AU/ACSC/0362/97-03

THE INTEGRATION OF OPERATIONS AND INTELLIGENCE

GETTING INFORMATION TO THE WARFIGHTER

A Research Paper

Presented To

The Research Department

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Maj. Mark E. Miller

March 1997

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense.

Contents

Page

Illustrations

Page

Preface

As the world prepares to enter the twenty-first century, the role of the United States and its military forces will undoubtedly have a significant impact. Our armed forces have recognized the need to become more “purple” in nature as the dwindling defense dollars have driven the requirement to improve the efficiency of our operations through joint measures. It is not enough for us to improve in our joint operations; we must also get better in interagency cooperation. The integration of Operations and Intelligence is one way to improve in this arena. In this paper I will attempt to identify ways to accomplish this daunting task.

I would like to sincerely thank Lt Col Gary “Mo” Morgan for his help with this research topic. His unique qualifications in both the Ops and Intel communities are rare and his guidance has been superb. I would also like to acknowledge the efforts of a small group of people at the National Security Agency. Mr. Rob Schrier and the GRANDSLAM Team have been working for the past five years to push the valuable intelligence data collected by the national community to the lowest tactical level. His efforts, and the work of his team, have taken great strides at making the “green door” one that operators are finally getting to peek behind.

Abstract

Getting combat information in a timely manner from the stovepipes of the intelligence world to the operators that require has been a problem for years. The process is not one that will improve unless *both* the Operations and Intelligence communities make a concerted effort to understand each other better. In this paper I will use a combination of primary and secondary sources, along with personal interviews, to establish a historic recap of both good and bad examples of Ops/Intel integration. I will then examine the current intelligence cycle and attempt to identify critical links between it and the operations world. These links will be the key in creating a synergy between Ops and Intel that is critical if the two disciplines are to be *integrated* effectively. The goal of the cycle should be to ensure that the final intelligence product accomplishes the objective it was initially intended for; that is, get pertinent information to the warfighter in a timeframe and format for him to exploit it. At this point it will become apparent that there are certain roadblocks that must be overcome in order to accomplish the previously stated goal. Identifying these roadblocks is only half of the problem. Offering reasonable solutions is the other half. My goal in the final portion of this paper is to do exactly that. I will offer simple cost-effective solutions aimed at dismantling some of the Ops/Intel integration roadblocks. In this age of shortened time-lines and information overload, the Ops/Intel team that works best together will own the "information high ground." This is an objective that is critical to success on the battlefield of tomorrow.

Chapter 1

Introduction

Know the enemy and know yourself; in a hundred battles you will never be in peril.

—Sun Tzu

The success of the US led coalition against the world's fourth largest military during Desert Storm has been characterized as a "textbook" military operation. The war provided the opportunity for the US to demonstrate its technological dominance in a new era of warfare. The devastating combination of stealth, precision weapons, and information dominance produced a lopsided victory that could not have been predicted by even the most optimistic planners in the Pentagon. Despite the outcome of the Gulf War, many in the US military have expressed their disappointment with the role of the intelligence community. General Schwarzkopf's post-war testimony to Congress stated that the "intelligence community as a whole did a great job, he felt that he, as a theater commander, was not well served."[1] In addition, commanders characterized much of the Desert Storm intelligence as "irrelevant to the operational commander and designed for high level policy makers."[2] Should the blame for perceived disconnects between the operations community and the intelligence world be levied solely on the intelligence community? A closer examination of the Ops/Intel relationship must be performed before we can answer this question.

Joint Publication 2-0, Joint Doctrine for Intelligence Support states that one of the basic principles of intelligence is to "synchronize intelligence with operations."[3] This principle leads one to believe that operations and intelligence functions are separate and occur independently. This is entirely incorrect. It is, however, prevalent in the minds of many operators and members of the intelligence community. Instead of synchronizing intelligence and operations, we should be making strides to *integrate* the two disciplines. *Webster* defines integration as the process to "make whole or complete by adding or bringing together parts."[4] This mentality encourages development of a team that will strive to accomplish a common goal. The profession of arms is a serious business that cannot afford to tolerate anything less than total unity of effort in matters directly affecting its operations.

In order to best integrate the operations and intelligence worlds a systematic approach must be taken. History has provided numerous examples of successful (as well as unsuccessful) military operations that can be directly tied to inputs provided by intelligence sources. A review of some of these operations will provide some common links that were (or were not) used to create a synergy between Ops and Intel and directly affected the results of the operation. We must then use these links and apply them to the intelligence cycle to determine where they have the largest impact. An analysis of these links and their relationship to the intelligence cycle will identify some inherent roadblocks to effectively integrating Ops and Intel. These roadblocks not only exist in the Intel community, but, in the Ops community as well. The key to breaking through these roadblocks lies in the combined education of the Ops and Intel communities. Intelligence personnel must become "smarter" in their knowledge of military operations and predict

what level of support will be required. As the US military moves into the twenty-first century it will be required to perform "more with less." It is not enough for the intelligence community to improve its support to military operations; the operations community must do its part to communicate focused requirements that must be satisfied within the intelligence cycle. This can only be accomplished by understanding the capabilities of the intelligence community as well as the limitations. Operators must make a dedicated effort to include their Intel counterparts in all aspects of planning and execution and stop the process of using Intel to "fill gaps" in the plan. The frequently observed "just tell me what I need to know" attitude must disappear. Only then will Ops and Intel be integrated into a truly efficient team.

Notes

[1] Thomas A. Kearney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report,* (Washington, D.C.: Government Printing Office, 1993), 121.

[2] Lt Col Ronald J. Norman, "The Intelligence Road to Recovery" (AWC research paper, April 1995), 22.

[3] Joint Pub 2-0, *Joint Doctrine for Intelligence Support to Operations,* 5 May 1995, ix.

[4] *Webster's New World Dictionary of the American Language,* (New York, N.Y.: The World Publishing Company, 1972), 732.

Chapter 2

Historical Perspectives of the Ops/Intel Interface

> *Historical examples clarify everything and also provide the best kind of proof in the empirical sciences.*
>
> —Carl von Clausewitz

In order to develop an effective gameplan to integrate Ops and Intel better, we must envision what our desired "end-state" will look like. A comparison of historic examples will portray the levels of integration that have occurred in the past and allow us to identify certain links between Ops and Intel that must be strengthened.

Operation Desert Storm

The lightning tempo of operations during Desert Storm identified two major weaknesses in the support provided by the intelligence community. The first major disconnect surfaced during Desert Shield as CENTAF began planning an offensive air campaign against Iraq. The CENTAF commander, Lt Gen Charles A. Horner, established a compartmentalized group of Ops planners known as the "Black Hole" to conduct this planning.

> Due in no small part to the political sensitivity of offensive campaign planning at this early juncture, the Black Hole planners set themselves up as a special access organization and made little effort to inform intelligence personnel of their concept of operations. CENTAF intelligence went ahead with its own target planning and viewed initial requests from Black Hole

> planners as a nuisance. When intelligence personnel failed to respond expeditiously to their initial requests, the Black Hole regarded them as generally nonresponsive and looked elsewhere for support. Thus began an unfortunate rift between theater intelligence organizations and the Black Hole, a gap that widened as time went on.[1]

Black Hole planners set up direct contact with national intelligence agencies in Washington and simply bypassed CENTAF Intelligence for the remainder of the campaign. "The Black Hole's ready access to targeting intelligence from national intelligence agencies had the unfortunate effect of cutting Central Command J-2 and CENTAF Intelligence out of the communication loop."[2]

The second major Ops/Intel disconnect concerned battle damage assessment (BDA). Black Hole planners developed their high priority target list with the assumption that BDA would be timely enough to task restrikes, should they be required, within 48-72 hours. Considering the 72 hour Air-Tasking Order (ATO) cycle, this meant that the planners were demanding near real-time combat assessment of executed strikes.

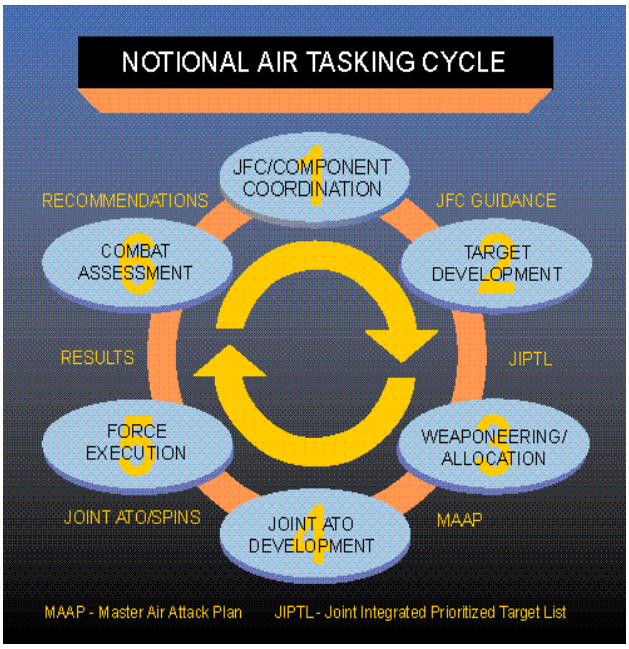

Figure 1. ATO Cycle

Not only was this an unrealistic assumption on the planners' part, the requirement and rationale were not communicated to theater intelligence personnel until Desert Storm kicked off. This misunderstanding stemmed directly from a lack of capability knowledge on the part of the planners and a failure to fully grasp the significance of the ATO cycle on the part of the Intel personnel.

> Collection managers had to set priorities for the imagery collected from limited assets, but these managers often had not taken part in target planning, nor were they aware of changes to the daily air tasking order. Furthermore, Black Hole planners were unfamiliar with collection tasking procedures and did not attend meetings of the coordinating boards that assigned priorities to collection lists. This meant that people not involved in planning the air campaign and unaware of its direction determined each day's reconnaissance requirements.[3]

These Desert Storm examples vividly display the gap between Ops and Intel from an education perspective. This is a link that must be strengthened if we are to effectively integrate Ops and Intel.

Attack on the USS Liberty

Desert Storm was an example of a major regional conflict that resulted in an overwhelming military victory despite the aforementioned problems between Ops and Intel. The 1967 attack by Israeli aircraft and gunboats on the USS *Liberty* was a tragic example of what can result if Ops and Intel are not on the same sheet of music. The USS *Liberty* was a modified "Victory" ship assigned to the US Navy's Atlantic Fleet. Officially designated as an Auxiliary General Technical Research vessel, it is accepted knowledge today that the mission of the *Liberty* was communication intercept and analysis.[4] The crew was composed of 294 men of which all but three were American sailors. The additional three crewmembers were civilians from the National Security Agency (NSA). The US

Navy's Sixth Fleet maintained operational control of the *Liberty* and NSA maintained technical control. On the 8th of June 1967, the *Liberty* was patrolling in the Mediterranean Sea off the Gaza Strip when she was attacked by Israeli fighters and torpedo gunboats. Just hours prior to the attack, the *Liberty* commander, Captain William McGonagle, had been assured by the Sixth Fleet Commander that he would be provided jet aircraft support within ten minutes in the "unlikely" event of an "accidental" attack.[5] The USS *America* and USS *Saratoga* carrier battle groups were less than 100 miles from the *Liberty*.

As the *Liberty* came under fire at 1158Z she immediately began making distress calls to the carrier battle groups. Neither carrier was prepared to respond. The only aircraft ready to launch from either carrier were nuclear loaded alert F-4s on the *America*. Four of these F-4s were launched to aid the *Liberty*. All were recalled by the Pentagon upon learning of their configuration.[6] Seventy-five minutes later the attack was over. Thirty-four Americans were dead and 171 wounded. The Israelis apologized for the attack and claimed that they had mistaken the *Liberty* for an Egyptian tanker. Numerous sailors on the *Liberty* confirmed the presence of the US flag and reported that the Israelis had made several low reconnaissance passes prior to the attack. The next day Israel launched its ground offensive in the Six Day War. The lack of resources capable of responding to the *Liberty* attack from the carrier battle groups make it clear that the operations personnel in those battle groups did not fully grasp the capabilities of the resource they had agreed to protect. Apparently the Israeli Ops/Intel team did not suffer from the same problem.

World War II—Battle of Midway

Not all previous experience between Ops and Intel has been negative. The force enhancing capabilities of correctly applied intelligence can produce significant operational advantages over a lesser informed enemy. Such was the case in the Pacific during WW II. After its remarkable success in attacking Pearl Harbor in December 1941, Japan hoped to secure key strategic islands in the Pacific to set the stage for a quick and decisive victory over the US Navy. This would guarantee free access to the sea lines of communication and open the door for a possible invasion of Hawaii. The American government might then be forced to sue for peace on Tokyo's terms. Midway Island was the key to the Japanese plan and an attack was planned for the summer of 1942.

> Unknown to the Japanese, however, US Navy cryptologists in Hawaii were having success in intercepting and breaking the Japanese Navy's encoded communications. As a result, American forces knew in advance Japan's intent to attack Midway and its plans for doing so. Armed with that intelligence, Admiral Nimitz ambushed the Japanese armada north of the island on June 4, destroying four enemy carriers and, in the process, virtually eliminating Japan's ability to carry out further, large scale operations in the Pacific. The Battle of Midway was a decisive defeat for the Japanese and a turning point in the war; it ended any hope on Japan's part that the war could be won quickly, if at all.[7]

The technical knowledge of the cryptologists, along with the operational understanding on their part of the strategic significance of Midway Island, allowed them to intercept and deliver critical information to Admiral Nimitz. Armed with this information, Nimitz employed his air assets to complete the integration process and defeat the Japanese fleet.

Operation Peace For Galilee–1982

A more recent example of the powerful force enhancing capabilities of the Ops/Intel team was demonstrated in the Middle East in 1982. In the largest single air battle of the

second half of the twentieth century, the Israeli Air Force (IAF) devastated the Syrian Air Force on 9 June 1982. To support Operation PEACE FOR GALILEE, the IAF's mission was to neutralize Syrian SA-6 sites and destroy reacting enemy fighters. At every level planning and execution were enhanced by accurate intelligence. In the one-year period following the April 1981 introduction of SA-6 missiles into the Bekaa Valley, Israeli military intelligence had focused on the new surface-to-air threat. Their collected data allowed aircrews to rehearse the strike missions in the Negev Desert against highly accurate replicas of the missile sites. On the day of the attack, Syrian airspace was scanned by E-2C surveillance aircraft flying off the Lebanese coast. A Boeing 707 signals intelligence platform monitored Syrian communications and radar activity. With F-15 and F-16 pilots flying combat air patrols, IAF F-4s armed with SHRIKE anti-radiation missiles, and F-16s loaded with standoff Maverick missiles and conventional munitions attacked 19 SA-6 sites and several SA-2 and SA-3 sites.

In a superb example of real-time intelligence application, the IAF strike commander monitored the ongoing operation from video provided by forward orbiting Scout and Mastiff remotely piloted vehicles. On the first day of the air campaign, 17 SA-6 sites were destroyed along with several SA-2 and SA-3 installations. On 9 June, the Israelis downed 23 Syrian MiG-21s and MiG-23s. On 10 June they shot down 15 more MiGs. By the end of September, Israeli pilots had destroyed 29 surface-to-air missile sites in seven raids, 85 Syrian MiGs, and had lost only two IAF aircraft to enemy ground fire.[8] This Ops/Intel team produced results that would have been unachievable without effective integration.

History has provided us with countless examples of failures and successes stemming directly from the level of cooperation between Ops and Intel. The previous examples are

just a few. We must now examine the intelligence cycle to determine where the greatest impact of effective integration can be made.

Notes

[1] Thomas A. Kearney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report,* (Washington, D.C.: Government Printing Office, 1993), 129-130.

[2] Ibid., 133.

[3] Ibid., 141.

[4] James M. Ennes Jr., "USS Liberty Homepage," n.p.; on-line, Internet, 15 January 1996, available from http://www.halcyon.com/jim/ussliberty/liberty.htm.

[5] Ibid.

[6] James M. Ennes Jr., *Assault on the Liberty,* (New York: Ivy Books, 1979), 89-92.

[7] Abram N. Shulsky, *Silent Warfare*, (New York: Brassey's, 1993), 30.

[8] Benjamin S. Lambeth, "Moscow's Lessons from the 1982 Lebanon Air War," in *War in the Third Dimension: Essays in Contemporary Airpower*, ed. R. A. Mason (London: Brassey's Defense Publishers, 1986), 127-148.

Chapter 3

The Intelligence Cycle

> *What is called "foreknowledge" cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation..*
>
> —Sun Tzu

In order to effectively support the warfighter, intelligence products must be accurate, timely, and usable. "Accuracy is the prime principle of military intelligence. With accurate intelligence, all aspects of strategic, operational, and tactical planning and execution proceed on the basis of fact. Without accurate intelligence on the enemy's location, capability, and intent, planning is an unfocused and wasteful exercise, and execution may result in defeat."[1] Accuracy is a relative term, though. If increasing the accuracy of a product causes excessive delays in getting the information to the user, it simply becomes highly accurate, but unusable, "news." Different levels of operational users have different accuracy and timeliness criteria. The F-16 pilot being engaged by an SA-6 is much more concerned with timeliness than the operational planner sitting in an air-conditioned facility. The planner, however, cannot task an F-117 to target a critical radar facility without accurate target coordinates regardless of how quickly he receives the information. Only through an understanding of the particular operational user and his requirements, will intelligence be able to satisfy these specific needs effectively. Raw data collected by an

intelligence source is rarely in a useable format for the operator. "The intelligence cycle is the process by which information is converted into intelligence and made available to users."[2] Joint Pub 2-0 lists the five steps in the intelligence cycle as planning and direction, collection, processing, production, and dissemination (see Figure 2).

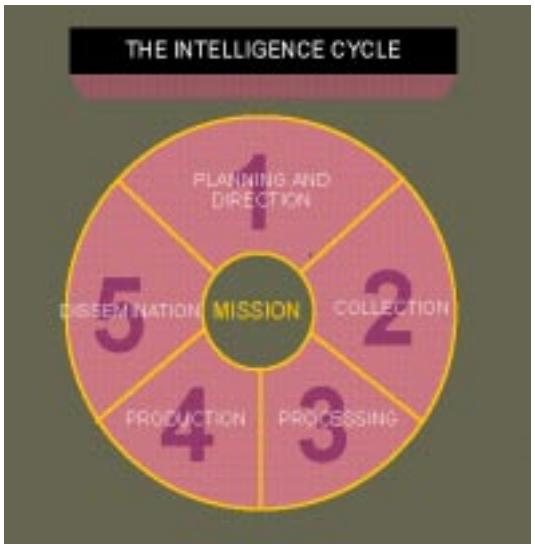

Figure 2. The Intelligence Cycle

The publication also differentiates between information and intelligence by stating that the application of critical analysis transforms information into intelligence. At times it appears that this cycle is not being completed in a timeline that meshes with operations. According to the former director of the Defense Intelligence Agency (DIA), Major General Clapper:

> Intelligence simply must situate itself within the operational cycle rather than outside it. In other words, the intelligence collection, production, and dissemination cycle must be compressed so that it fits within the operational cycle for targeting to support strike and restrike operations.[3]

With this point in mind, it is important to look at the intelligence cycle and relate each step back to operational requirements to ensure that the cycle is in fact integrated effectively.

Planning and Direction

This step involves establishing command relationships between intelligence elements and identifying, prioritizing, and validating intelligence requirements.[4] This must be accomplished at all levels of command for the intelligence cycle to work smoothly. It is critical that the intelligence personnel (J-2) and the operations staff (J-3) establish a solid working relationship. The J-2 and his staff must understand the missions they are supporting and anticipate requests for information. It is equally critical for Ops planners to keep Intel informed. Even in the most sensitive operations, such as the Black Hole planning, an Intel representative must be included from the beginning. Failure to do so could result in an unrecoverable deterioration of the working relationship, as was the case in Riyadh. This cooperative relationship must go all the way down to the wing and squadron level. Squadron and wing Intel personnel must be familiar enough with the operational missions of their unit to anticipate the need for national level support should it be required. Operators must also be familiar with the capabilities of national systems to optimize their requests for intelligence products. The planning and direction phase of the intelligence cycle is the most critical phase in the Ops/Intel integration process. Failures in this step will cascade throughout the process and ensure that the best team does not take the field.

Collection

The collection step in the intelligence cycle provides the link between the tactical and theater level requirements and national support. “Collection includes both the acquisition of information and the provision of this information to processing and/or production

elements."[5] The J-2 must be aware of all available collection resources. This is the responsibility of the collection manager. The theater collection manager must know exactly what collection assets are assigned to the theater and can be tasked directly to fill an operational requirement. The collection manager and the J-2 staff must also have access to national databases to determine if the requested information is already available. National databases will be discussed in-depth during the dissemination phase. If information is not available, and assigned assets cannot provide the requested information, collection managers must be familiar with national systems' capabilities and the tasking procedures to receive the information in a timely manner. It is very important for the collection manager to understand the *required* accuracy and timelines of the requested information. If a high degree of accuracy is required, and time permits, the collection manager should task multiple resources to verify and improve the accuracy of the final product. If, on the other hand, timeliness is critical, the collection manager may elect to task only the fastest resource and accept a less accurate product. This information must be clear in the original request from the initiating unit.

Despite the critical role played by theater collection managers, the intelligence community has not placed a high enough priority on training individuals in this role. The following excerpt from the Gulf War Airpower Survey reinforces this assertion:

> Although regulations and operations plans detailed organizational structures to handle tasking of national reconnaissance assets, the system did not work well in practice because of inadequate numbers of trained, qualified personnel. To complicate matters further, only a small portion of those assigned to CENTAF intelligence during the crisis had any experience in collection management.[6]

The commitment to produce and train more collection managers from within the Intel community, combined with national system capabilities and limitations training to Ops, will significantly fill this void in the future.

Processing

This step in the intelligence cycle involves converting information and data into formats that can be readily used by intelligence personnel.[7] This is primarily a technical step that does not require integration with Ops.

Production

This step is the final packaging of information into a deliverable intelligence product. Production involves the integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence. This step is frequently termed "intelligence application." A principle guideline in intelligence application is to focus on the purpose and use of the intelligence. The producer needs to know who will use the intelligence and at what level.[8] Much has been done to institutionalize the production of intelligence in recent years, but, not enough has been done to integrate the analyst and the operator/user. "Institutional solutions have the advantage that they can be implemented top-down through managerial decisions and directives; they do not, however, attack the heart of the problem of intelligence failures, the thought process of the individual analyst."[9] Intelligence producers are too often guilty of pushing as much information forward for fear of being accused of "withholding" important information.

> The problem lies in a systematic orientation that favors data flow over user needs. This at least partially explains the debate between intelligence and operations over the intelligence system's Desert Shield/Storm performance.

> That is, intelligence delivered "tons" of information as fast as possible (IN's self-imposed measure of merit), while operations wanted specific "pounds" of it delivered much more quickly than the system was capable of.[10]

In order to attack this problem, intelligence analysts from the squadron level to the national level must learn as much as possible about the operations they support. This will allow them to focus their products better and eliminate the potential for information overload while improving the quality of what is produced.

Dissemination

Dissemination is the process of conveying intelligence information to users in a suitable form. This information can be delivered in many forms and by numerous methods. Each intelligence dissemination method can be categorized as secure or nonsecure, over dedicated or common user communications, and as either raw or finished intelligence.[11] The majority of intelligence in the past was disseminated by the traditional "push" system. That system was based on intelligence products flowing from the producer to the headquarters level and then on to the unit(s) that the headquarters felt needed it or, in some cases, the unit that requested it. As discussed in the production phase of the cycle, the analyst that produces the intelligence must be familiar with the user's needs. The push method of dissemination is designed such that the producer is frequently multiple levels above the user and cannot possible fully understand the user's needs. This significantly contributes to unusable products and an overload of irrelevant information that has to be deciphered at the unit level. This process is time consuming and cumbersome.

Dissemination of intelligence products is the phase in the intelligence cycle that is experiencing the greatest amount of change in today's information era. Technology is

allowing intelligence producers to disseminate information much faster and to increasingly lower levels in the military. Technology is also allowing dissemination to move away from the push method and towards a "smart push" or "pull" method. The smart push method allows users to receive broadcast intelligence data in a form that they choose. The Air Force's Constant Source is one method of receiving this information. The smart push method allows units to set filters and manipulate receivers to customize their displays. An example of a broadcast currently available is the Tactical Information Broadcast Service (TIBS). The TIBS broadcast takes multiple producers ranging from the tactical to the national level and combines them using a centralized management point. The TIBS manager then masks the source to protect sensitive producers, and broadcasts the results over secure communications at the Secret level. Examples of some of the information in a typical TIBS broadcast include ground threats, air situation information, and ship locations. Individual units can then set their filters to receive certain desired information. For example, filters can be set to display surface-to-air missile (SAM) acquisition radar signals, filter out early warning radars, and display SAM targeting radar signals along with an associated alarm.[12] The most important thing for operators and unit level intelligence personnel to grasp about smart push broadcast information is the capabilities *and limitations* of the intelligence collectors themselves. An SA-6 displayed on the planned ingress route should be avoided if possible; a clear ingress route, however, does not guarantee a milk run!

"Smart push" offers vast improvement over the traditional "push" dissemination system and is quickly being augmented by an even better "pull" system. The Air Force is currently fielding a new intelligence workstation called Combat Intelligence System (CIS).

CIS is an integrated intelligence workstation that not only provides access to near-real-time signals intelligence and enemy order of battle data, but also includes the standard Joint Defense Intelligence Support System (JDISS) software. This will allow units to pull information directly from air component command's, theater, and national databases. This "pull" capability will carry over to imagery products contained in the databases, greatly improving response time for target imagery.[13] The future of dissemination improvements will include the Global Broadcast Service (GBS). GBS uses the latest phased-array antenna technology and provides a DOD version of the commercial Direct Broadcast System. GBS will provide units with imagery, weather, unmanned aerial vehicle (UAV) video, threat and targeting data, and ATO access. GBS will allow an ATO that took hours to be passed in Desert Storm to be received in less than one second.[14] Clearly the intelligence cycle's dissemination system is improving to the point that operators cannot afford to remain ignorant of the collection system's capabilities and limitations.

The intelligence cycle points out many areas that Ops and Intel need to integrate better to become a lethal team. Technology is improving the capability for the intelligence producer to get information to the user in near real-time. This technological capability will only succeed if both Ops and Intel strive to learn more about what each brings to the fight. Both communities have their work cut out for them in the twenty-first century.

Notes

[1] Col Gary D. Payton, USAF, ed., "The Art of Intelligence, by the General," *AirpowerJournal*, Winter 1993, 19.

[2] Joint Pub 2-0, *Joint Doctrine for Intelligence Support to Operations*, 5 May 1995, II-2.

[3] Maj Gen James R. Clapper, Jr., "Challenging Joint Military Intelligence," *Joint Force Quarterly*, Spring 1994, 94.

[4] Joint Pub 2-0, II-3.

Notes

[5] Ibid., II-4.

[6] Thomas A. Kearney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report*, (Washington, D.C.: Government Printing Office, 1993), 140.

[7] Joint Pub 2-0, II-6.

[8] Ibid.

[9] Abram N. Shulsky, *Silent Warfare*, (New York: Brassey's, 1993), 81-82.

[10] Colonel Edward Mann, USAF, "DESERT STORM, The First Imformation War?" *Airpower Journal*, Winter 1994, 11.

[11] Joint Pub 2-0, II-7.

[12] *Near Real-Time Combat Information User's Training Guide* (U), 14 September 1995. (Secret) Information extracted is unclassified.

[13] Lt Col Ronald J. Norman, "The Intelligence Road to Recovery" (AWC research paper, April 1995), 11.

[14] Col Jack Fry, USAF, "Progress Report - Getting Space to Warfighters," *Space Tactics Bulletin*, Spring 1996, 3.

Chapter 4

Roadblocks to Effective Integration

> *Great part of the information obtained in war is contradictory, a still greater part is false, and by far the greatest part is of a doubtful character.*
>
> —Carl von Clausewitz

The information presented in the previous section has made it increasingly clear that the need for better integration of Ops and Intel will not only improve the final product delivered to the warfighter, but, will make the intelligence producer's job easier. With the process benefiting all involved, why has the integration process not occurred years ago? The answer lies in a number of roadblocks that have been established within both the intelligence and operations communities as well as between the two. Some of these roadblocks are institutional and others have grown over time. The important step is to identify these roadblocks and take steps to eliminate them. The focus of this discussion will be on identifying these roadblocks.

Career Education Flow

The education process received by intelligence officers and operators is a logical place to start looking for potential problems. Formal training for USAF intelligence officers is taught by Air Education and Training Command (AETC) at Goodfellow AFB, Texas. All

officers initially receive the *Fundamentals of Intelligence Course*. This course is a 760 hour, 19 week, non-Air Force Specialty Code (AFSC) awarding course. The course attempts to provide the students with an introduction to all aspects of the intelligence career field. It is currently divided into 15 blocks of instruction that range from national collection systems (and their capabilities) to air, ground, and naval tactical systems and their employment.[1] This course does an excellent job covering the range of intelligence operations from the national strategic level to the unit tactical level. It only provides an introductory level of knowledge to these topics though.

Upon completion of the fundamentals course, each officer must then decide which of two AFSCs to pursue. Each AFSC, 14N1A Intelligence Operations Officer, and 14N1B Intelligence Applications Officer requires a twelve week follow-on course to complete the officer's training. The courses taught at this level are significantly different. The operations track emphasizes national and theater level intelligence systems and support activities. This track covers signals intelligence (SIGINT), imagery intelligence (IMINT), and human intelligence (HUMINT).[2] Graduates from the operations course frequently spend the majority of their careers working for and within the national intelligence community. The applications track covers an entirely different syllabus. Courses in this track emphasize analysis, production, and dissemination skills used at the operational unit level.[3] Graduates from the applications course normally go directly to an operational flying unit to work with aircrews at the squadron/wing level. The vast difference between the two primary intelligence career fields lays the foundation for future problems. In order to increase their proficiency, Intelligence Operations officers spend a significant amount of time learning technical skills and procedures while interacting with other national intelligence

organizations. Little time is available to “get into the weeds” and develop credibility at the operational flying level. On the opposite side of the coin, Intelligence Applications officers spend most of their time interacting directly with squadron and wing level flying units. They must attempt to fully understand the missions and requirements they support daily. This leaves little time to acquire more than the introductory level knowledge on national system capabilities that was previously discussed. This often puts applications officers in the uncomfortable position of not being able to fully exploit the information that may be available to support flying operations. They frequently serve as the “middle-man” between aircrews requesting intelligence and the national level producers of the information.

Now that we have identified the potential for an integration roadblock from within the intelligence community, a look at the operational flying community’s education will solidify the existence of the problem. All aircrew members receive their wings through similar USAF pilot/navigator training. Due to the workload and objectives of these programs, there is little exposure to intelligence. Initial threat awareness training, and increased interaction with intelligence, comes once the aircrew member has been certified in his major weapons system. This exposure is less of an interactive process and more of a “spoon fed” learning process. Intel personnel provide “threat-of-the-day” and “current intelligence” briefings, academics on enemy capabilities, and assistance in daily mission preparation. Aircrew members perfect their employment skills and attempt to refine tactics to defeat adversary threat systems. These day-to-day tasks build an unhealthy mindset. Operators tend to treat intelligence information as something that will always be there when they need it. There is very little attempt to include intelligence personnel in “blue” tactic development and even less of an effort to better understand the capabilities of the

front-end intelligence systems that they are using to base the assumptions for their tactics development. In a speech to the NSA, Lt Gen Howell Estes, Director Of Operations (J-3), stated that; "Operators have not done their part to meet the intelligence community halfway."[4] He went on to commend the intelligence community for their efforts to learn more about operations and criticized operations for taking the "just tell me what I need to know" attitude. Clearly, the already established division within the intelligence community, combined with the "just tell me what I need to know" mindset, has created a significant roadblock to effective Ops/Intel integration.

Intelligence "Stovepipes" & Product Dissemination

Another major roadblock in the integration of Ops and Intel relates to the "stovepiped" collection and dissemination of intelligence products. According to Major General Clapper, "Intelligence organizations have been characterized by a proliferation of stovepipe collection, processing, and analysis organizations. Stovepipe is a term given to vertical organizations that collect, process, analyze, and disseminate one category of intelligence without integrating other types of intelligence into the final product."[5] Stovepiping within the intelligence community, along with the push method of dissemination, have combined to quickly overload the operator with too much information. In the high tempo operations of today's military, large volumes of uncorrelated information are normally brushed aside.

Relating to the problem of stovepiping is the frequent overclassification of intelligence products. A significant amount of SIGINT and HUMINT products are classified at the Special Compartmentalized Information (SCI) level. Intelligence producers use this level

of classification to restrict dissemination and thereby, protect the source of the information better. “The better the information the analysts have available, the more inhibited they are about using it and perhaps alerting the adversary to their intelligence capabilities.”[6] This is a viable concern within the Intel field. Ops must be aware of it and work within the constraints presented. Since the average USAF fighter/bomber squadron contains very few individuals with an SCI clearance, not working closely with Intel in this area will frequently result in less than optimum support. This issue is important enough that the solutions to overcome this roadblock must be discussed now.

The first step that must be taken is for Ops personnel to be as specific as possible when stating their requirements for intelligence products. This includes not overstating the requirements with the assumption that a lesser product will result. This is important so that the collection method used to satisfy the requirement will appropriately reflect the need. For example, if the activity level of a particular building is required in order to target it at a time when minimum loss of civilian life would occur, that is how the requirement should be explained. The unit Intel personnel can then relay the requirement up the chain and numerous sources could be used to gather the requested data. If however, the target activity information required is so specific that the presence of specific individuals in the building must be known, entirely different collection methods will most likely be required. It should be obvious that the latter request will require the use of much more sensitive sources and, therefore, take longer, if received at all. The unit Intel officer taking the initial request must be familiar with the mission and ensure that he understands exactly what the requested information is needed for. It is clear that the integration displayed between Ops

and Intel in this situation will potentially make the difference between a requirement being filled or not.

Another way that Ops can directly help in the protection of intelligence sources involves the concept of "plausible cover." This concept involves presenting the enemy with an alternative source from which information was gathered while concealing the actual method. The following example illustrates this concept:

> During World War II the British knew, from intercepted and decrypted communications, the precise schedule of the German ships bringing supplies across the Mediterranean to General Erwin Rommel's forces in North Africa. Nevertheless, to prevent the Germans from becoming suspicious about the security of their communications, the British adopted the rule that no ship could be attacked before it was overflown by reconnaissance aircraft, thus providing the Germans with an alternative explanation of how the ship came to be located and attacked.[7]

Not only did Ops continue to receive perfect intelligence in this area, the sources remained secure throughout the war. This is a classic example of the benefits provided to both members of the Ops/Intel team with effective integration.

The three roadblocks mentioned here are not the only obstacles to the effective integration of Ops and Intel. They are significant ones that must be overcome, though. Plausible cover is one that will require constant efforts by both the Ops and Intel communities. In this age of information warfare, imaginative concepts will have to be employed to protect sources of our intelligence data in the future. The areas of education and intelligence stovepiping are still significant areas that we must improve in. Education is especially critical as it helps to dissolve numerous other less significant obstacles. The next section will propose means to break down some of these barriers and ensure that Ops and Intel are running the same play once the ball is snapped.

Notes

[1] *Course Syllabus for Fundamentals of Intelligence Course,* X3OQR14NO 003, Goodfellow AFB, Tex., 14 January 1997, 1-4.

[2] *315th Training Squadron, Training Courses*, Goodfellow AFB, Tex., 15 August 1996, 4.

[3] Ibid., 5.

[4] Lt Gen Howell M. Estes III, "Intelligence and Operations Today," lecture, National Security Agency, Fort Meade, Md., 23 February 1996.

[5] Maj Gen James R. Clapper Jr., USAF, "Desert War was Crucible for Intelligence Systems," *Signal*, September 1991, 77.

[6] Abram N. Shulsky, *Silent Warfare*, (New York: Brassey's, 1993), 53.

[7] Ibid.

Chapter 5

Proposed Solutions

> *How can any man say what he should do himself if he is ignorant about what his adversary is about?*
>
> —Baron Antoine-Henri Jomini

The process of identifying a problem in the Ops/Intel relationship through the study of historic examples, examining key areas in the intelligence cycle that require better integration, or recognizing barriers to the integration process only lays the foundation for the final objective of creating a finely oiled Ops/Intel machine. The recommendations presented in this section are specifically designed to break down the barriers between (and within) the Ops/Intel communities.

Two-Way Educational Improvements

When AF officers are told that they will be scheduled for "mandatory" training as part of their semiannual or annual requirements, a less than enthusiastic response normally follows. The response is due to the feeling that another "square" will be filled at the expense of precious "real mission" training. Frequently, the squares that are filled are exactly that; academics or briefings in an area that will most likely have little impact on accomplishing the day-to-day mission. When the day-to-day mission happens to be putting "bombs on target", or getting the required information to allow someone else to put those

same bombs on the *correct* target, without getting shot down, a little training that will help accomplish this does not sound as bad. It will only take one "Dear Mrs. X, I regret to inform you..." type of letter to make the training look even better.

In order to prevent this scenario from developing as a result of poor or incomplete intelligence, the knowledge gap between the Intelligence Applications and Operations career fields must be decreased. Intelligence Operations Officers must learn more about theater and tactical level missions and the commensurate support required. At the same time, Intelligence Applications Officers must become more familiar with national systems and their products. They must then pass this knowledge on to the aircrews they support with a combination of briefings on national capabilities and examples of actual products. Ops personnel must also be aware of the limitations of these collection systems. This is particularly true for the SIGINT and IMINT disciplines. This program would serve two purposes. It would provide operators with knowledge not currently available, thus, allowing them to communicate their requirements better. It would also build stronger ties between unit Intel personnel and unit aircrews. AETC, in coordination with Air Intelligence Agency (AIA), is currently developing a program to require Intel officers in each career field to complete a "cross-training" academic program.[1] The purpose of the program is to broaden the officer's knowledge of the entire intelligence process after they have gotten some hands-on experience. The implementation of such a program would be a good initial step in narrowing the Intel career field gap. In addition to the cross-training program, AETC/AIA should consider incorporating commercial conflict simulation wargames into the Operations training program. This would be a relatively inexpensive way to give a hands-on operational focus to the national intelligence community. The

incorporation and maturation of these programs would be a significant step in the educational improvements required to successfully integrate Ops and Intel.

Another outstanding opportunity to better cross-educate operators and intelligence officers resides at the USAF Weapons School (WS) located at Nellis AFB, Nevada. The WS is the premier training course for giving highly qualified aircrews and intelligence officers Ph.D. level instruction in the employment of all major weapons systems in the USAF inventory.

> The WS curriculum trains the graduate to be an expert in the full array of weapons, and weapons related equipment capable of employment by his aircraft; the avionics and systems which support weapons delivery; the potential threats that Combat Air Forces (CAF) may have to face; and the array of tactics available for effective weapons system employment. He is familiar with the structure and policies of the CAF and can interface with all elements to help bring about effective combat ready forces.[2]

WS graduates go on to supervise weapons and tactics shops, intelligence organizations, and planning cells from the squadron level to the Air Staff level. They are expected to be the commander's expert in all areas of tactical and operational employment. Many members of the Black Hole planning staff during Desert Shield/Storm were WS graduates. Unfortunately, the current syllabus for all weapons systems reflects the same educational roadblock that has held up the effective integration of Ops and Intel. In the 304 hours of academic instruction received by the F-16 and F-15E aircrews, only four hours are taught on national intelligence capabilities.[3] An even more unbelievable fact is that in the 406.5 hours of academic instruction that are taught in the intelligence officer's course, only eleven hours are dedicated to national intelligence capabilities.[4] Students in the intelligence officers' course come primarily from the applications career field. Upon graduation they normally return to an operational wing and supervise/support Wing Intelligence. In

today's environment, the level of knowledge on national capabilities must be higher for the individuals supervising the training and unit level intelligence support to operations. The only WS syllabus that includes a significant amount of emphasis in the national intelligence area is the relatively new Command and Control course. The Command and Control Division of the WS educates RC-135 and Airborne Warning and Control System (AWACS) operators. Their current syllabus contains 69 hours dealing with national capabilities in a 447 hour program. It also includes a field trip to national agencies in the Washington D.C. area and a trip to observe actual products being used during an army field training exercise.[5] This example could serve as a guide for changes to the Intel Division's syllabus. As intelligence information becomes more and more critical in the execution of military operations at all levels, national systems will play an increasing role in filling this requirement. WS syllabi must be changed to reflect this fact. More emphasis on national intelligence systems and their products, to include hands on exposure to these products, must be integrated into the WS.

Training Improvements

The above mentioned improvements in education are only the first step in an improved Ops/Intel relationship. We must also train like we will fight. Units at all levels must incorporate a robust training program to ensure that all wartime intelligence functions are practiced in peacetime. Aircraft videotape review is an example of one of these functions. The demand for near real-time BDA during Desert Storm highlighted a major weakness in this capability. CENTAF intelligence personnel attempted to satisfy BDA requirements using "classic" intelligence sources of collection. As presented earlier,

these sources were frequently not capable of producing results in a timely manner. This forced operational planners to look for other means to satisfy their BDA requirements. Their solution was to review forwarded aircraft videotape and make their own assessment on the level of damage. Valuable time was wasted compiling these tapes and reviewing them in Riyadh. Units must create a standard videotape review procedure practiced during peacetime training. Aircrews and unit Intel officers should review mission tapes together and make educated assessments on the damage inflicted. This peacetime practice could then be carried forward during hostilities, saving critical time for theater operational planners. Peacetime practice will be required for accurate wartime assessments in this role.

In addition to training the way we intend to fight, another peacetime training function that would improve Ops/Intel integration involves creating an intelligence "devil's advocate" cell during major unit training exercises. This concept would involve the creation of a small team of approximately one operator and one or two intelligence individuals. Their purpose would be to study actual unit training plans, missions, and tactics and propose enemy reactions based on this information. The benefits of creating a cell such as this for major exercises are twofold. First it allows Ops and Intel personnel to work together and pool their individual knowledge in the creation of tactics and plans at the squadron/wing level. The fallout from this would be an unavoidable improvement in the understanding of what both Ops and Intel bring to the table when forced to work together under time critical conditions. The second benefit goes to the unit in that they now have the ability to predict possible enemy courses of action under a "worst case" scenario. The "perfect intelligence" reaction may reveal weaknesses in the unit's planning,

tactics, or both. The specific individuals in this "devil's advocate" cell should be rotated every exercise to allow maximum participation by unit members.

Decrease Vertical and Increase Horizontal Coordination

The final area for improvement falls primarily in the intelligence community structure. In order to decrease intelligence stovepiping and increase the amount of *useful* intelligence that reaches the warfighter, coordination within the intelligence community must improve. Intelligence organizations must build bridges between the different disciplines and decrease the distance between the producer and the user of intelligence products. One method of increasing horizontal coordination used today is the establishment of a Joint Intelligence Center (JIC) or National Intelligence Support Team (NIST). These units combine service intelligence personnel, CIA, NSA, and DIA representatives to produce all-source intelligence products for a theater or Joint Task Force (JTF) commander. These units are frequently formed as "hot spots" develop that warrant US military involvement. The successful fusing of multiple sources of data by the JIC/NIST frequently leads to more accurate products and less duplication of effort in the intelligence gathering process. These types of products must be the norm and not the exception in the future.

An improved horizontal coordination process will improve the accuracy and reduce the amount of useless information that the warfighter receives, but, will not in itself guarantee that the intelligence data be received in a timely manner. An important step that must be taken to achieve this goal is to decrease the number of levels that exist between the producer and the user of the data. Continued development of the "pull" system discussed earlier will take a big step in the right direction in this area. High priority must

be placed on developing and refining the GBS. Technology is making GBS possible, however, will not improve the support given to warfighters by itself. Unit level intelligence personnel must expand their knowledge of the support required by their operators and must be aware of how to pull this from national databases quickly.

The solutions proposed in this section are just some of the measures that can be taken to help integrate Ops and Intel. Some involve evolving technology and others are purely simple fixes that can be implemented today. The common thread that exists between all of these proposals is that they all require a dedicated effort from both communities in order to be effective.

Notes

[1] Maj Michelle Gomez, Air Intelligence Agency Headquarters, interview by author, 10 December 1996.

[2] *USAF Fighter Weapons Instructor Course Syllabus, F-16*, January 1996, 1-2.

[3] Ibid., 3-17.

[4] *USAF Intelligence Weapons Instructor Course Syllabus*, July 1994, 3-18.

[5] *USAF Weapons Instructor Course Command and Control Operations Syllabus*, July 1995, 3-16.

Chapter 6

Conclusion

Everything in war is simple, but the simplest thing is difficult.

—Carl von Clausewitz

Clausewitz's reflections on the simplicity of the tasks in war, yet, the difficulty in accomplishing these tasks is especially applicable in the integration of operations and intelligence. History is riddled with examples of tragic results when armies engage in battle with poor or incomplete intelligence. We can also see examples of numerically inferior forces completely overwhelming their enemy due to the synergistic effects caused by the correct application of forces at the right place and right time based on a key piece of intelligence in the correct hands. *Joint Vision 2010* states that:

> In all operations technological advances and our use of information will give the warfighters at the individual, crew, and small unit levels major qualitative advantages over potential adversaries. Our forces will be able to sense dangers sooner. They will have increased awareness of the overall operational environment, including the situation of friendly forces, allowing them to make better decisions more rapidly. They will have an enhanced ability to produce a range of desired effects by bringing together the correct mix of assets at the place and time most favorable to success.[1]

Will technology be the panacea that will allow the US military to dominate any adversary in the future? Without educated people and an informed force, technology is nothing more than fancy bells and whistles. Effectively integrating Ops and Intel will require a dedicated effort by both communities. Each must attempt to learn the strengths

and weaknesses of the other. Only through knowledge of these capabilities will we be able to compensate for weaknesses by capitalizing on our individual strengths. The United States is entering the twenty-first century in a unique position. There is no obvious threat to our national security that we must prepare for. It is for this reason that our military forces must be ready for any contingency. The effective integration of operations and intelligence into one team will insure that we are ready!

Notes

[1] Gen John M. Shalikashvili, USA, *Joint Vision 2010*, 12.

Glossary

AETC	Air Education and Training Command
AF	Air Force
AFSC	Air Force Specialty Code
AIA	Air Intelligence Agency
ATO	Air Tasking Order
BDA	Battle Damage Assessment
CAF	Combat Air Forces
CENTAF	Central Command Air Force Component
CIA	Central Intelligence Agency
CIS	Combat Intelligence System
DIA	Defense Intelligence Agency
GBS	Global Broadcast Service
HUMINT	Human Intelligence
IAF	Israeli Air Force
IMINT	Imagery Intelligence
IN	Intelligence
JDISS	Joint Defense Intelligence Support System
JFC	Joint Force Commander
JIC	Joint Intelligence Center
JIPTL	Joint Integrated Prioritized Target List
JTF	Joint Task Force
MAAP	Master Air Attack Plan
NIST	National Intelligence Support Team
NSA	National Security Agency
SAM	Surface-to-Air Missile
SCI	Special Compartmentalized Information
SIGINT	Signals Intelligence

SPINS	Special Instructions
TIBS	Tactical Information Broadcast Service
UAV	Unmanned Aerial Vehicle
US	United States
USAF	United States Air Force
WS	Weapons School

Bibliography

Clapper, Maj Gen James R. "Challenging Joint Military Intelligence." *Joint Forces Quarterly,* Spring 1994, 92-99.

Clapper, Maj Gen James R. "Desert War was Crucible for Intelligence Systems." *Signal*, September 1991, 77-80.

Course Syllabus for Fundamentals of Intelligence Course, 14 January 1997.

Ennes, James M. *Assault on the Liberty.* New York, N.Y.: Ivy Books, 1979.

Ennes, James M., "USS Liberty Homepage." n.p. On-line. Internet, 15 January 1996. Available from http://www.halcyon.com/jim/ussliberty/liberty.htm.

Estes, Lt Gen Howell M., III, Director of Operations (J3). "Intelligence and Operations Today." Lecture. National Security Agency, Fort Meade, Md., 23 February 1996.

Fry, Col Jack. "Progress Report - Getting Space to Warfighters." *Space Tactics Bulletin*, Spring 1996, 3.

Joint Pub 2-0, *Joint Doctrine for Intelligence Support to Operations.* 5 May 1995.

Kearney, Thomas A., and Eliot A. Cohen. *Gulf War Air Power Survey Summary Report.* Washington D.C.: Government Printing Office, 1993.

Lambeth, Benjamin S. "Moscow's Lessons from the 1982 Lebanon Air War." In *War in the Third Dimension: Essays in Contemporary Airpower.* Edited by R. A. Mason. London: Brassey's Defense Publishers, 1986.

Mann, Col Edward. "Desert Storm, The First Information War?" *Airpower Journal*, Winter 1994, 4-13.

Near Real-Time Combat Information User's Training Guide (U), 14 September 1995 (Secret) Information extracted is unclassified.

Norman, Lt Col Ronald J. "The Intelligence Road to Recovery." AWC research paper, April 1995.

Payton, Col Gary D., ed. " The Art of Intelligence, by the General." *Airpower Journal*, Winter 1993, 16-25.

Shalikashvili, Gen John M. *Joint Vision 2010.*

Shulsky, Abram N. *Silent Warfare.* New York: Brassey's, 1993.

USAF Fighter Weapons Instructor Course Syllabus, F-16. January 1996.

USAF Intelligence Weapons Instructor Course Syllabus, July 1994.

USAF Weapons Instructor Course Command and Control Operations Course Syllabus, July 1995.

315th Training Squadron, Training Courses, 15 August 1996.