NAVAL WAR COLLEGE
Newport, R.I.

OPTIMIZING INTELLIGENCE SHARING IN A COALITION ENVIRONMENT: WHY
U.S. OPERATIONAL COMMANDERS HAVE AN INTELLIGENCE DISSEMINATION
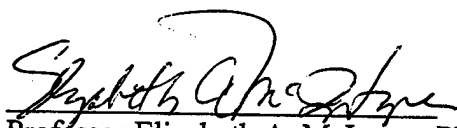CHALLENGE

by

George K. Gramer, Jr.
Colonel, United States Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the re-
quirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by
the Naval War College or the Department of the Navy.

Signature: _Geo K Gramer Jr._

17 May 1999

Professor Elizabeth A. McIntyre, Ph.D.,
Joint Military Operations Department
Faculty Advisor

19991122 190

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	

6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207

8. Title (Include Security Classification): OPTIMIZING INTELLIGENCE SHARING IN A COALITION ENVIRONMENT: WHY U.S. OPERATIONAL COMMANDERS HAVE AN INTELLIGENCE DISSEMINATION CHALLENGE (U)
9. Personal Authors: GEORGE K. GRAMER, JR., COLONEL, U.S. ARMY

10. Type of Report: FINAL	11. Date of Report: 17 MAY 1999

12. Page Count: 33
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.
14. Ten key words that relate to your paper: COALITION, INTELLIGENCE, DISCLOSURE, POLICY, DISSEMINATION, COMMANDER, MULTINATIONAL, DOCTRINE, SHARING, IFOR

15. Abstract: Future U.S. military operations and military operations other than war will almost certainly involve other allied nations or entities. U.S. operational commanders must develop a framework for the dissemination of intelligence information to appropriate recipients in their area of operations.

U.S. policy, particularly DCID 5/6 and NDP-1, provides guidance on intelligence sharing, however joint and service doctrine often makes the operational commander's responsibilities confusing. Of all the elements of the intelligence cycle, optimal intelligence dissemination becomes critical in a multinational environment by enhancing coalition unity of effort and force protection from the planning stage through war termination.

NATO Operation JOINT ENDEAVOUR provided examples of difficulties with intelligence disclosure, among them a lack of timely releasable intelligence, each nation's reliance on its own intelligence capabilities, and the intelligence differences inherent among the nations. Sharing intelligence becomes difficult for the U.S. because of sensitive sources and means, national differences within a coalition, sophisticated technologies, the lack of multi-level security systems, other nations' security programs, and U.S. policy.

While change is difficult, change is necessary. Provisions for tailored releasable intelligence for a coalition must be made as early as possible. U.S. national intelligence agencies are adjusting to that need. Both operational commanders and the national agencies have major roles in the improvement of intelligence sharing in a multinational environment.

16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users

17. Abstract Security Classification: UNCLASSIFIED
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-6461	20. Office Symbol: C

Abstract of

OPTIMIZING INTELLIGENCE SHARING IN A COALITION ENVIRONMENT: WHY U.S. OPERATIONAL COMMANDERS HAVE AN INTELLIGENCE DISSEMINATION CHALLENGE

Future U.S. military operations and military operations other than war will almost certainly involve other allied nations or entities. U.S. operational commanders must develop a framework for the dissemination of intelligence information to appropriate recipients in their area of operations.

U.S. policy, particularly DCID 5/6 and NDP-1, provides guidance on intelligence sharing, however joint and service doctrine often makes the operational commander's responsibilities confusing. Of all the elements of the intelligence cycle, optimal intelligence dissemination becomes critical in a multinational environment by enhancing coalition unity of effort and force protection from the planning stage through war termination.

NATO Operation JOINT ENDEAVOUR provided examples of difficulties with intelligence disclosure, among them a lack of timely releasable intelligence, each nation's reliance on its own intelligence capabilities, and the intelligence differences inherent among the nations. Sharing intelligence becomes difficult for the U.S. because of sensitive sources and means, national differences within a coalition, sophisticated technologies, the lack of multi-level security systems, other nations' security programs, and U.S. policy.

While change is difficult, change is necessary. Provisions for tailored releasable intelligence for a coalition must be made as early as possible. U.S. national intelligence agencies are adjusting to that need. Both operational commanders and the national agencies have major roles in the improvement of intelligence sharing in a multinational environment.

Preface

The author is an Army intelligence officer with over 24 years of active service. He has worked in multinational situations in Korea, Honduras, United States Southern Command, and Bosnia and Herzegovina. He commanded combined units in Korea and Honduras with tactical command (TACOM) over foreign soldiers and civilians. He also served as Director, Combined Joint Intelligence, in the North Atlantic Treaty Organization (NATO) Implementation Force (IFOR) in Sarajevo, Bosnia and Herzegovina, from February to June 1996.

The author thanks the faculty of the Department of Joint Military Operations of the Naval War College, the staff of the Naval War College Library, and the support personnel of the Office of Naval Intelligence Detachment for their assistance.

Table of Contents

I. Introduction

U.S. Intelligence is a national asset to be conserved and protected and will be shared with foreign governments only when consistent with U.S. national security and foreign policy objectives and when an identifiable benefit can be expected to accrue to the United States. It is the policy of the U.S. Government to share intelligence with foreign governments whenever it is consistent with U.S. law and clearly in the national interest to do so.
— Director of Central Intelligence Directive 5/6[1]

Military operations and military operations other than war in the 21st Century that involve the United States will almost certainly involve other allied nations and entities as well. The operations may include alliance partners, coalition members, or non-governmental organizations from the United States, the United Nations, or other countries. These future operations will require the sharing[2] of intelligence information.

Current U.S. joint and service doctrine alludes to the commander's responsibility to establish a framework for the dissemination of intelligence information. There is much doctrinal guidance and policy, sometimes contradictory or at least confusing, that 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).[3]

Existing joint and service doctrine provides neither the specificity nor the easily understood detail required for the operational commander to establish and conduct intelligence disclosure with foreign entities.[4] Much of this policy is classified, so unclassified generic examples of specifics are used in this paper.

The bottom line is that U.S. joint doctrine glibly declares intelligence dissemination to be a commander's responsibility yet provides little substantive assistance or guidance to

the commander to accomplish that mission. The confusing joint doctrine and regulatory guidance adds to the difficulty the operational commander faces.

This paper will analyze the issues associated with intelligence disclosure and release to coalition partners, particularly in light of recent U.S. military operations in Bosnia. With this analysis in hand, the author will then suggest ways for the operational commander to optimize actions in this complicated arena. Finally, the paper will include improvements for the National Intelligence Community[5] policies governing intelligence sharing that would improve the position of the operational commander in this critical area.

How Can Disclosure Impact Operational Success?

Gathering and disseminating intelligence can have a major impact on successful coalitions. Planning and preparations must provide timely military intelligence to all partners. The degree of dissemination will undoubtedly vary depending on the individual member. In ad hoc coalitions the United States may be operating with partners with whom there is a reluctance to share intelligence, especially when it might reveal sensitive sources or collection methods.[6]

The operational commander is responsible for all that is done or fails to be done with regard to planning and executing major operations and campaigns. Among his intelligence responsibilities, the operational commander must define intelligence support needs. He must ensure that service component and joint collection, processing, production, and dissemination occurs successfully.[7] When an operation includes multinational players, the operational commander gains an inherent command responsibility to ensure that intelligence disclosure to those multinational participants is optimized.

In multinational operations, a shared situational awareness of the battle space is necessary for unity of command or unity of effort, mission deconfliction, and avoidance of duplication of effort.[8] The timely dissemination of perishable tactical and operational intelligence to the forces involved is a mission imperative. Multinational headquarters and forces

will need to use releasable intelligence to accomplish their estimates, plans, orders, targeting, battle damage assessment (BDA), and maneuver activities. Shared situational awareness will enhance early warning and force protection (to include provisions for the protection of non-military personnel in the area of operations). Shared awareness will also improve the coalition's ability to defend against the adversary's counterintelligence, espionage, sabotage, terrorism, and deception threats. All of these are key to the success of any plan or operation.

Achieving a multinational shared awareness will not be without difficulty. "During peace operations, free exchange of information between military forces of different nations may not exist. This causes nations to conduct regional analysis independently which may not support (the commander's) overall plan."[9] Building consensus is a critical element of effective multinational operations. Without satisfactory levels of intelligence disclosure, the communications used for intelligence fusion or even the coalition headquarters could become off-limits to many coalition members. Proper levels of disclosure will enhance the cooperation and coordination of operational activities within the headquarters and throughout the coalition area of operations. It will enhance the credibility of the United States with the allied nations and non-governmental organizations operating in the area of operations.

Besides, English may not be the primary language of the majority of the coalition forces, and in some cases, the U.S. will not be in the lead for a given operation. The critical shortage of U.S. linguists will often require the augmentation by coalition partners of U.S. intelligence collection and processing units or translation, interpretation, or interrogation teams, thus requiring intelligence disclosure.

The bottom line is that the commander must ensure that the process for intelligence disclosure fully supports multinational operational needs and maximizes dissemination of releasable intelligence throughout the area of operations.

Current U.S. Disclosure Policy

We are continuing to adapt and strengthen our alliances and coalitions to meet the challenges of an evolving security environment. ... We assist other countries in improving their pertinent military capabilities, including peacekeeping and humanitarian response. With countries that are neither staunch friends nor known foes, military cooperation often serves as a positive means of engagement, building security relationships today that will contribute to improved relations tomorrow.
—A National Security Strategy for a New Century[10]

Both NDP-1 and DCID 5/6 provide three general criteria concerning foreign disclosure: that it be consistent with U.S. foreign policy and national security objectives, that it clearly benefit the United States, and that its release is not likely to be harmful to the United States.[11]

Joint Chiefs of Staff Joint Publications and service doctrine direct operational commanders to prepare for the dissemination of intelligence information to foreign entities. The challenge for the commander and his staff is that most of these doctrinal publications direct the commander to disclose intelligence successfully, yet provide little help or guidance on the specifics to accomplish that task.[12]

These admonitions from the Joint Staff and the services seem to oversimplify the reality of a very complex requirement. Operational commanders cannot merely wave their hand and magically receive tailored, releasable intelligence with which to conduct a multinational operation. Rather, the commander and his staff must start early to ensure that the coalition's intelligence sharing needs are met.

II. Analysis

A Background Case Study: IFOR

Intelligence is one of the hardest things to share in a coalition environment. 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. Furthermore, there are differences in national doctrine and disclosure rules. For IFOR, there was some confusion as to roles and responsibilities and duplication of effort. In spite of this, the coalition members were willing to cooperate and share information. The nations shared intelligence to a remarkable degree and certainly beyond most expectations.[13]

When the North Atlantic Treaty Organization (NATO) and allied coalition partners banded together in 1995 to establish the NATO Implementation Force (IFOR), Headquarters IFOR experienced multiple problems with intelligence disclosure. This section will enumerate difficulties in sharing intelligence as derived from historical accounts of IFOR's first year.[14] The subsequent section will then analyze reasons why these problems may occur in any multinational force having U.S. participation.

In IFOR, releasable intelligence was initially in scant quantity, and often was not timely. Releasable intelligence reporting throughout IFOR by all participants often tended to be redundant. In many cases, the same releasable information was reported by different headquarters multiple times over a span of several days. Releasable signals intelligence was particularly untimely. The coordination draft of Joint Pub 3-16 recognized these problems, "the usefulness of intelligence information to the Multinational Force Commander is directly proportional to its timeliness and accuracy, especially in targeting and maneuver."[15] Additionally, releasable national and multinational intelligence had very little analysis applied to it by the originators.

Intelligence collected by exclusively national sources often seemed to be siphoned off into national command channels; in most of those instances, the intelligence was never shared with the coalition. The low-level coalition intelligence that remained was information

at the lowest common denominator. Thus, the U.S. commander of one of the multinational divisions relied heavily on the U.S. intelligence structure that was more responsive to his needs and provided greater detail. This situation was symptomatic of U.S. frustrations in a coalition environment when control of the intelligence process was not entirely in U.S. hands.

The extent to which nations were willing to share information with NATO and coalition partners was initially unclear. One area that varied across the IFOR operation was information sharing. Theater plans did not elaborate responsibility and sanitization procedures of sensitive national information.

A U.S. National Guard officer serving in IFOR stated, "not only did we have to establish guidelines for passing information, but we also had to learn to gather and assimilate intelligence from ... very different organizations...."[16] NATO intelligence doctrine states that in peacetime, NATO commanders have to rely on member nations for the intelligence they need. In wartime, the majority of NATO commanders' intelligence may still come from the member nations; however, they will also acquire intelligence from many different sources and agencies such as assigned combat units, reconnaissance units, and aircraft. The NATO and non-NATO IFOR participants developed their national intelligence capabilities as they were accustomed, whether robust or minimal. For example, the U.S. deployed more than a brigade of intelligence personnel to the theater, while some nations brought no organic intelligence capabilities whatsoever. Also, there was no single doctrine for multinational intelligence operations or intelligence architecture. In the first year, each nation developed its own ad hoc approach to establish the foundation on which IFOR and its successor organization later built a more successful multinational intelligence operation.

However, intelligence sharing was sometimes a one-way street. NATO and many of the NATO nations had not yet made the change that the U.S. intelligence community had begun in terms of more open sharing. For example, the Allied Rapid Reaction Corps (ARRC) G2, a British officer, released information strictly on a "need to know" basis. This conflicted with U.S. doctrine of shared situational awareness and broadcast intelligence.

Thus in the first year of NATO operations in Bosnia, the intelligence system was plagued by a lack of timely, releasable intelligence; nations' reliance on their exclusive national systems; and distinct differences in the ways each nation conducted intelligence activity, to include dissemination.

Analysis of Why U.S. Intelligence Sharing is Complex

An information-rich environment is thus a sharing environment. That needn't mean an environment without standards, rules, conventions, and ethical codes. It does mean the standards, rules, conventions, and codes are going to be different from those created to manage the zero-sum bargains of market trading and traditional international relations.[17]

Many institutional issues in the United States government make intelligence sharing a difficult task. The principal reason used for non-disclosure of U.S. intelligence is the sensitivity of collection sources and methods. Since World War II, the U.S. has used technologically sophisticated technical means and has employed sensitive human and other sources for the collection of the most sensitive intelligence information. In a multinational operational environment, sharing as much operational and tactical intelligence information as possible has great merit, as long as sources and methods receive protection from harmful disclosure.

Intelligence disclosure to any individual – foreign or domestic – is based on the recipient's clearance for the level of intelligence information to be received and whether that potential recipient has a "need-to-know." In a coalition, a sliding scale of risk may also apply -- from most to least secure:

> --U.S. personnel
> --America-Britain-Canada-Australia (ABCA) personnel
> --Alliance personnel
> --Coalition personnel
> --Totally or partially U.S. non-government entities (Non-governmental organi-
> zations, private voluntary organizations, United Nations relief agencies, and
> international organizations)
> --Totally non-U.S. non-government entities

Even within the categories of "alliance personnel" and "coalition personnel," there may be extensive differences in the attitude the U.S. may have concerning the disclosure of intelligence information. For example, in IFOR, members of the former Warsaw Pact operated side-by-side with U.S. and other NATO personnel. As a result, NATO used multiple layers of disclosure (U.S. only, NATO releasable, and IFOR releasable). U.S. Army doctrine indicates why such a policy caused difficulty:

> *(F)orces will need to share intelligence information to some degree. This may involve sharing intelligence information with military forces of nations with which we have no intelligence-sharing agreements or sharing intelligence that is not covered by existing agreements. In some cases, we may have existing agreements that discriminate among allies within the multinational force. For example, our standardized exchange systems with NATO nations may create friction where we have NATO and non-NATO partners in a peace operation.[18]*

Another issue is that of reciprocity. DCID 5/6 and NDP-1 indicate the need for national benefit; in some instances that will involve a *quid pro quo* relationship. In a multinational coalition, there will be four possibilities in any bilateral disclosure agreement:

> (1) intelligence the U.S. will share
> (2) intelligence the other nation will share
> (3) intelligence the U.S. will not share
> (4) intelligence the other nation will not share

Optimally, the largest amount of tactical and operational intelligence will fall into categories (1) and (2).

A comparative study by Loch Johnson contrasts the ways in which intelligence organizations around the world accomplish their missions. He cites several features of U.S. intelligence that make our system different. In contrast to most nations, the U.S. has a large number of intelligence personnel deployed worldwide; many of them have a high degree of technical capability. That technical capability often results in a need for protection that inhibits multinational dissemination. Additionally, the U.S. system has a high degree of accountability and ethics.[19] The U.S. characteristics contrast with Canada. Because of Canada's limited personnel and technological assets, small budget, and lesser status as a world power, the country actively seeks a two-way exchange of intelligence in a safe and constructive manner with other nations such as the U.S. and UK.[20]

Another difficulty in sharing arises from U.S. sophistication in technology and automation. The U.S. proliferates classified intelligence fusion, collection, and dissemination systems (for example, Joint Deployable Intelligence Support System (JDISS), Joint Worldwide Intelligence Communications System (JWICS), All-Source Analysis System (ASAS), LOCE {within NATO}, Scaleable Transportable Intelligence Communications System (STICS), etc.) Not all coalition partners can use or afford U.S. technology, and the U.S. will not want to share all of its advanced technology with all elements of a coalition.[21] Communications capabilities, to include the cryptologic systems required for the secure transmission of communications, may not be able to be disseminated to all coalition participants.

Additionally, lack of multi-level security in systems will complicate the intelligence sharing picture. Such a capability would allow the combination of intelligence having multiple classification levels and releasability within the same system. Access to any given piece of information within the system would be restricted to only those with appropriate clearance

9

and "need to know." "A multi-level security system does not currently exist that can easily facilitate sanitization and dissemination of intelligence to U.S. and allied and/or coalition operational commanders."[22] Until we attain that important technical capability, sharing via U.S. technical systems will be difficult or will always require the physical presence of U.S. personnel at the system computer terminal.

U.S. concerns for security of our intelligence are valid, since different nations have entirely different personnel, physical, electronic-computer, and CI/HUMINT threat security programs. Joint Pub 2-01 outlines the security that is to be afforded U.S. intelligence released to a foreign entity.[23] Although the foreign governments are required by doctrine to afford security equal to that of the U.S., it is difficult to believe that will always be the case. Likewise, other coalition members' security concerns come into play.[24] Finally, the complexity and length of U.S. intelligence and security regulations directing security, intelligence transfer, and disclosure make it difficult for the operational commander to sort out the details easily and clearly.[25]

Arguments for the Status Quo

Selective release of intelligence of all varieties has for some time been a tool of the U.S. in the geopolitics of the modern world.... However, decisions to provide U.S. intelligence information to foreign countries is a national-level decision made after careful consideration of the effects of such release.[26]

Change is difficult. In light of recent spy cases and the loss of sensitive national defense intelligence information to unwanted foreign recipients, there will likely be dissent to any further drastic changes to simplify or ease national disclosure policy. The continued protection of sources and methods will be paramount and is logical.

There is no need, however, to provide extensive intelligence information to coalition partners. What is required is <u>sufficient</u> releasable intelligence information to allow all multi-

national participants to accomplish the mission successfully. Clearly everything should not be releasable – the coalition or alliance does not need 100 percent of the available U.S. national intelligence. The coalition requires tailored, viable, timely, sharable tactical and operational intelligence information. Sanitized information should safeguard and protect lives, information sources, and operations.

On a positive note, national intelligence agencies have already made internal changes to accommodate intelligence support to military operations, and as a by-product, intelligence sharing. Both the CIA and NSA have flag-rank deputy directors for military support. Also the intelligence community has banded together in support of the National Intelligence Support Team (NIST) concept, in which the agencies deploy qualified personnel to military operations in direct support of the operational commander and his staff's intelligence needs. Leveraging releasability through the NIST enhances intelligence dissemination.

Therefore, as difficult as it is to change a bureaucratic system, there has been positive practical progress from the national agencies in support of the operational commanders. It is possible to change when the situation demands change.

III. Recommendations

How Can the Operational Commander Improve Intelligence Sharing?

The success of any crisis deployment hinges on the existence of a reliable system ... for gathering, analyzing, and disseminating strategic and tactical intelligence.
—*General H. Norman Schwarzkopf*[27]

As complex as intelligence dissemination is, the operational commander can take positive steps to optimize multinational intelligence sharing. A thorough understanding will enhance the commander's capability and ensure that dissemination is maximized without exceeding regulatory or policy restrictions.[28]

11

Personal involvement: While Army doctrine states, "the supporting CINC can make a major contribution to the deploying commander simply by ensuring at the outset that intelligence is decompartmented and releasable to multinational units,"[29] that is not within the operational commander's nor the CINC's authority; the power rests at DCI level. For that very reason, operational commanders must become personally involved with the issues concerning intelligence disclosure. Joint Pub 3-16 states, "The senior U.S. officer needs to become personally concerned with the issues of intelligence sharing and releasing of information early in the process."[30]

Standardization: Despite the lack of a single intelligence doctrine for multinational operations, standardization is essential. Potential multinational headquarters must take that into consideration and develop peacetime missions and functions statements and standing operating procedures (SOPs) that support the information sharing requirement.[31] Extensive coordination may compensate for a lack of established procedures, but it would be far better if that coordination were effected by qualified intelligence liaison personnel.[32]

Planning and training: Early in the planning for an operation, the commander needs to obtain any necessary additional national guidance for intelligence disclosure; his J2 will not, on his or her own, have the authority necessary to get the favorable guidance needed. He must ensure that his J2 staff has developed appropriate and complete intelligence disclosure procedures. He must continuously train, develop, and exercise his staff in this function. A most important link is the training and qualification of the Designated Intelligence Disclosure Officer (DIDO) on the J2 staff. In preparation for the possibilities of conflict or military operations other than war, the command should include intelligence disclosure as an element of

the intelligence annex of all Concept Plans (CONPLANS) and Operations Plans (OPLANS) developed.[33]

Personnel augmentation: Prior to deployment, the commander should also request personnel augmentation, particularly for the foreign disclosure staff and the combined intelligence production element to expedite the sanitization and sharing of applicable intelligence.

Coalition intelligence organization: The commander must tailor the coalition to make best use of the intelligence capabilities each coalition member nation brings. The operational commander must flexibly adjust for differences and adapt to the complementary nature of the capabilities of each coalition partner.[34] He must strengthen unity of effort through establishment of a combined-joint intelligence element and intelligence processing center. That will foster intelligence cooperation and sharing and create a central focus for all multinational intelligence requirements. Since all coalition member nations will have unique intelligence strengths and weaknesses; by maximizing this synergy, the commander will optimize intelligence capabilities throughout the coalition.[35]

Dissemination and liaison: As part of the overall communications architecture, the command must develop a rapid system for the transmittal of releasable intelligence information.[36] Use of a releasable system will strengthen the coalition's ability to disseminate intelligence information throughout the area of operations and to the majority of command and control headquarters. The assignment of intelligence liaison personnel in all multinational headquarters will also help to bridge problems associated with the transmittal, disclosure, and understanding of releasable intelligence.[37] By making the command's intelligence processing center multinational in character, the intelligence contributions of all multinational partners will be enhanced, and many dissemination problems may be resolved quickly.[38]

Use of the National Intelligence Representatives: Each agency in the National Intelligence Community will likely provide a senior, qualified command representative to the CINC. During operations, the national intelligence community will provide a small National Intelligence Support Team (NIST) comprised of personnel from the agencies' headquarters who will work in direct support of the operational commander. The commander must maximize the utility of the national intelligence community representatives during the planning and early execution phases of an operation. Once the operation is ongoing and the NIST is in theater, the commander must exploit its capability as a crucial direct link back to the national intelligence agencies to obtain and provide tailored releasable intelligence for the coalition.

Intelligence Reporting Techniques: The national intelligence representatives, the NIST, and the combined-joint intelligence element and intelligence processing center can ensure that reportable intelligence uses releasability techniques such as tear lines and portion markings to provide a separation of the releasable intelligence from the non-releasable. They can also ensure that theater intelligence producers classify products at the lowest level possible. Commanders should also ensure that units in theater maximize unclassified operational and informational reporting.[39]

Leadership and influence: Finally, in his leadership role the operational commander or CINC must influence multinational coalition members to share their nation's intelligence as fully as possible with the coalition in support of the greater coalition goals.

How Can the National Intelligence Community Improve

Intelligence Sharing?

Expanded military support: There has been significant progress to correct the disconnect between military and civilian intelligence cultures. Examples include the creation of

the flag officer positions in CIA and NSA and the establishment of NIST teams. National

agencies must continue to provide high quality CINC representatives and NIST members

who maintain a military focus and who are attuned to the requirements of intelligence disclo-

sure.[40] CIA, in developing a post Cold War mission, clearly has increased their support to

military operations, as evidenced in the "Guidelines and CONOPS for U.S. Intelligence

Sharing with IFOR" published in late 1996 which expedited the dissemination of releasable

intelligence products.[41]

Policy guidance: The national agencies must develop tailored disclosure guidance in

support of military operations, improving on the generic nature of current guidance. Agency

Representatives to the CINCs can help coordinate applicable disclosure requirements in

CONPLANS and OPLANS for theater contingencies. The National Intelligence Community

must keep NDP-1 current, especially the disclosure charts. They can also ensure other policy

documents focus on the needs for military operations, to include thorough agency staffing

review of Joint Pubs.[42] Providing clear, understandable regulatory and doctrinal guidelines

for intelligence disclosure is perhaps the best means to assist the operational commander and

his staff.

Multi-level security development: The U.S. must move ahead as quickly as possible

with the development of multi-level security systems. When this technical capability is per-

fected, it will enhance not only multinational intelligence support, but also all manner of op-

erations and special operations capabilities by allowing users to access only that information

for which they are cleared and have the "need to know."

Alternative intelligence sources and methods: National agencies must also investi-

gate the use of alternative, less-classified sources for intelligence such as commercial im-

agery and the use of techniques such tear lines, portion markings, and sanitized releasable photo imagery.[43]

Minimize ORCON reporting: ORCON is the most restrictive intelligence control marking. Its dissemination beyond the initiating headquarters requires advanced permission from the originator, since its unauthorized release could make the adversary aware of technical penetration or an irreplaceable human source. Where it is possible, national agencies could improve the utility of ORCON material to the multinational operational commander by concurrent dissemination of ORCON with a releasable tear line section. This would eliminate the requirement to consult the originating headquarters for a sanitized version. This will expedite intelligence information to the multinational force and reduce the time lag that would otherwise inhibit multinational use of the intelligence.

Leadership and influence: As was the case with the operational commander and the CINC, the National Intelligence Community may be able to influence multinational intelligence sharing based on their existing liaison relationships with the intelligence agencies of the coalition partners.

The National Intelligence Community recognizes that major difficulties still exist in the dissemination of intelligence in a multinational environment. The operational commander and his staff must continue to work closely with the National Intelligence Community to improve intelligence sharing to the fullest extent possible from the start to the finish of every operation, and then capture that progress in changes to future policy and procedures.

IV. Concluding Thoughts

It is not enough just to be joint when conducting future operations. We must find the most effective methods for integrating and improving interoperability with allies and coalition partners. Although our Armed Forces will maintain decisive unilateral strength, we expect to work in concert with allied and coalition forces in nearly all of our future operations, and increasingly, our procedures, programs, and planning must recognize this reality.
—Joint Vision 2010[44]

Before intelligence sharing is optimized in a multinational force, there are challenges for the U.S. operational commander and his staff to overcome. He must be able to understand the policy and procedural difficulties inherent in intelligence sharing, take aggressive proactive measures within his command to enhance intelligence sharing capability, apply the J2 staff and national agency representatives' talents to the maximum extent possible, incorporate the best of each coalition member's intelligence capabilities within the command, and always be flexible enough to overcome unexpected difficulties.

Therefore, the operational commander in close coordination with the National Intelligence Community must make every effort to optimize intelligence sharing in multinational force operations correctly, quickly and effectively. Commanders and staffs must begin efforts now to be as ready as possible to accomplish intelligence sharing successfully during future operations. Consistent with existing U.S. national policy and national security considerations, operational commanders and their staffs can thereby leverage the power of releasable intelligence to serve as a combat multiplier in multinational military operations and military operations other than war.

Notes

[1] Central Intelligence Agency, Director of Central Intelligence Directive 5/6, Intelligence Disclosure Policy (Washington: 1998), paragraph 2-a.

[2] There are nuances of difference in the terms "sharing," "disclosure," "dissemination," "release," etc. Appendix A provides the definitions for selected terms used in this paper.

[3] Because DCID 5/6 and NDP-1 represent the crux of national policy concerning intelligence disclosure, Appendix B provides a brief synopsis of the contents of each document.

[4] For example, Joint Pub 3-0 states that the collection production, and dissemination of intelligence as "a major challenge." (VI-10) Joint Pub 2-01 directs, "Resolve foreign disclosure and/or release procedures" (II-11) as one of dozens of elements of Crisis Action Planning. That same Joint Pub misnames NDP-1 in its list of references (J-2). Among the multitude of references that either require the operational commander to accomplish intelligence disclosure or which tell him how to accomplish it are 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 5200.1-R, DoD Directive 5230-11, NDP-1, Joint Pub 2-0, Joint Pub 2-01. Joint Pub 2-02, Joint Pub 3-0, Joint Pub 3-07.1, Joint Pub 3-07.3, Joint Pub 3-16, Joint Pub 5-00.2. Field Manual 100-20, and Field Manual 100-23. The complete publication data on each is provided in the bibliography.

[5] The National Intelligence Community is headed by the Director of Central Intelligence (DCI) and includes, among others. the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the National Security Agency (NSA), and the National Imagery and Mapping Agency (NIMA). The four agencies listed are the most critical to the issues of intelligence disclosure discussed in this paper.

[6] Terry J. Pudas, "Preparing Future Coalition Commanders," Joint Force Quarterly, Winter 1993-94, 42.

[7] For a complete discussion of intelligence support to operations, see Joint Pub 2-0.

[8] Michael I. Handel points out that disclosure enhances unity of effort, which extrapolates to the intelligence situation in a multinational organization. He writes, "Excessive secrecy in handling information poses a related problem. Perhaps the most obvious symptom of this problem is the compartmentation within and among intelligence organizations, as well as between the intelligence community and other military and civilian agencies. Consequently, one organization often is not privy to the information held by another, an arrangement that may bring about failures to act, duplication of effort, or the inadvertent interference of one agency in the operations of another." Michael I. Handel, "Strategic Surprise: The Politics of Intelligence and the Management of Uncertainty," in Intelligence: Policy and Process ed Al-

fred C. Maurer, Marlon D. Tunstall, and James M. Keagle (Boulder: Westview Press, 1985), 264-265.

[9] Joint Warfighting Center, <u>Joint Task Force Commander's Handbook for Peace Operations</u> (Fort Monroe, VA, 1997), VII-2.

[10] William J. Clinton, <u>A National Security Strategy for a New Century</u> (Washington, D.C., 1998), 13.

[11] Central Intelligence Agency, DCID 5/6, Appendix A. Appendix B to this paper provides a synopsis of DCID 5/6 and NDP-1.

[12] See note four for the partial listing of national, joint, and service documents impacting the operational commander.

[13] Larry K. Wentz, "Intelligence Operations," in <u>Lessons from Bosnia: The IFOR Experience</u> ed Larry K. Wentz (Washington, D.C.: National Defense University, Institute for National Strategic Studies, 1997), 53.

[14] This section derives examples of intelligence dissemination problems in IFOR from three sources: George K. Gramer, Jr., "Operations JOINT ENDEAVOR: Combined-Joint Intelligence in Peace Enforcement Operations," <u>Military Intelligence Professional Bulletin</u>, October-December 1996, 11-14; Wentz, <u>Lessons from Bosnia</u>, 53-118 (particularly pages 53, 89, 91-94, and 115); and Joint Warfighting Center, Chapter VII.

[15] Joint Chiefs of Staff, <u>Joint Doctrine for Multinational Operations</u> (Joint Pub 3-16) (Washington, D.C.: Final Coordination 2 September 1997), III-4-III-5.

[16] Joint Warfighting Center, VII-7.

[17] Harlan Cleveland, "Educating for the Information Society," in <u>Challenges and Opportunities from Now to 2001</u> ed Howard F. Didsbury, Jr. (Bethesda: World Future Society, 1986), 271.

[18] Department of the Army, <u>Peace Operations</u>, Field Manual 100-23 (Washington: 1994), 47.

[19] Loch K. Johnson, "Strategic Intelligence: An American Perspective," in <u>Security and Intelligence in a Changing World New Perspectives for the 1990s</u> ed A. Stuart Farson, David Stafford, and Wesley K. Wark (London: Frank Cass, 1991), 47-48.

[20] Christopher O. Spencer, "Intelligence Analysis Under Pressure of Rapid Change: The Canadian Challenge," undated, <http://www.hil.unb.ca/Texts/jcs/bin/get.cgi?directory=S96/articles/&filename=spencer.html> (9 April 1999).

[21] Wentz, <u>Lessons from Bosnia</u>, 115.

[22] Joint Chiefs of Staff, Joint Intelligence Support to Military Operations (Joint Pub 2-01) (Washington, D.C.: 20 November 1996), IV-2.

[23] Ibid., E-4-E-5.

[24] The following four examples depict aspects of other nations' concerns:

"(S)ome U.S. intelligence personnel become frustrated when their Republic of Korea (ROK) counterparts cannot share all of their information due to security constraints. The ROK military is very security conscious in dealing with ROK-produced classified information and employs very stringent measures in handling classified or sensitive documents." Robert E. Goodson, Jr., "Working on a Combined Staff in the Republic of Korea," Military Intelligence Professional Bulletin, January-March 1999, 9.

"Collecting, disseminating, and sharing intelligence [with multinational forces] is made difficult by the fact that each nation imposes its own operational and electronic protection measures on its forces." Joint Chiefs of Staff, Joint Task Force Planning Guidance and Procedures (Joint Pub 5-00.2) (Washington, D.C.: 13 January 1999), VI-6.

"Free exchange of intelligence information between military forces of different nations may not exist. This lack of free exchange may cause nations to conduct regional analysis independently, a practice that may not support the JTF's overall plan." Ibid., VI-10.

"Nations which offer forces as part of a coalition will almost certainly have their own operational intelligence capability. To some extent, these countries will establish connectivity in order to provide their national intelligence to their forces. However, intelligence capability and interests will vary widely. Indeed, many nations will not have had an intelligence interest in the coalition theater of operations prior to joining the coalition...much less an intelligence interest designed to support military operations." Stephen R. Sadler, "Intelligence Support to Coalition Warfare Is There a Welcome Mat at the Green Door?," (Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1993), 14.

[25] Extensive regulatory guidance appears in both DoD Directive 5230.11 and DoD Directive 5200.1-R which together represent 132 single-spaced printed pages. A partial listing of the many actions required by the operational commander and his intelligence staff appears on pages E-4 to E-6 of Joint Pub 2-01.

[26] Sadler, 6.

[27] Joint Pub 2-01, IV-1.

[28] One helpful piece of instructional guidance is "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations" (CJCS Instruction 5221.01), which delegates limited intelligence disclosure authority to the CINCs and allows further delegation to subordinate commanders whenever appropriate. Nonetheless, it still requires the CINC or operational com-

mander to follow NDP-1 except to disclose the imminence of war or under actual or imminent hostilities to disclose information the commander considers essential for a foreign government's support of combined military operations. The delegation does not give the commander *carte blanche*, but does clarify the CINC's abilities under NDP-1. It also provides special delegation to USCINCSPACE, USCINCPAC, USCINCSOC, and USCINCSO to disclose specifically identified intelligence relevant to their commands.

[29] FM 100-23, 45.

[30] Joint Pub 3-16, III-3.

[31] Writing about their experiences in combined Operation DESERT THUNDER (involving Combined Task Force-Kuwait – CTF-K), Colonels Moore and Boll state, "CENTCOM support in the technical area of foreign disclosure was another success story. Early deployment of a functional area expert from the CENTCOM unified command staff eased the way for a frank intelligence exchange among all the Coalition partners. A trailblazing foreign disclosure standing operating procedure (SOP) has been incorporated into the CTF-K command and control process. Common sense and cooperation are standard in the CTF-K intelligence system." They echo the ideas put forward in Joint Pub 3-16 Coordinating Draft, page III-3, although Joint Pub 3-16 only "suggests" what Moore and Boll says to do as a matter of course. William R. Moore and Kenneth H. Boll, Jr., "Intelligence for the Coalition: The Story of Support to Coalition Task Force-Kuwait," Military Intelligence Professional Bulletin, January-March 1999, 6.

[32] Concerning this, Joint Pub 3-16 states, "Within alliances, it is common for intelligence procedures, practices, and standardized agreements to be established and tested prior to actual use. Coalitions, however, are frequently ad hoc organizations, created and disbanded relatively quickly. It is imperative therefore to compensate for the lack of standardization through coordination." Joint Pub 3-16, III-5.

[33] Concerning this, Joint Pub 3-0 states, "(Joint Force Commanders) need to determine what intelligence may be shared with the forces of other nations early in the planning process. The limits of intelligence sharing and the procedures for doing so need to be determined during initial coordination and negotiation between senior political and military representatives from member nations." Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3-0) (Washington, D.C.: 1 February 1995), VI-10.

Joint Pub 2-0 recommends, "Solutions to problems should be developed and tried before they are required for actual operations so doctrines and procedures are not left to a trial and error methodology during combat." Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations (Joint Pub 2-0) (Washington, D.C.: 5 May 1995), VIII-3.

Army doctrine indicates, "Situations exist where intelligence should be shared with NGOs outside usual political-military channels. Therefore, these operations require policy and dissemination criteria and authority for each instance. At the outset, intelligence planners should establish a decompartmentation cell--provided by the Defense Intelligence Agency

(DIA). Other special intelligence arrangements for multinational operations may include a single director of intelligence and combined intelligence centers." FM 100-23, 47.

[34] Joint Pub 2-0 states, "Intelligence efforts of the nations should be complementary. Because each nation will have intelligence system strengths and limitations or unique and valuable capabilities, the sum of intelligence resources and capabilities of the nations should be available for application to the whole of the intelligence problem." Joint Pub 2-0, VIII-5.

[35] See also Michael Herman, Intelligence Power in Peace and War (Cambridge: Cambridge University Press, 1996), 208-212, for a more extensive discussion of national differences.

[36] Joint Pub 3-16, III-5.

[37] Joint Pub 3-07.1 states that, "An active intelligence liaison should be ongoing between the Host Nation, Country Team, and combatant commander's intelligence staff, thus establishing the basis for any intelligence and communications sharing." Joint Pub 3-07.1, IV-20.

Joint Pub 2-0 suggests, "Intelligence liaison among commands and among supporting and supported organization should be used to bridge problems of understanding between cultures, languages and terms, doctrines and methodologies, and operational intelligence requirements." Joint Pub 2-0, VIII-5

[38] Concerning the intelligence processing center, Joint Pub 3-16 states, "Intelligence processing centers should be multinational in character, service the MNFC (Multinational Force Commander) but also recognizing intelligence that has value in support of national missions. However, establishment of these multinational processing centers, particularly in the case of ad hoc coalitions, will require extensive personal involvement and support from the MNFC and his nation in order to make this a functioning reality." Joint Pub 3-16, III-5.

Joint Pub 2-0 indicates, "Where there is a multinational command, a multinational intelligence center should be established so that the commander, the C-2, and staffs have the facility and capability for developing multinational intelligence requirements statements and for acquiring and fusing the nations' intelligence contributions. The Multinational Intelligence Center should include a representative from all nations participating in the multinational operations." Joint Pub 2-0, VIII-5.

[39] This was a problem for IFOR in 1996: "Progress is still needed in the classification and releasability of combined-joint intelligence information. Operation JOINT ENDEAVOUR led to great progress in information sharing, even with IFOR nations which a few years ago would never have intentionally received NATO intelligence. Today, we should foresee continued combined and coalition operations and plan for future releasability based on that reality. Also, NATO appears to be strengthening its post-Warsaw Pact role in Europe. We must have policies and procedures in place to ensure the widest dissemination of all available intelligence information among the sixteen NATO partners." Gramer, 14.

[40] Michael Herman warns, "Intelligence employs ordinary people, in large numbers and with wide varieties of skills and expectations. There is still a high proportion of lifetime careers in single organizations. The most distinctive feature of the organizational culture is intelligence's secrecy and the sense of difference and mystique it produces. Secrecy combines with long-term employment to produce high but slightly brittle morale." Herman, 384.

[41] Lessons from IFOR says the following of the CIA CONOPS: "the Director of Central Intelligence (DCI) commissioned a task force in early 1996 to examine the release and dissemination of U.S. intelligence in support of IFOR. Recommendations from this task force led to the enactment of a new DCI directive and concept of operation titled "Guidelines and CONOPS for U.S. Intelligence Sharing with IFOR." The intelligence dissemination principles in the 1996 revision of DCI Directive 1/7 placed greater U.S. emphasis on the direct dissemination of IFOR-releasable intelligence products and reporting from the U.S. national level. The intent of the directive was to ensure that the majority of U.S. theater-level operational and situational intelligence for force protection and threat warning was produced not only at the U.S. system high level but also at the REL NATO and REL IFOR level. Production at these levels would allow coalition-tailored products to be provided directly to the theater coalition command staffs at the ARRC and IFOR. Alternatively, products could be placed directly on the LOCE network or air-gapped to the Task Force Eagle (the U.S.-led multinational division) IFOR independent LAN (local area network). As a result, the dissemination of releasable operational intelligence could be made directly to IFOR members without obtaining permission from Washington. Coalition intelligence support and threat warning could be near real-time, as the majority of initial sanitation [sic] and tailoring work was done at the U.S. national level prior to transmission." Wentz, Lessons from Bosnia, 91-92.

[42] For example, the "Checklists for the Multinational Force Commander" in Joint Pub 3-16, Appendix A, lack any specificity about intelligence disclosure requirements. Joint Pub 5-00.2, VI-19 identifies only three items on the checklist for JTF J2 multinational interaction. All joint publications need to be more realistically honest and pragmatic about the difficulties and challenges of intelligence disclosure. The national intelligence agencies must ensure the Joint Pubs are reviewed thoroughly during staffing to avoid misconceptions, omissions, and errors.

[43] The Tofflers believe "Consumer Services for War" will expand technology and intelligence capabilities, particularly commercial off-the-shelf intelligence capabilities, to many nations. Alvin Toffler and Heidi Toffler, War and Anti-War (New York: Warner Books, 1993), 219-220.

[44] John M. Shalikashvili, Joint Vision 2010 (Washington: 1997), 9.

Bibliography

Aftergood, Steven. "Secrecy and Accountability in U.S. Intelligence," Center for International Policy, Seminar on Intelligence Reform, 9 October 1996, <http://www.us.net/cip/secrecy.htm> (9 April 1999).

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

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

Chairman Joint Chiefs of Staff, Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations, CJCS Instruction 5221.01. Washington: 29 September 1995.

Cleveland, Harlan. "Educating for the Information Society," in Challenges and Opportunities from Now to 2001, Edited by Howard F. Didsbury, Jr. Bethesda: World Future Society, 1986.

Clinton, William J. Executive Order, "Access to Classified Information," Federal Register (2 August 1995), 12968.

_____. A National Security Strategy for a New Century. The White House, October 1998.

Goodson, Robert E., Jr. "Working on a Combined Staff in the Republic of Korea," Military Intelligence Professional Bulletin, January-March 1999, 7-8.

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

Handel, Michael I. "Strategic Surprise: The Politics of Intelligence and the Management of Uncertainty," in Intelligence: Policy and Process, Edited by Alfred C. Maurer, Marlon D. Tunstall, and James M. Keagle. Boulder: Westview Press, 1985.

Herman, Michael. Intelligence Power in Peace and War. Cambridge: Cambridge University Press, 1996.

Johnson, Loch K. "Strategic Intelligence: An American Perspective," in Security and Intelligence in a Changing World New Perspectives for the 1990s, Edited by A. Stuart Farson, David Stafford, and Wesley K. Wark. London: Frank Cass, 1991.

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

Moore, William R. and Kenneth H. Boll, Jr. "Intelligence for the Coalition: The Story of Support to Coalition Task Force-Kuwait," Military Intelligence Professional Bulletin, January-March 1999, 4-6, 52.

Pudas, Terry J. "Preparing Future Coalition Commanders," Joint Force Quarterly, Winter 1993-94, 40-46.

Reagan, Ronald. Executive Order, "United States Intelligence Activities," Federal Register (4 December 1981), 12333.

Sadler, Stephen R. "Intelligence Support to Coalition Warfare Is There a Welcome Mat at the Green Door?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1993.

Shalikashvili, John M. Joint Vision 2010. Washington: 1997.

Spencer, Christopher O. "Intelligence Analysis Under Pressure of Rapid Change: The Canadian Challenge." undated. <http://www.hil.unb.ca/Texts/jcs/bin/get.cgi?directory=S96/articles/&filename=spenc er.html> (9 April 1999).

Toffler, Alvin and Heidi. War and Anti-War. New York: Warner Books, 1993.

U.S. Department of the Army. Peace Operations. Field Manual 100-23. Washington: 30 December 1994.

U.S. Departments of the Army and the Air Force. Military Operations in Low Intensity Conflict. Field Manual 100-20/Air Force Pamphlet 3-20. Washington: 5 December 1990.

U.S. Department of Defense. Disclosure of Classified Military Information to Foreign Governments and International Organizations. DoD Directive 5230.11. Washington: 16 June 1992.

_____. Information Security Program. DoD Directive 5200.1-R. Washington: January 1997.

U.S. Department of State. "National Disclosure Policy A Primer on the Process," Defense Trade News, April 1994, <http://jya.com/dtn0494.htm> (7 April 1999).

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.: 5 May 1995.

_____. Joint Doctrine for Multinational Operations (Joint Pub 3-16) Washington, D.C.: Final Coordination 2 September 1997.

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

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

_____. Joint Tactics, Techniques, and Procedures for Peacekeeping Operations (Joint Pub 3-07.3) Washington, D.C.: 29 April 1994.

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

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

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.

_____. "Unifying the Analysis of Bosnia C3I Lessons Learned," <http:www.dodccrp.org/bosnia.htm> (7 April 1999).

Appendix A – Terms of Reference

Alliance: the result of formal agreements between two or more nations for broad, long-term objectives which further the common interests of the members (Joint Pub 3-16, vii)

Coalition: an ad hoc arrangement between two or more nations for common action (Joint Pub 3-16, vii)

Disclosure: showing or revealing classified intelligence, whether orally, in writing or in any other medium, without providing the recipient with a copy of such information for retention (DCID 5/6)

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

Information: unprocessed data of every description which may be used in the production of intelligence (Joint Pub 2-0, GL-8)

Intelligence: the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas (Joint Pub 2-0, GL-8)

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 (EO 12968, Section 1.1(h))

ORCON: intelligence control marking meaning "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; it is the most restrictive intelligence control marking (DCID 1/7)

Release: providing the recipient of classified information with a copy, whether in writing or any other medium, of such information for retention (DCID 5/6)

Sanitization: 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)

Sharing: activities involving the disclosure or release of intelligence (DCID 5/6)

Tear Line: the place in 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 of the information below the tear line (DCID 1/7)

Appendix B – Synopsis of DCID 5/6 and NDP-1

DCID 5/6 of 30 June 1998 establishes policy for disclosure and expands on previous guidance. The directive declares intelligence a U.S. national asset and provides several means to protect U.S. intelligence information. It authorizes designated representatives of heads of departments and agencies of the Intelligence Community to have Designated Intelligence Disclosure Officers (DIDOs). DIDOs execute DCI disclosure policy within their agency, service, or command.

DCID 5/6 also provides three general criteria for the appropriateness and suitability of disclosure:

      (1) that it be consistent with U.S. foreign policy and national security objectives

      (2) that it clearly benefit the United States

      (3) that its release is not likely to be harmful to the United States

It lists categories of what may and may not be disclosed and dictates certain procedures, to include record-keeping provisions. While referencing other policies, DCID 5/6 takes precedence over all other disclosure policies, to include NDP-1.

"National Disclosure Policy" and NDP-1 are the short titles for "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations." NDP-1 provides regulatory guidance governing the disclosure of classified information to foreign governments and representatives thereof through specifically designated personnel (e.g., DIDOs), who may disclose or deny classified military information in accordance with the provisions of the national disclosure policy. Its authority derives from the Under Secretary of Defense for Policy who is responsible for disclosure by the U.S. military.

NDP-1 identifies eight categories of intelligence eligible for disclosure. Of those eight, Category 5 (*Combined Military Operations, Planning, and Readiness.* Information necessary to plan, assure readiness for and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises.) and Category 8 (*Military Intelligence.* Military intelligence comprises information of a military character pertaining to foreign nations and areas as delimited by the criteria for the disclosure of intelligence.) are the most germane to disclosure as discussed in this paper.

NDP-1 also contains two sets of charts. The first set displays the maximum classification levels within each category of classified military information that may be released to the listed foreign governments or organizations. The second set of charts indicates the dates the United States entered into a General Security of Information Agreement with the countries concerned, the date an Industrial Security Agreement was concluded, the date the last NDP Committee Security Survey was completed, and the date of the last CIA Risk Assessment.

28

NDP-1 declares that disclosure criteria must be consistent with U.S. foreign policy and national security objectives concerning the proposed recipient foreign government. That occurs when:

      (1) the recipient government cooperates with the U.S. in pursuance of military and political objectives that are compatible with those of the U.S.

      (2) a specific U.S. national purpose, diplomatic or military, will be served

      (3) the information will be used in support of mutual defense and security objectives