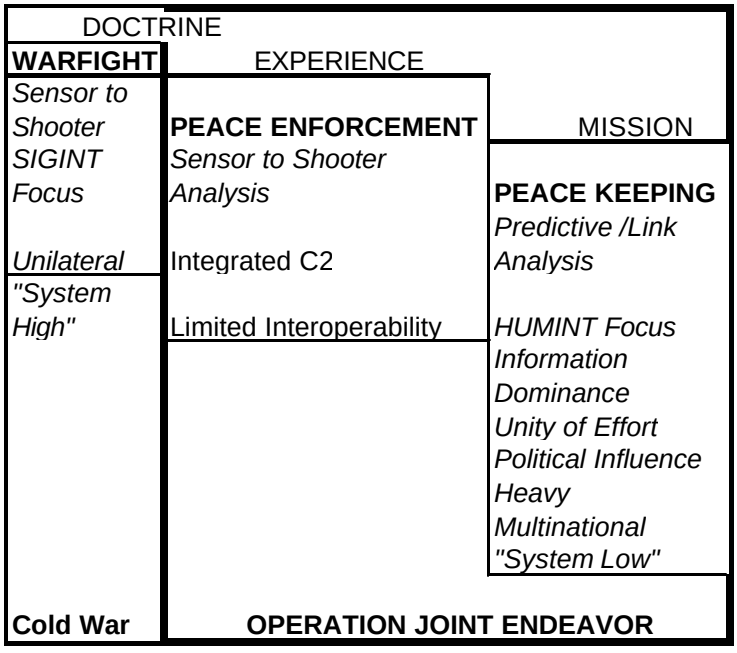


Figure 4: Operational Intelligence Paradigm Shift

The DSB Task Force made a number of critical recommendations for improved operational Intelligence sharing so that users can exploit the increased availability of information without becoming overwhelmed. If realized, their action will no only support our Bosnia war fighters but will support our 21st Century war fighters. Urgent tasks requiring continued and focused attention include proliferating the communications infrastructure and tools to get useful information down to the battalion level. Next, forcing a paradigm shift where higher level intelligence centers become proactive providers of targeted information to the lower level users, and forming collection management teams able to coordinate tasking of national, theater, and organic assets in support of mission objectives.[91]

Progress is still needed in the classification and releasability of combined-joint intelligence information. Operation Joint ENDEAVOR led to great progress in information sharing, even with IFOR nations which a few years ago would never have intentionally received NATO intelligence. It is possible to provide greater information support for the brigade and battalion headquarters. Wider deployment of the Joint Broadcast System (JBS) to combat brigades and battalions would allow pushed/pulled information to reach war-fighters more quickly, especially if the tools and applications were deployed as well to ensure meaningful use of the data, again a doctrinal issue.[92] Information provided to IFOR/SFOR level must be classified at that level in order to be usable within those HQs. If provided a U.S. only or compartmented classification level, the information cannot be acted upon within IFOR/SFOR.

No perfect organizational structure exists that will meet every mission requirement, but we could do better by focusing more on joint and combined operations. The days of Army-only operations are virtually gone. To meet this challenge the intelligence community must adapt.

> We (Intelligence community) need to ensure that we have the systems and training necessary to fight and win on joint and coalition teams. Clearly, the effect on an organization is different as we move higher from brigade level to corps level. Today, however, even a brigade headquarters may need to form an

[91] Defense Science Board, *"Report on Improved Application of Intelligence to the Battlefield:* p 64.
[92] Ibid., 28.

> Army Forces (ARFOR) headquarters requiring joint and possibly Coalition connectivity.[93]

The author in conclusion with the Defense Science Board suggests changes as well and proposes adapting and exploiting the concept of smart push, smart pull. Down at the battalion and brigade levels, commanders cannot afford the extra support staff it would take to have an inherent, robust analytical capability to exploit the information now available from higher echelons. However, an area for further research is addressing the saturation of data and information at the lower levels that would occur if current procedures and systems remained unchanged. The research supports that when sharing operational intelligence in a multinational operation, *Operation Joint Endeavor*, the process can fail because cold war policies and stovepipe system operability hinder effective dissemination in stability and support operations. With few exceptions, the author suggests that the operational intelligence tenets and principles are still relevant for the 21st century; however, the overall effectiveness of multinational operations is dependent on a paradigm shift that is superior to interoperability between organizations, processes, and technologies.

[93] Steve Iwicki, "Generating the Task Force for Combat Intelligence Operations, *Military Intelligence Professional Bulletin*, Volume 26 Number 1, (January-March 2000), p 9.

APPENDIX A- Terms of Reference

Alliance: the result of formal agreements (i.e. treaties) between two or more nations for broad, long-term objectives, which further the common interests of the members; (FM 100-8, The Army in Multinational Operations, p G-0)

Coalition: an arrangement between one or more nations for common action; multinational action outside the bounds of established alliances, usually for single occasions or longer cooperation in a narrow sector of common interest; or a force composed of military elements of nations that have formed a temporary alliance for some specific purpose. (DCID 5/6)

Dissemination: conveyance of intelligence to users in a suitable form (Joint Pub 2-0, II-7)

Intelligence: The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. (DODD 5230.11, para 9)

Multinational operations: is a collective term to describe military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance (Joint Pub 3-0)

Need to Know: a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function (Executive Order 12968, Section 1.1(h))

Operational intelligence: is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations.(Joint Pub 2-0, II-1)

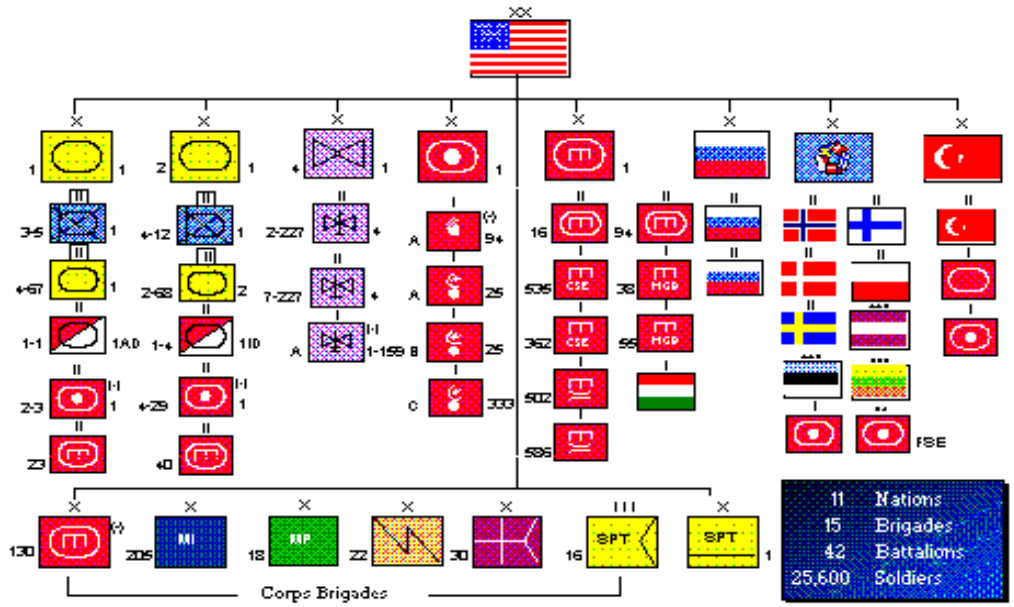
ORCON: it is the most restrictive intelligence control marking, defined as information controlled by originator; dissemination beyond the initiating headquarters requires advanced permission from the originator; ORCON may be used only on classified intelligence that clearly identifies or would reasonably permit ready identification of intelligence sources and methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness; (DCID 1/7)

Sanitation: the process of editing or otherwise altering intelligence information or reports to protect sensitive intelligence sources and methods, capabilities, and analytical procedures in order to permit wider dissemination (DCID 5/6)

Tear Line: is the place on an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and /or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the need to know principle and foreign disclosure guidelines, of the information below the tear line. (DCID 1/7, para 3.5)

APPENDIX B-Organizational Diagrams

FIGURE: 3, Task Force Eagle's Multinational Organization[94]



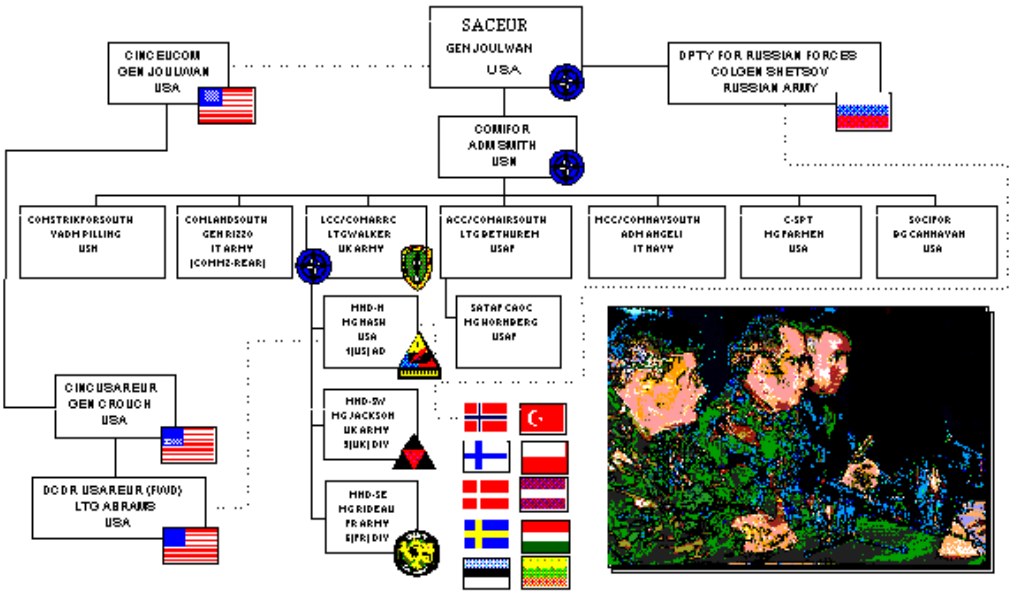


FIGURE 2: IFOR COMMAND AND CONTROL[95]

[94] Center for Army Lessons Learned, *Joint Military Commissions*, Newsletter No. 96-8, p III-5.

[95] Center for Army Lessons Learned, *Joint Military Commissions*, Newsletter No. 96-8, U.S. Army Training and Doctrine Command, Fort Leavenworth, Ks, figure III-1.

BIBLIOGRAPHY

Adams, Thomas K., "The Real Military Revolution", *Parameters*, US Army War College Quarterly vol. XXX, No. 3, Autumn 2000, p. 59

Agee, Collin A., "Joint STARS in Bosnia: Too Much Data Too Little Intel?", *Military Intelligence Professional Bulletin*, October-December 1996, p.8

Boyd, Charles G. "Making Peace with the Guilty: The Truth about Bosnia." *Foreign Affairs* (September/October 1995): 22-38.

Burg, Steven L, and Paul S. Shoup, *The War in Bosnia-Herzegovina: Ethnic Conflict and International Intervention*, Armonk, New York:. M.E.Sharpe, 2000.

Center for Army Lessons Learned. *"BiH National Elections: Tactics, Techniques, and Procedures."* Volume 1. Center for Army Lessons Learned Newsletter 98-18. Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, September 1998.

_____. *"BiH National Elections: Tactics, Techniques, and Procedures*." Volume 2. Center for Army Lessons Learned Newsletter 98-19. Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, September 1998.

_____. *"Draft Lessons Learned Report: Bosnia Contingency Planning and Training; Operations Other than War."* Center for Army Lessons Learned. Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, September 1994.

_____. *Initial Impressions Report: Task Force Eagle Initial Operations: Operation JOINT ENDEAVOR.* Center for Army Lessons Learned. Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, May 1996.

_____. *Initial Impressions Report: Task Force Eagle Initial Operations: Operation JOINT ENDEAVOR.* Center for Army Lessons Learned. Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, September 1996.

_____. *Intelligence Preparation of the Battlefield*. Center for Army Lessons Learned Newsletter 96-12. Center for Army Lessons Learned Fort Leavenworth, KS: US. Army Training and Doctrine Command, December 1996.

_____. *Joint Military Commissions*, Newsletter No. 96-8, Center for Army Lessons Learned Fort Leavenworth, KS, U.S. Army Training and Doctrine Command, , September 1996.

Central Intelligence Agency, Director of Central Intelligence Directive 5/6, *Intelligence Disclosure Policy*. Washington: 30 June 1998.

_____. Director of Central Intelligence Directive 1/7, *Security Controls on the Dissemination of Intelligence Information.* Washington: 15 June 1996.

Clausewitz, Carl von, *On War*, ed. And translated by Michael Howard and Peter Paret (Princeton,

N.J.: Princeton University Press, 1976.

Cuevas, Hector M. Jr, "Collection Management and Imagery Support to Deep Operations in Kosovo", *Military Intelligence Professional Bulletin*, Volume 26, Number 1, The U.S. Army Intelligence Center and Fort Huachuca, January-March 2000,p16.

Defense Science Board, "*Report on Improved Application of Intelligence to the Battlefield: May-July 1996*," Office of the Under Secretary of Defense for Acquisition and Technology, Washington, D.C., July 1996.

Gramer, George K., Jr. "Operations JOINT ENDEAVOR: Combined-Joint Intelligence in Peace Enforcement Operations," *Military Intelligence Professional Bulletin*, October-December 1996, 11-14.

_____. "Optimizing Intelligence Sharing in a Coalition Environment", *Naval War College*, 1999.

Grange, David L. and John S. Rovegno, *Shaping The Environment*, unpublished article submitted to Joint Forces Quarterly, 1997.Article located on LTC Rich Holden's "Standard Intel Data Dump" CD as of 16 March 2000.

Hall, Wayne M., *The Janus Paradox: The Army's Preparation for Conflicts of the 21st Century*, Paper, Interim Brigade Combat Team (IBCT) O&O Concept, Hall, 15 August 2000

Hammond, John C., SFOR Tour Report; Memorandum For the COMSFOR, 4 December 1996 to 26 September 1997. Article located on LTC Rich Holden's "Standard Intel Data Dump" CD as of 16 March 2000.

Headquarters, U.S. Army Training and Doctrine Command, *Force XXI Operations*, TRADOC PAM 525-5 (Fort Monroe, VA: TRADOC), 1 August 1994.

Iwicki, Steve, "Generating the Task Force for Combat Intelligence Operations", *Military Intelligence Professional Bulletin*, Volume 26 Number 1, The U.S. Army Intelligence Center and Fort Huachuca, January-March 2000.

Joint Warfighting Center, *Joint Task Force Commander's Handbook for Peace Operations*. Fort Monroe, Virginia, 16 June 1997.

Knudsen, Harold, "Fire Support for the Nordic-Polish Brigade: An Interoperability Lesson for the Future", *Field Artillery Journal*, May-June 1997.

Machiavelli, Niccolo, "The Prince", translated by W.K. Marriott, Aldine Press for J.M. Dent & Sons LTD, London, 1908.

Olsen, Howard, and John Davis, "Training U.S. Army Officers for Peace Operations: Lessons from Bosnia", *United States Institute of Peace Special Report*, www.usip.org/oc/sr991029nb.html

Patrick, Melissa E. *Intelligence in Support of Peace Operations*, USAWC Strategy Research Project, Carlisle Barracks, PA: U.S. Army War College, 2000.

Rice, Anthony J. "Command and Control: The Essence of Coalition Warfare," *Parameters*, Spring 1997: 152-167.

Scales, Jr. Robert H., "Trust, Not Technology, Sustains Coalitions", *Parameters*, US Army War College Quarterly, vol. XXVIII, No. 4, Winter 1998-99,4-10.

Siegel, Pascale C., *Target Bosnia: Integrating Information Activities in Peace Operations*, Washington D.C. National Defense University Institute for National Strategic Studies 1998.

Shanahan, Stephen W., "Information Operations in Bosnia", *Military Review*, November-December 1997, p 55-57.

Smith, John W., "Essential Stability and Support Operations Planning Factors", *Military Intelligence Professional Bulletin*, Fort Huachuca, Vol 22 No. 4, October –December 1996

U.S. Army Training and Doctrine Command, *"Operations (DRAG Edition) Field Manual 3-0,"* Fort Leavenworth, 15 June 2000, p11-7.

U.S. Department of State, Bosnia Fact Sheet: *Human Rights Abuses in the Balkans*, updated and released by the Bureau of Public Affairs, 11 December 1995

U.S. Department of the Army, *Collection Management and Synchronization Planning, Field Manual 34-2*; Washington, DC, 8 March 1994.

_____. *Peace Operations. Field Manual 100-23*. Washington: 30 December 1994.

_____. *Decisive Force: The Army in Theater Operations, Field Manual 100-7*, Washington 31 May 1995.

_____. *The Army in Multinational Operations, Field Manual 100-8*, Washington 24 November 1997.

U.S. Joint Chiefs of Staff, *Doctrine for Joint Operations* (Joint Pub 3-0) Washington, D.C.: 1 February 1995.

_____. *Joint Doctrine for Intelligence Support to Operations* (Joint Pub 2-0) Washington, D.C.:

_____. *Joint Doctrine for Multinational Operations*, (Joint Pub 3-16) Washington, D.C.:

_____. *Joint Intelligence Support to Military Operations* (Joint Pub 2-01) Washington, D.C.: 20 November 1996

_____. *Joint Task Force Planning Guidance and Procedures*, (Joint Pub 5-00.2) Washington, D.C.: 13 January 1999.

_____. *Joint Tactics, Techniques and Procedures for Foreign Internal Defense, (*Joint Pub 3-07.1) Washington, D.C.: 26 June 1996.

_____. *Joint Vision 2010*. Washington 1997.

_____. *National Intelligence Support to Joint Operations* (Joint Pub 2-02) Washington, D.C.: 28 September 1998.

USAREUR Headquarters *Operation Joint Endeavor After Action Report*, Volume1 & II, May 1997.

Van Creveld, Martin L. *Command in War*. Cambridge, Harvard University Press, 1985.

Waldrop, M. Mitchell. *Complexity: The Emerging Science at the Edge of Order and Chaos*. New York: Simon & Schuster, 1992.

Wentz, Larry K. "Intelligence Operations," in *Lessons from Bosnia: The IFOR Experience*, Edited by Larry K. Wentz, Washington, D.C.: National Defense University, Institute for National Strategic Studies, 1997.