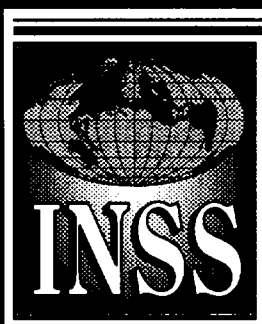


INSTITUTE FOR NATIONAL STRATEGIC STUDIES

INTEROPERABILITY

A DESERT STORM CASE STUDY

STERLING D. SESSIONS
and
CARL R. JONES

NATIONAL DEFENSE UNIVERSITY

McNair Paper Eighteen

A popular Government,
without popular information or the means of acquiring it,
is but a Prologue to a Farce or a Tragedy; or perhaps both.
Knowledge will forever govern ignorance;
And a people who mean to be their own Governors,
must arm themselves with the power which knowledge gives.

JAMES MADISON to W. T. BARRY
August 4, 1822

INTEROPERABILITY

A DESERT STORM CASE STUDY

STERLING D. SESSIONS
and
CARL R. JONES

McNair Paper Eighteen
July 1993

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

NATIONAL DEFENSE UNIVERSITY
Washington, D.C.

NATIONAL DEFENSE UNIVERSITY
□ *President:* Lieutenant General P. G. Cerjan
□ *Vice President*: Ambassador H. K. Walker

INSTITUTE FOR NATIONAL STRATEGIC STUDIES
□ *Acting Director:* Stuart E. Johnson

Publications Directorate □ Fort Lesley J. McNair □ Washington, D.C. 20319–6000 □ Phone: (202) 475–1913 □ Fax: (202) 475–1012
□ *Director:* Frederick T. Kiley □ *Deputy Director:* Lieutenant Colonel Barry McQueen □ *Managing Editor, JFQ:* Robert A. Silano □ Chief, Publications Branch: George C. Maerz □ *Editors:* Calvin B. Kelley, Kathleen A. Lynch, Martin J. Peters, and Mary A. Sommerville □ *Circulation Manager:* Myrna Morgan □ *Editorial Assistant:* Patricia Williams

□ *Text design and editing:* Kathleen A. Lynch □ *Cover Design:* Juan A. Medrano

Dr. Sterling Sessions is an adjunct professor of strategic management at the Naval Postgraduate School, Monterey, California. Dr. Carl Jones is a professor of command and control at the Naval Postgraduate School.

From time to time, INSS publishes short papers to provoke thought and inform discussion on issues of U.S. national security in the post–Cold War era. These monographs present current topics related to national security strategy and policy, defense resource management, international affairs, civil-military relations, military technology, and joint, combined, and coalition operations.

Readers are invited to submit (nonreturnable) manuscripts for consideration for publication in WordPerfect 5.1 on 3.5 inch diskettes with one printout.

Second printing, December 1993

ISSN 1071-7552

Contents

PREFACE

The Command and Control Research Program (CCRP) is a part of the Institute for National Strategic Studies at NDU. Established in 1983, the CCRP directs research on emerging national issues in command and control, including ways to improve instruction on this vital topic in Joint Professional Military Education. The CCRP provides an active constituency within Joint Professional Military Education for command and control while performing a "bridging" role between the Joint doctrine, operational and technological communities. The CCRP also promotes general understanding of command and control through sponsored research, resulting in products such as this case study.

Operation Desert Shield and Desert Storm are a rich source of examples that emphasize the problems of information management, the effective use of information systems technology, and the interdependent way these systems interact both within our own services and among coalition partners. A smooth flow of information, and hence the way leading-edge technologies process and communicate information to key decision makers, is essential to the success of any modern operation. Interoperability has become critical to commanders at all levels.

This case study and analysis of interoperability by Dr. Sterling Sessions and Dr. Carl Jones was sponsored by CCRP. Though originally designed for classroom use at the senior service college level, as a monograph it offers useful insights to any reader interested in this integral element of organizational efficiency and the fast-moving communications revolution.

Command and Control Research Program
Institute for National Strategic Studies
NATIONAL DEFENSE UNIVERSITY

INTEROPERABILITY
A Desert Storm Case Study

STERLING D. SESSIONS
and
CARL JONES

The ultimate goal is simple: give the battlefield commander access to all the information needed to win the war. And give it to him when he wants it and how he wants it.

GENERAL COLIN L. POWELL[1]

---

1 Interoperability

General Powell's ambitious vision statement, in July 1992, heralded a new era for interoperability: an era of budget cuts, multinational services, and public clamor for congressional efficiency. At the same time, specialized, regionally based conflicts took the place of vast ocean and huge land-mass battlefields.

Interoperability has many facets. Its definition encompasses two radios talking to each other, an Ocean Venture exercise, hardware and software matching, and cross-service

training. It is "equipment, procedures, doctrine, and training" and "the ability of people, organizations, and equipment to operate together effectively."[2]

During the Storm

Desert Storm typified the new era with its successful melding of many units from many services and many countries. But a lack of interoperability caused enough tactical problems to give any seasoned observer pause. "Communications for artillery fire support were a particular problem because the (radio) equipment lacked sufficient range or frequencies," according to one Marine General. Some platoon leaders could not talk on the radio to squad leaders "a mere 75 feet away,"[3] said one Army battalion Commander. These problems were part of a broader category including hardware and software systems, functions, and processes, all comprising an element of C^4I system's interoperability, or the compatibility of communications hardware, as formulated by Dr. Stuart Starr (see below). Policy decisions on role assignments were to blame for other interoperability breakdowns. The Gulf anti-air warfare ships, for example, could not exchange data directly with the on-station E-3As (airborne warning and control systems) assigned to cover the land-related portion of the Kuwaiti theater. In contrast, the Gulf-based ships received airborne early-warning data from shore-based Marine Corps tactical air operation and command centers. These circumstances hampered early detection and tracking efforts in that target-rich domain.[4] Admittedly, this illustration is more in the domain of Command and Control wherein a Commander "assigns forces in the accomplishment of a mission." But whenever time is a factor, interoperability is, too.

In a similar sense, problems of operating procedure were associated with the Air Tasking Order (ATO). The

Gulf ATO was an intricate, computerized, daily list of all air assets in a Joint Task Force (JTF) environment (see Appendix A for a facsimile). From the ATO, strike mission planners could obtain information about numbers of missions, squadrons assigned, targets, restricted operating zones, low-level transit routes, drop/landing/extraction zones, and air refueling areas. It did not specify tactics or flight plans.

During Desert Storm ATO was an unusually effective system yet not without imperfections. From one Naval officer's vantage point, while the Air Force considers the ATO "the playbook for the vastly successful Air Bowl. . .

> We in the surface Navy, from our more parochial perspective, remember it simply as the 300-page, 'Personal For,' flash-precedence, randomly sorted message, rarely received before the middle of the day to which it applied. The sheer bulk of the document implies that the Air Force—whose own composers designed it—expected a lot more people around who could make sense of it. The JFACC's (Joint Force Air Component Commander) six-pound Air Tasking Order had to be picked up in Riyadh at 0200, delivered to the carrier, and transferred to the surface ships (usually a three to four hour mission). The people who published this tome probably never envisioned that a couple of junior enlisted air controllers on a three-week caffeine high in the back of a combat information center would have to flip through this six-pound chunk of fanfold paper on their knees to find the whereabouts of a tanker for their combat air patrol."[5]

Yes, but the data were "not user friendly," another Naval officer responded. "The Navy and Air Force have since learned a great deal about the process and have made progress in providing that data via other means."[6]

The ATO was to be transmitted in digital form through personal computers, but the Navy's computers and software

were not up to the volume of traffic. As a result, the ATO was flown on Lockheed S-3A Vikings to the carriers.

The Air Force had its own problems in using the ATO and initially sent it to its forces on F-15 Eagles.[7] Eventually, the Air Force managed to double its data transfer capability but had no hardware to spare for the Navy. Even with the right computers and software, however, "the Navy . . . would have been impeded by satellite circuit capacity limitations."[8]

The arguments between the Air Force and the Navy concerning centralized air control were not the only issues. After Desert Storm, Army Corps commanders criticized the Air Force for targeting only 300 (15 percent) of the 2,000 Army-nominated targets.[9]

An Air Force officer justified this situation on the basis of, (1) a two- to three-day lag in Army intelligence from CENTAF and (2) a redundancy in the target lists. He also said that half of the Marine Corps' sorties (150 to 200 a day) were dedicated to MARCENT (Marine Corps Command Center) and therefore not available to the Joint Forces Air Command Center (JFACC), which narrowed the effectiveness of JFACC management of the air effort.[10] Centralized air command was superior to allowing theater commanders to operate relatively independently, he concluded.

Storm Workarounds

"We've come along ways from the bombing of Libya," said another officer, where the Air Force took the west side of the country and the Navy the east, "in a perfect recipe for fratricide . . ."[11]

> In the Gulf we ran the air offensive through a single management. The CENTCOM was first located in August 1990 on a parking lot in Riyadh surrounded by an "awesome" four-foot

> high fence—a satchel charge thrown over the fence could have destroyed the center. We soon moved to the basement of the Royal Saudi Air Force Center and Ministry of Defense which was a nice place to be. However, as far as bomb proofing was concerned, there wasn't much protection since we had to leave the doors open for the power cables which ran from room to room.[12]

Cables also ran from the rooftop DSCS (Defense Satellite Communications System) satellite terminal, over and down the wall, through a window to the basement. The entire communications network consisted of a few voice and data circuits routed through four tactical ground-based terminals.[13] Soon, this rudimentary system was enhanced allowing Desert Storm Commanders to talk to their counterparts in the United States. By January 1991 the number of downlinks had increased from 1 to 118 with 12 commercial satellite terminals in place. These gateways supported 324 voice trunk lines and 30 Automatic Digital Network data circuits. Additional dedicated voice circuits were established between the Joint Staff operations director in the Pentagon and the CENTCOM war room in Riyadh to accommodate message flows approximating two billion characters each day.[13]

One of the first major telecommunications challenges related to a call completion rate to the United States of only 20–30 percent a day. It took the military and representatives of AT&T and GTE three months to identify the problem as incompatible signaling between tactical and fixed systems. The solution was later found over a long weekend by AT&T Bell Lab employees.

A second problem related to the communications switches in the Army's new Mobile Subscriber Equipment which would not work with the vintage-technology switches in other services' equipment. The solution was derived by

JTC3A (Joint Tactical C^3 Agency) over 17 days: new software made the Army's switches work with the Marine/Air Force Level Circuit Switch and the French RITA communication system.

A third problem was created by the vast volume of message traffic and the relative shortage of military satellites to do the job. Commercial suppliers immediately assembled 15 ground-based stations from off-the-shelf components which handled 20 percent of the traffic during the war.

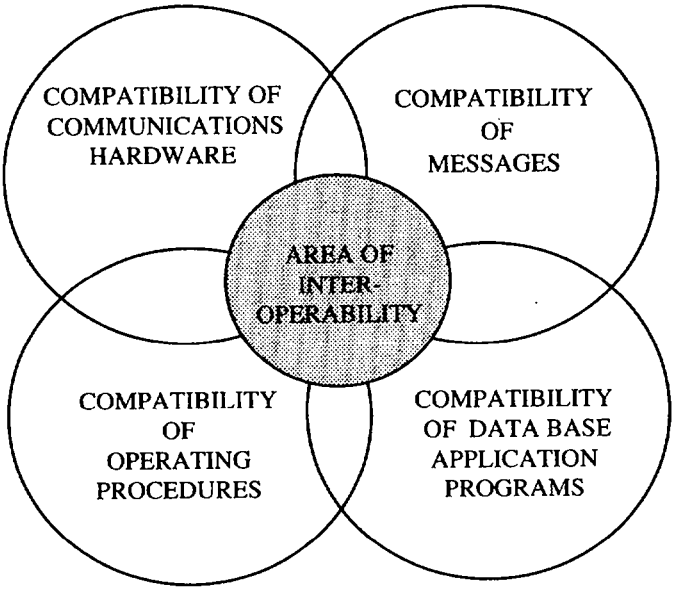
Also in short supply were Global Positioning System (GPS) receivers, known as Sluggers, which linked with the Pentagon's 16 GPS satellites. Almost immediately over 8,000 off-the-shelf receivers,[14] the size of a paperback book, were obtained to aid in mapping, clearing minefields, and guiding the navigation of troops who swept through Kuwait. "We have known for some time that we need to do a better job of standardizing our data links and protocols: a more widespread deployment of Joint Tactical Information Distribution System (JTIDS) terminals will help in this regard," commented one contemporary C^3 player.[15]

These few illustrations of workarounds focused on the managerial responses to particular problems that were not anticipated or came earlier than anticipated. Both conditions suggest some framework for structuring interoperability analyses to prevent such problems from reemerging.

Managing Interoperability

Interoperability is somewhat like quality. It is an integral part of an institution's output, always present in some degree, a determinant of an institution's continued life— yet difficult to define, pinpoint, and manage. Often it is seen as a truism, something that is evident and expected. Once someone derives a pragmatic, clear approach to coping

FIGURE 1.1 ELEMENTS OF INTEROPERABILITY



Source: Stuart H. Starr, MITRE Corporation, "Perspectives on C^3 Interoperability," briefing at Naval Postgraduate School, Monterey, California, July 1990 .

with interoperability, it may sound like "just common sense" but it deserves attention.

A case in point is Stuart Starr's perception of the elements of interoperability. His Venn diagram shows that the elements of interoperability are interrelated but have distinct boundaries (Figure 1.1).

Operating procedures indicate the frequencies to use, pattern of employment, and codes; compatibility of messages (the identification of message length, message field contents, and order of the message fields). Data base applications among systems must use the same formats for records, for example, is it 10 May or May 10?[16]

Other definitions of interoperability are more strategic than Starr's, but sometimes reach a point of abstraction that

makes implementation difficult. While general descriptions of overarching goals are a necessary part of the process of formulating any workable strategic statement, they must be completed by details. The accompanying description must analyze and explain (1) an institution's technological, legal, and economic operating environment; (2) its competition (which interservice rivalry in the congressional arena constantly provides), and (3) its precise strengths and weaknesses. Finally, all these factors must be evaluated in terms of the values of the institution or what is important to senior leadership.

Strategic Implications for Interoperability

C⁴I for the Warrior, produced and published by the Joint Staff in June 1992, documents the answer to General Colin L. Powell's charge, "The time is ripe to set a course to resolve our C⁴I interoperability issues." The document resolves the interoperability issues in concept, but one of its framers, an Army Colonel, questions how well it will work in real life. "Interoperability gets to the worst of human nature: giving up the short term to envision, plan, and pull it off," he said. But, he added "We cannot afford any longer to fix these elements later without an over-riding process that leads from jointness to oneness."[17]

Turning to the demise of the Soviet Union, from threat to world peace to now "having lunch with the Allies at NATO, the Colonel said:

> Once this took place we did Command and Control without acknowledging the threat, anyplace, anytime in the world. This was a classic stovepipe [systems] environment as indicated particularly in Ernest Fury when no one had the same signals, meaning that J6 was kept outside the huddle. These circumstances continued until the second day of Desert Shield when an electronic connection was found to link the stovepipes

> together. This was an ideal situation because we never want to force a standardized approach on the Services.
>
> To accommodate this principle I see interoperability as driving the train with standards being the engine or locomotive . . . enforc[ing] the standards . . . is not an easy thing to do in Washington where the only game is money, and the JCS has no leverage over the Planning, Programming, Budgeting System (PPBS). This means that you can only exercise control over the expenditure of Service-related dollars through policies and standards which affect the acquisition processes. This is the major reason we are building this concept into *C^4I for the Warrior*.

Marine Corps General Harry W. Jenkins, Assistant Chief of Staff C^4I^2, reinforced that comment:

> The Gulf War saw the first space/electronic assault based on highly intelligent systems. It succeeded in many areas and failed in others. It did prove that the Services will never again operate independently; jointness is in. But, we must have better performance standards as far as software is concerned to make interoperability work.[18]

Many of the managerial issues raised by these officers, relating to the tactics or implementation of interoperability strategy, are part of the global interpretation of what interoperability is, what it is designed to do, and when. Some of the positions outlined in *C^4I for the Warrior* show how all such issues fit together:

> Interoperability is the ability of systems, units or forces to provide services to, and to accept services from other systems, units or forces, and to use the exchanged services to operate effectively together.

And, a more comprehensive, even strategic version in the same document:

> Interoperability encompasses doctrine, procedures, and training as well as systems and equipment. It is the capability of people, organizations, and equipment to operate effectively together so that "every unit on the battlefield can share information with every other unit on the battleground."[19]

A final description of the importance and meanings of interoperability is contained in the National Military Strategy Document, which assigns interoperability Number One priority.[20] The ramifications of stressing interoperability extend to: (1) *technology:* providing the means for exchanging information among systems and users, through the use of common standards and protocols designed into the equipment and systems; (2) *applications:* providing a common understanding of how information will be fused,[21] processed, and used; (3) *data:* to be freely shared and transferred among systems and applications without translation; (4) *procedures and doctrine:* requiring parallel development among systems; and (5) *equipment and systems:* Information Systems Agency (DISA) through the Joint Interoperability Test Center (JITC).

Looking Ahead

Interoperability, in summary, has been illustrated and defined, both from a tactical, managerial outlook and from a strategic viewpoint. This will lead to a review of other problems associated with Desert Storm, with subsequent solutions: some temporary to meet the vital day by day needs of the war, but most still in the process of being solved.

> A serious issue [with Desert Storm] was the lack of trained users of the technology in U.S. forces. Most of the computers were user owned and operated—no special staff existed to develop software, maintain the data, or provide quality control.

> It was not uncommon to see a singular junior enlisted soldier or officer act as the expert on a staff. Unfortunately, the quality of their knowledge of the computer, its application, and the data which it processed received little scrutiny from superiors who were just as often ignorant of the limitations of the technology.[22]

This statement focuses on the computer as the driver of the nature of the message, which drive tactics, which drives strategy. This situation is in sharp contrast to the conservative, traditional lines of thought wherein top leadership derives and implements strategy, including a communications strategy. Now, with so many lateral information systems in existence catering to text, voice, imagery, and data links, it is often hard for the uninitiated to catch up, and leaders can turn into followers.

The overwhelming amount of data produced and disseminated during Desert Storm is another aspect of computer information. Sometimes excessive amounts of data forced organizations to focus on particular data sets, which created blind spots for other information. Stories are legion about the masses of computerized and telephonic data generated during the operation, including 700,000 telephone calls and 152,000 telephonic messages daily. "The services put more electronic communications connectivity into the Gulf in 90 days than we put into Europe in 40 years," according to Lieutenant General James S. Cassity, Director of C^3 for the Joint Chiefs of Staff.

According to *C^4I for the Warrior*, the administrative power of information and information systems will serve as a common denominator for future military engagements. How the common denominator will evolve, in spite of service rivalry, is precisely described:

> The common global vision of *C^4I for the Warrior* is to create

> for these joint war fighters a single view of military C⁴I. This view is a widely distributed, user-driven network to which the Warrior "plugs in." This network provides seamless, secure connectivity through multiple, highly flexible nodes to all other operational elements and data bases (which are automatically updated and from which desired information can be pulled) for any assigned mission.

Looking ahead, if you were a "commander, director or department head of interoperability" exactly what would your job entail if you were to implement these C⁴I charges? Once you had defined and determined the elements of interoperability how would you manage needed changes? What would you need to know to be responsive to the greater economic and political environment where you have to manage? How would you assess your present interoperability status in terms of equipment, systems, and personnel? On what basis would you determine your overall goals and objectives? How would you establish the requirements for moving from where you are to where you would like to be, in keeping with strategic directions? Aside from equipment acquisitions how would you set up a training program for those involved with interoperability? Training for what?

2 Looking Backwards

Any discussion of a "single view of military C⁴I" should be rooted in past attempts at jointness to the extent that it can be. After all, only one Desert Storm has been fought, and the explosion of communications technology over the past 15 years is without precedent. Times do change. Yet, the past abounds with similar injunctions from seasoned military commanders and civilian specialists. That hasn't changed. For instance, back in 1982 Harvard Professor

Tony Oettinger said:

> Interoperability has been around so long that one wonders it's not being killed with kindness. Everybody is so much for it, and asking for such total interconnectivity, that people throw up their hands at the cost and complexity—particularly Congress and the appropriations committees. So nothing happens—which may be a sophisticated way of reaching the end result desired in the first place, in keeping with service autonomy.[23]

Oettinger's plain words sizing up the late 1970s and early 1980s are linked to other informed observers' views of the military scene:

> The problem today (1980) as it was in the days of Pearl Harbor is elementary. It lies simply in the institutional failure to assign proper responsibility and accountability to major operational commanders.[24]

> Because there are four Services grappling with broad missions in conditions of uncertainty and, at the same time, operating in an environment of scarce resources, there is built-in conflict between the services. The conflict will always exist, no matter how you organize the Department of Defense. The Chiefs [JCS] don't even want to open the unified command book because it becomes a bloodletting when they do.[25]

> All the Secretary of Defense has to do is saddle up somebody in the Office of Secretary of Defense (OSD) and give him the clout to enforce interservice integration. They've tried to do that with the C^3I position, but they've just never given it the same authority and the responsibility to do it.[26]

Integrating the services and promoting a "single view of military C^4I" are admittedly different but related matters. In times past, the particular role of each service as determined by geography, precedence, and warfighting capabilities has

weighed against jointness for many of the reasons mentioned above. The question now, with Desert Storm as the format and the attending resolve by those who fought in that war to "never again be inoperable" is, "Will the JCS with its C^4I and the Warrior be able to reach higher levels of interoperability by controlling acquisitions and establishing common protocols and doctrines, for instance?" Will service autonomy, as stressed by the above quotations, be too much to offset? A comment by Army Colonel David Bryan of the Joint Staff in May 1992 provides a clue:

> JIEO (Joint Interoperability and Engineering Organization) will establish the standards and architecture (for equipment including software acquisitions) under a charter from its parent organization DISA (Defense Information Systems Agency). I can assure you this encroaching on one of the Services' last protected domains was not their idea. It has created a firestorm here in the Pentagon.

Other Voices

Paul A. Strassmann, Director of Defense Information in the Office of the Assistant Secretary of Defense, had this to say:

> The excessive emphasis on hardware platforms is not tenable any more. We are going to go, as a civilization, towards hardware as a commodity and therefore what matters is software. You must make software [development] a repeatable, defined, and managed process.[27]

This attitude toward the acquisition of commercial products, both hardware and software, as a dominant procurement policy was substantiated by Desert Storm, according to General John A. Wickham, Jr., U.S. Army (Ret.). Wickham wrote:

> Many critics believe that NDI (nondevelopmental item or commercial) equipment, which is not militarized or ruggedized, will break down under field operations and fail to satisfy military requirements. But NDI equipment in general continues to perform superbly [re: Desert Storm]. As a result, much of the controversy over NDI has been replaced with recognition that the philosophy of off-the-shelf hardware and software acquisitions for many applications makes good sense and must continue.[28]

Representing the DOD, Strassmann continued his description of future military engagements and consequent military force structures:

> It is the need of small, mobile, rapidly deployed (e.g., fighting anywhere with 48 hours' notice) and locally managed, joint forces that are going to be the focus of our efforts for the next decade and maybe the next two decades. We must look at just-in-time warfare with just-in-time information technology that cannot be cooked, predetermined and prestaged according to a war plan, because the chances are that in most of the engagements we will never be able to execute a war plan that's on the shelf, exactly the way that it's on the shelf.

Strassmann relies on Corporate Information Management (CIM) to reinforce development of these objectives, CIM integrates technology, organizational problem solving, process redesign, and the warfighting doctrine into a whole. However, this holistic approach of Strassmann's is not meant to lead to centralization:

> The objective of CIM is not to scoop everything up into one giant galactic division, because that doesn't work . . . CIM should never be looked at as an information technology project, but primarily as the platform or rails on which a major savings train will be able to proceed with speed, certainty, accurateness, and neatness without derailing.[29]

How do you square centralized, culturally autonomous service-related viewpoints with Strassmann's and his constituents' decentralized approach? Is his pursuit of jointness premature? How do you assess Strassmann's definition of future military engagements and corresponding need for new military configurations? Is his argument for almost exclusive use of off-the-shelf, commercial hardware realistic? Is software the main determinant of interoperable effectiveness?

3 Contemporary Solutions to Past Problems

Many projects are underway to solve interoperability problems associated with Desert Storm. The nature of Desert Storm—a coalition of 19 nations, the battlefield terrain, the adversary, its rapid execution, reliance on high technology, dominance of the air, and minimal casualties—qualifies the operation as a forerunner of one type of future conflict. This assumes there will be no more global wars.

To the contrary, many future armed conflicts will be subconventional,[30] as in Bosnia and Somalia, with the delivery of food and medicine by peacekeeping agencies. Then there are the persistent conflicts as in Northern Ireland with British involvement and in Lebanon with the Syrians where no truce exists and a modest, yet tragic number of casualties continues. Finally, in a third kind of subconventional war the peacekeepers, though numerous and well-armed, are overpowered by the peacebreakers which triggers intervention with countervailing forces and resultant casualties for the adversary. The Gulf war typified this latter scenario and the mid-summer 1993 conflict in Sarajevo, Bosnia-Herzegovina may also qualify.

Again, the warfighting characteristics of the Gulf war serve as a model of required factors; superb aerial reconnaissance; satellite communications; highly technical firepower with precise, accurate aiming capabilities; airborne radar; extensive armor plating, and the necessary electronics to make interoperability seamless, fused, and flexible.

The most likely places in the world for extensive outbreaks of war are

> North Korea, with its acquisition of nuclear arms, and the Muslim crescent running through south-west Asia and north Africa, with its powerful combination of oil, Islam, and a long history of anti-western resentment.

Are there similarities in these regions to that of the Gulf war?

Far from the Gulf, geographically, was the summer 1992 exercise Ocean Venture, designed to refine jointness, particularly in matters of Command and Control including interoperability. A mythical island, Viarta, within the Atlantic Command had been attacked by Jaguar, a neighboring island nation. Viarta asked the President of the United States for help. He agreed and asked the Secretary of Defense to initiate crisis-action planning utilizing Colon, another neighboring island nation, as a forward staging base.

A task force of over 30,000 troops representing the Army (82nd and 101st Airborne Divisions), Air Force, Navy, Marines (28th Expeditionary Unit), Special Forces and Coast Guard were to take and occupy Jaguar. At least two major lessons were learned. First,

> Enlightened as Ocean Venture was, its command-and-control structure applied joint doctrine in a way that would stifle the

> fast-paced performance demanded of today's expeditionary forces."[31]

The reasoning behind this observation related to the Joint Force Air Component Command (JFACC) component approach to jointness. This approach is characterized by a Joint Task Force (JTF) of three or four service components such as the 82nd Airborne Division. In theory, a joint commander can organize these components as he sees fit, for example, working directly with an airborne division. In practice, two or more airborne divisions, for instance, will be combined into an Army Force (ARFOR). This means a joint commander must go through the ARFOR commander to reach the division commander, a cumbersome and time-consuming process, and one certain to deserve the above criticism concerning stifling fast-paced performance.

The second lesson, somewhat related, pertained to Desert Storm's effective but cumbersome ATO—"unfriendly" to users; incompatible with Navy PC's, software, and satellites; and not interactive with the Navy and Marines. Ocean Venture was expected to overcome some of these handicaps.

To establish JFACC for Ocean Venture, Air Force General Walter T. Worthington, head of the Air Force component was named to head JFACC with a Navy flag officer to execute JTF-J3 (operations). Once the ATO had been prepared, JFACC and the Joint Target Coordination Board (JTCB) could modify it to reflect changes in battle situations and JTF priorities. A major addition was the use of the Modular Air Control Center's remote computer terminals; an Air Force contribution that improved performance. Finally, the ATO's length for 1,000 missions was 170 pages instead of Desert Storm's 300 to 700 pages.

How effective was Ocean Venture in refining some of

the interoperability and broader Command and Control processes? One answer came from General Cushman:

> No one in the exercise believed that the Atlantic Command had found the final JFACC solution. Computerization and better communications have improved its performance, and new procedures provide concerned parties a better shot at reflecting their capabilities and needs, but JFACC operations still require substantial streamlining. Further, its process of target coordination negotiation, not bad in principle, suffers from the bureaucracy of the component approach."[32]

What did Ocean Venture represent in terms of the amount of time required to make changes? Again, are Starr's four elements of interoperability applicable as a method of diagnosing some of the problems Cushman refers to? If not why not? What approach would you use? Is there any relation to Cushman's description of JFACC and interoperability? If so, what? If not, why not? Where did interoperability really start and end in Ocean Venture?

4 Communications

To continue a discussion of contemporary changes while on the blue waters, the Navy's Vice Admiral Jerry O. Tuttle maintains:

> Ultra high frequency communications (UHF) are the weak link in the command, control and communications chain. In future conflicts, the Navy must possess super high frequency (SHF) satellite communications for its theater and global communications requirements.[33]

Tuttle's main concern is about jamming. He insists that Saddam's jamming of the UHF satellite communications would have created a difficult situation.

A possible future trend was signaled with the Marine's use of commercial main frame computers and local area networks (LAN) to handle the vast amount of data in Desert Storm. From their force automated services center in Jubail, Saudi Arabia, the Marine expeditionary force command arranged a file transfer of the ATO from Riyadh to Jubail. Then, the air tasking orders were distributed to its units via LAN, often in less than an hour. Similarly, Marine units requested air missions through their air tasking officer who would in turn, validate them and then send the requests to CENTCOM. As to the extent and robustness of LAN during the first 36 hours of the ground war, the Marine's local area networks processed 1.3 million electronic mail messages with no delays, outages, or system degradation.[34]

Local area networks are also part of the Army's future plans. By using fiber optics, millimeter wave radio, and antenna multiplexing, LAN networks will be protected against electronic and visual interception. The networks will possess multiple attributes including voice, digital data, facsimile, graphics, and video imagery.[35]

Many of the newer developments relate to a joint interoperability standard which is currently being established by and for the Department of Defense. Once there is a standard that qualifies and defines data elements, data base, and communication protocols, information can be exchanged among machines. Such an exchange will allow machines "to perform totally different functions in totally different ways using totally different software and languages."[36] This situation represents interface commonality as determined by the joint interoperability standard. As a consequence the electronics industry is searching for systems and techniques to:

> Provide inexpensive interchanges (via translators) among command and control systems . . . to achieve over the longer term an integrated and interoperable command and control system to support combat commanders.[37]

It is evident from this approach that the objectives and general directions of CIM are compatible with the Joint Chief's attempt to enhance interoperability through *C⁴I for the Warrior.* An illustration of how far both entities have proceeded along a common path is JOTS (Joint Operations Tactical Systems) in regard to geographical position reporting (GPS). This system and its instrumentation is valid for many functions within DOD; some apart from direct military consequence. A similar joint use of an information system by combined forces in South Korea was TACCIMS (Theater Automated Command and Control Information Management System).

Standards alone, of course, will not assure interoperability; they are merely a beginning. A much broader framework exists and will exist on the assumption that:

> Each Service will bring its own command and control system to the fray including the Army tactical command and control system (ATCCS), the Navy's Copernicus architecture, the Marine Corps tactical command and control system and the Air Force contingency tactical air control planning system (CTAPS). . . . Each Service brings unique capabilities that make joint warfare effective.[38]

5 Making the Most of Information

Most of the people quoted here place no price tag on planned changes, acquisitions, etc., which perhaps reflects the sensitive and classified nature of such information. They treat information as a free good in the sense that just saying

that "total interoperability" is a justifiable goal makes it so. But this approach is not realistic. What is needed is "enough" information, similar to inventory management models where the costs of ordering inventory are balanced against storage costs and estimated demand and prescribed service levels are the other dimensions. For instance, virtual certainty about information that shapes battle-management decisions will cost a commander more than will 85 percent certainty.

Additionally, the future outlook for interoperability places the process in a "pull" mode wherein a commander seeks the information he needs to make a decision. This contrasts with a "push" mode where a commander is provided with the information someone else thinks he needs. The assumption underlying the pull mode is that commanders know better than anyone else what kind of information they need and when they need it—a classical entrepreneurial or decentralized approach.

A major argument for the pull model is to avoid *information overload,* being at the bottom of a funnel brimming with information from many sources. This argument also assumes that an individual can avoid information overload at will. But exactly what are ideal information levels? How are they derived? How is the value of information determined?

6 Joint Systems Interoperability

It is going to take a long time to reach the degree of interoperability described by General Colin L. Powell: "all the information needed to win the war . . . when he wants it and how he wants it."

C^4I for the Warrior recognized this dynamic situation

with its portrayal of: (1) an immediate or quick fix phase, perhaps during the 1990s, merging into, (2) a mid-term phase into the early 2000s, and (3) a final phase thereafter. The last phase would embrace many of the far-out, almost fantasy-laden inventions and processes that futurists speak of today. With some very basic artificial intelligence models already in place, modest movement toward the dream has taken place. Additional esoterica such as, "multilevel security solutions using a multiple layer concept for encryption, combined with electronic, benign, transparent cryptographic key distribution, automated key management approaches, and data compression and transmission technologies,"[39] will undoubtedly occupy the interests of those in defense-related research and development for many years.

In the meantime, two interoperability assets JTIDS (Joint Tactical Information Distribution System) and IRIDIUM (telecommunications network) continue to attract considerable developmental involvement from both public and private sectors. JTIDS dates back to the late 1960s and, 25 years later may find new applications, beyond AWACs and F-15s, when JTID equipment is placed on F-14 and F-16 aircraft in the mid-1990s. The lessons learned from this extraordinary technological development and the people who have resisted it could be instructive to the believers in total interoperability's resulting primarily from executive fiat.

Interoperability in joint operations has taken many forms, ranging from geographic isolation and coordination in the 12-minute bombing raid in Libya (where the Air Force took the west side and the Naval pilots the east) to the use of an ATO in Desert Storm.[40] An obvious observation: when one service component uses another service's component to strike mutual targets radar must tell each

force's commander what the other force is doing. To accomplish this critical objective, Tactical Digital Information Links (TADILS, see Appendix B) Voice Systems, the Identification of Friend or Foe (IFF), and Tactical Air Navigation (TACAN) were designed.

JTIDS is a nodeless, many-to-many architecture, based on the Time Division Multiple Access design, which uses TADIL J to increase the performance of C^2 over joint forces. With JTIDS, messages can be transmitted over an extended range of 500 miles. Its antijam capability results from the use of spread spectrum and frequency-hopping techniques.[41]

Thousands of participants can be on the link at any one time, which results from the TDMA design. This feature led one observer to characterize JTIDS as "a disc drive in the sky."[42] Other features include position location and identification to JTIDS-equipped elements and a secure system that provides participants with digitized voice capability.

Hill and Ulrich summarized the importance of JTIDS as follows:

> The JTIDS can assist in achieving interoperability among the Services for a wide range of applications. Its deployment on a variety of airborne, shipboard, and ground platforms allows communication of both voice and data among the combatants as well as providing a common grid to these participants. The JTIDS will provide an effective means of coordinating tactical assault and defense activities.

From the history and evolution of JTIDS it is apparent that a joint product, system, effort, or process is bound to run into obstacles from its inception. In the case of JTIDS, which has yet to be fully funded and developed, there was a major conflict between the Air Force and the Navy over

TDMA versus DTDMA.[43] The Air Force preferred the TDMA architecture, being concerned with ground-based jammers and the necessity for the hardware to fit in fighter aircraft. The Navy supported DTDMA to protect its carrier-based battle groups against airborne jamming. Were it not for a DOD/OSD fiat in 1975, which followed a bitterly contested battle, the two services might have had their own systems, or stovepipes, but still not have been able to communicate with each other, according to Hill and Ulrich. As it turned out the Air Force was selected as the executive agent for JTIDS utilizing TDMA.

Are there possible, even probable, similarities between the Air Force/Navy account above and *C⁴I for the Warrior*'s prescription for assigning the JCS Chairman "the responsibility for achieving interoperability among the services?" Continuing, "Through the Military and Communications and Electronics Board (MCEB) and in accordance with the policies of the ASD [Assistant Secretary of Defense, C³I], that responsibility will be focused on identifying and resolving interoperability and standardization issues relevant to joint and combined operations." Similarly, a "Quick Fix Phase" in the same document, calls for "adherence to a common set of joint standards, rigorous testing for conformance and configuration management enforcement."

What is the likelihood of such an agreement? If you were to mastermind such conformance what elements would you like to control? Is financial control over acquisitions adequate? Does the JCS have the required clout with DOD and Congress to prevent "end runs" by services? Is this really the beginning of jointness for interoperability? If not, what obstacles do you see ahead and how would you forestall or overcome them?

7 IRIDIUM

Motorola's futuristic telecommunications network of 77 satellites, as originally planned, was named IRIDIUM after the chemical element with an atomic number of 77. Since then, the original design the number of satellites has been reduced to 66, and the system's transponders have been reduced from 48 to 37. These reductions were to diminish the coverage of the polar regions with their minuscule populations, thereby reducing costs. Whether Motorola will change the name of the system to Dysprosium, the chemical element with an atomic number of 66 is doubtful given the amount of publicity already accorded to IRIDIUM. On the other hand, the word Dysprosium, a rare earth metallic element, is derived from the Greek *dyspros(itos)* which means "hard to get at." Literally, a satellite system like Motorola's might justifiably bear such a name.

The satellites will orbit the earth at a relatively low altitude of 413 miles to assure communications with handheld radio telephones on the earth. This digital, cellular system will allow anyone on earth to reach anyone else on earth within reach of a telephone, regardless of location. Constructed from off-the-shelf technology it is supposed to be working in 1993–94. The government sector is expected to use 18 percent of its capacity; business and private sectors 42 percent and 40 percent, respectively. The satellite-based network will provide both terrestrial communications and coverage within an altitude of 100 miles. IRIDIUM is expected to serve millions of users, ten times the number now served by geosynchronous systems.[44]

Motorola has gone one step further in announcing a new pocket-sized device, named InfoTACH, that allows users of laptop and notebook computers to send and receive data over ARDIS, a national network operated by Motorola and

IBM.[45] Does this complement IRIDIUM?

A more recent development is Globalstar, a subsidiary of L'Oral. Globalstar will provide telecommunication services worldwide. The 48 low-orbiting satellites and local service telephones are scheduled for a 1997 debut.[46]

Given CIM's objective to use more off-the-shelf technology, to say nothing of *C⁴I for the Warrior*'s intentions, should Congress, through military appropriations be supporting IRIDIUM? Given the reduction in the number of satellites and transponders, would the military be justified in subsidizing the costs of IRIDIUM to gain uniform worldwide coverage? In the event, how would you allocate the developmental and operating costs, to say nothing of sharing profits? Or, should IRIDIUM remain totally in the private sector? What are the real differences between the public and private sectors as far as interoperability is concerned? Is it probable that IRIDIUM's projected governmental sector share of 18 percent is too low? On what basis would you predict market share by sector of use? Within what range of error?

8 Cyberspace, the Infosphere, and Interoperability

Cyberspace, a term for electronic space,[47] invites study, especially as it relates to the four information processes or functions: generating, organizing, transmitting, and archiving. Interoperability evolves from these functions to facilitate military decisionmaking. As we reflect on information and decisionmaking, we are reminded of their complexities. Yet seemingly simple goals such as "total interoperability" mask many of the complexities of deciding how and when to meet such objectives. The complexities are diverse and often territorial, as demonstrated by the

Air Force/Navy argument over multiple access alternatives. Consequently, matters of jointness extend well beyond hardware compatibility, for instance. Because the spatial boundaries of information could border on the infinite, information is all the more difficult to manage. Nevertheless, "Cyberspace is a frontier where territorial rights are being established and electronic environments are being differentiated."[48] Military information management has already migrated into that frontier.

Will demands for increased interoperability create unique problems or will existing public and private sector models for controlling information suffice? Who will arbitrate future information overlaps between the two sectors or will existing agencies like the Federal Communications Commission manage? Should some bandwidths be reserved for future needs? On what basis? Who should decide? When? Where?

"The INFOSPHERE, from *C⁴I for the Warrior*, contains the total combination of information sources, fusion centers, and distribution systems that represent the C⁴I resources a warfighter needs to pursue his operational objectives." Does this statement from *C⁴I for the Warrior* portend anything different or unusual about the future need for global capabilities along the lines of C^2 in general and interoperability in particular? If it does, what should be considered?

Future battles will utilize information more than ever before. Additionally, the rules of engagement will differ radically from the past because of the computer. In this regard, consider the offensive use of computer viruses and worms to destroy an enemy's war-making capabilities without launching a single missile.

The cleanliness of such tactics with little or no loss of human life would be welcomed. The devastation would be

primarily economic: retaliation might attempt to destroy the computerized elements of a nation's banks, its airline reservation systems, its telecommunications networks, and its air traffic control processes.

Were these basic utilities to go out, a nation would be stopped and its more conventional war-fighting assets would be valueless, except for war surplus materiel.

These are some of the implications of attempting to achieve a high degree of interoperability in the present and forthcoming Infosphere. No longer science fiction, the future is here, and only interoperability will manage its impact effectively.

NOTES

1. General Colin Powell, "Information Age Warrior," *BYTE*, July 1992.

2. Vice Admiral Richard C. Macke, U.S. Navy, "Information Exchange Poses Enhanced Warrior Prowess," *Signal*, June 1992.

3. Peter Grier, "Data Weapon," *Government Executive*, June 1992.

4. Lieutenant Commander Larry Di Rita, "Exocets, Air Traffic & The Air Tasking Orders, *US Naval Institute Proceedings*, August 1992.

5. Ibid.

6. Captain T. F. Marfiak, U.S. Navy, Comments and Discussion, *Naval Institute Proceedings*, September 1992.

7. Personal communication, Vice Admiral Jerry O. Tuttle, U.S. Navy, Director, Space and Electronic Warfare, Office of the Chief of Naval Operations, "U.N. Navy Seeks to Bolster Communication Weak Link," *Signal*, August 1991.

8. Ibid.

9. Lieutenant Colonel Rick Lewis, U.S. Air Force, "Importance of Centralized Control of Air at Desert Storm," private correspondence, November 1991.

10. The officer based his claim on the Marine AV-8s' flying about 4,000 sorties with 500 kills (13 percent) and Air Force A-10s' scoring 1,400 kills out of 4,000 sorties (35 percent).

11. Air Force Colonel R. Pastusek, private conversation.

12. Ibid.

13. Grier, June 1992.

14. At the time, civilian models could pinpoint a location anywhere on Earth within a 25-meter range and military models were even more precise. By late 1992, with military equipment market open to almost anyone who had the money, military GPS versions with accuracies of 5 yards were readily available. *Economist*, 5 September 1992.

15. Ibid, Dick How, head of the Pentagon's C^3 efforts. JTIDS will be discussed later.

16. Captain Kenneth E. Hill, Jr., and Captain Richard T. Ulrich, U.S. Air Force, "A Case Study of the Joint Tactical Information Distribution System (JTIDS)," unpublished Master's thesis, Naval Postgraduate School, Monterey, California, March 1991.

17. Conversation with Colonel J. David Bryan, U.S. Army, Chief, Architecture and Integration Division (J61), The Joint Staff, May 1992.

18. Conversation with General Jenkins, May 1992.

19. *C^4I for the Warrior*, Joint Staff, June 1992.

20. Chairman, Joint Chiefs of Staff, National Military Strategy *Document*, (NMSD) FY1994–1999, Annex C, (C4), June 1992.

21. From *C^4I for the Warrior*, "Fusion is the process of receiving and integrating all-source, multimedia, and multiformat information to produce and make available an accurate, complete summary that is as timely, but more concise, less redundant, and more useful to the Warrior than if the same information were received directly from separate multiple sources."

22. Captain Mike Macedonia, U.S. Navy, *Military Review*, October 1992.

23. Anthony G. Oettinger, Professor of Information Resources Policy, Harvard University, *C^4I Issues of Control*, National Defense University, Washington, D.C., 1991.

24. General John H. Cushman, U.S. Army (Ret.), in Oettinger 1991, p. 22.

25. Archie D. Barrett, Staff Member, House Armed Services Committee, 1985, in Oettinger 1991, pp. 247, 251.

26. General Robert T. Marsh, Commander, Air Force Systems Command, 1982, in Oettinger 1991, p. 227.

27. Keynote Address, Fourth Annual Software Technology Conference, *Cross Talk, The Journal of Defense Software Engineering*, April/May 1992. Strassmann is Director of Defense Information, C^3I, OSD (Office

of the Assistant Secretary of Defense).

28. General John A. Wickham, Jr., U.S. Army (Ret.), "Desert Storm and the High Technology Debate," *Signal*, March 1991.

29. "Information Technology Use Quenches Combat Cutbacks," *Signal*, August 1991.

30. "Defence in the 21st century," *Economist*, London, 5 September 1992.

31. Lieutenant General John H. Cushman, U.S. Army (Ret.), "Ocean Ventured, Something Gained," *Naval Institute Proceedings*, September 1992.

32. Ibid.

33. Vice Admiral Jerry O. Tuttle, Director Space and Electronic Warfare, Office of Naval Operations, "U.S. Navy Seeks To Bolster Communication Weak Link," *Signal*, August 1991.

34. General Merrill L. Pierce, Jr., U.S. Marine Corps, "Established Architecture Keys Marine Desert Data," *Signal*, August 1991.

35. "Communications in Future Will be Automated, Secure," *Signal*, March 1991.

36. Vice Admiral Richard C. Macke. U.S. Navy, director of C^3 for the Joint Staff, "Information Exchange Poses Enhanced Warrior Prowess," *Signal*, June 1992.

37. Ibid.

38. Ibid. (Macke).

39. *C^4I for the Warrior*, Joint Staff, June 1992.

40. Hill and Ulrich, "JTIDS."

41. Hill and Ulrich, "JTIDS." "Spread spectrum is used to describe a class of modulation techniques in which the data stream is coded in such a way that the total transmission bandwidth is greater than the information bandwidth. If the spectrum spreading is done properly, the transmitted signal looks [sounds] to the unauthorized listener like wideband noise." As to frequency hopping, "it is a jammer evasion

strategy rather than one which tries to resist or overcome the jammer. As the name implies, it is generated by hopping the signals in frequency. JTIDS is considered to be a fast frequency hopping system (thousand hops per second). But it is the dwell time (the number of hops per second) that is regarded as the single most important determination of jammer evasion capability. The shorter the dwell time, the greater the probability that the system will evade the jammer."

42. Dr. Carl E. Ellingson, Hill and Ulrich, "JTIDS."

43. Distributed Time Division Multiple Access (DTDMA), was fostered originally by the Navy to take advantage of its then existing organizational structures and to make use of existing TADILS. It is a channel-oriented architecture designed to permit separate concurrent communication channels.

44. Robert H. Williams, "Iridium Offers Contact to Any Point on Earth," *Signal*, February 1991.

45. "Motorola's Device Allows Laptops to Talk Via Radio," *Wall Street Journal*, 15 September 1992.

46. *Business Week*, 26 July 1993, p. 72.

47. Anne W. Branscomb, "Common Law for the Electronic Frontier," *Scientific American*, September 1991.

48. Ibid.

APPENDIX A AIR TASKING ORDER—SANITIZED ILLUSTRATION

```
MSNDAT/3015C/ZAF/BASSET 15/4F16/INT/-/4C872/-/23015/36435//
TGTLOC/240015Z/240030Z/-/SUPPLY/301623N0472624E/2M0971Z//
REFUEL/GUPPY 07/6307A/MANGO PST HIGH/ALT:200/242330Z/20/TAD07//
REFUEL/GUPPY 10/6310A/MANGO PST HIGH/ALT:205/242330Z/20/TAD10//
AMPN/ REMARK IDENTIFIER(S): A E V//
MSNDAT/3021C/ZAF/ROVER 21/4F16/INT/-/4C872/-/23021/36441//
TGTLOC/240030Z/240040Z/-/SUPPLY/301623N0472624E/2M0971Z//
REFUEL/GUPPY 07/6307A/MANGO PST HIGH/ALT:200/242345Z/20/TAD07//
REFUEL/GUPPY 10/6310A/MANGO PST HIGH/ALT:205/242345Z/20/TAD10//
AMPN/ REMARK IDENTIFIER(S): A E V//
MSNDAT/0501F/EAF/HUSKIE 01/8F16/INT/-/2M842/-/20501/36401//
TGTLOC/240530Z/240545Z/B1327CANC09/TUNNEL/334822.9N0442714.9E//
REFUEL/WALLEYE 14/6314B/RAILROAD PRE/ALT:200/240320Z/90/TAD14//
REFUEL/PIKE 26/6326S/RAILROAD PST/ALT:200/240600Z/56/TAD26//
AMPN/ REMARK IDENTIFIER(S): A C F P Q//
NARR/ UNIT REMARKS:  388TFW
UNIT REMARKS A
SEE TANKER SPINS FOR AAR INFO.
UNIT REMARKS C
CONTACT CENTRAL AWACS.  USE CENTRAL COMM PLAN.
UNIT REMARKS E
CONTACT EAST AWACS, USE EAST COMM PLAN.
UNIT REMARKS F
IF TGT WX PREVENTS EXPENDING ON PRIMARY TGT, PLAN MEDIUM ALT RETURN
ROUTE OVER GUARDS AREA.  TGT COORDS WILL BE PASSED FROM ASARS VIA
AWACS.
UNIT REMARKS P
YOU ARE PACKAGE COMMANDER.
UNIT REMARKS Q
COORD WITH 0551C, 0555C, 8 (F15, 1 TFW), 0561W (4 F-4G) 0575X
(2 EF-111),0573R (2 RF-4).
UNIT REMARKS V
IF ACTIVE SAM SITE OBSERVED PRIOR TO ATTACK, ATTACK SAM SITE. DO
NOT TROLL FOR SAMS.  KILL ZONE AF7 NE IF PRIMARY TGT NOT ACQUIRED.
UNIT REMARKS W
EXPECT REFUELING AFTER SCRAMBLE IN PAM OR TANGERINE A/R TRACKS.//
TASKUNIT/801PBW//
MSNDAT/5210B/ZZF/REAVER 10/3B52G/INT/-/4517L/-/25210/35230//
TGTLOC/242020Z/242100Z/B1427-CA1216/TROPO/363039N0432525W//
AMPN/ REMARK IDENTIFIER(S): A B C D E//
MSNDAT/5213B/ZZF/REAVER 13/3B52G/INT/-/4517L/-/25213/35233//
TGTLOC/242020Z/242100Z/B0427-01106/PWRSTA/363122N0524523W//
AMPN/ REMARK IDENTIFIER(S): A B C D E//
NARR/ UNIT REMARKS:  801PBW
UNIT REMARKS A
SEAD, CAP, SWEEP, COMM,SAFE PASSAGE, AND AIR REFUELING MUST BE
COORDINATED WITH JTF.

UNIT REMARKS B
SQUAWKS ARE FOR LEAD AIRCRAFT.
UNIT REMARKS C
ADJUSTMENTS TO TOTS, PACKAGE AND MISSION NUMBERS, AND SQUAWKS MAY
BE MADE PER JTF DIRECTION.  CENTAF WILL TRACK YOUR MISSION WITH
CENTAF ALLOCATED DATA.
UNIT REMARKS D
ADVISE 17AD(STRATFOR BOMBER PLANS) ASAP OF ANY DEVIATIONS FROM ATO.
UNIT REMARKS E
ALTERNATE TARGET IS EW SITE. BE 1340CAC392
OBJECTIVE-DESTROY/DAMAGE ATENNAS. AND SUPPORT BUILDINGS//
TASKUNIT/1612 MAS//
```

ANNEX 33 TO CHAPTER 3
AIR TASKING ORDER/CONFIRMATION (ATOCONF)

1. GENERAL

The ATOCONF is used to task intra-service organizations, to inform the requesting command and the tasking authority of the action being taken, and/or to provide additional information about the mission(s).

If the message requires changes or corrections, a Message Change Report may be used. The changes may be transmitted as another ATOCONF message identified as a deviation in Field 5 of the MSGID set, using a REF set to identify the original ATOCONF message. The PERID set specifies the period for which the message is effective.

This message includes the effective time period, tasked unit(s), and basic mission information: mission number, request number, priority, mission type, time on and off target, alert status, location, call sign, number and type of aircraft, ordnance type, IFF/SIF mode and code, and time and target location.

2. MESSAGE MAP

EXER/exercise name/additional identifier//

OPER/operation name/plan originator and number/option name/second option name//

MSGID/ATOCONF/originator/message serial number/month/qualifier/qualifier serial number//

REF/serial letter/(usmtf message short title) or (type of reference)/originator/date-time group /(msg ser number) or (DOCSN: doc ser number)/special notation/(sic) or (filing number)//

AMPN/free text to explain preceding reference set//

NARR/free text to explain preceding reference set//

CANX/(usmtf message short title) or (type of reference)/originator/date-time group /(message) or (document) serial number/special notation/(sic) or (filing number)//

PERID/time from/TO: time to/ASOF: as of time//

AIRTASK/air tasking/air tasking comments//

TASKUNIT/tasked unit designator/ICAO location/comments//

MSNDAT/mission number/package identification/aircraft call sign/number and type aircraft /mission type/alert status/primary configuration code/secondary configuration code /iff-sif code and mode//

MSNLOC/mission start day-time/mission stop day-time/mission location name /(altitude) or (flight level)/air support request number/area coordinates//

TGTLOC/day-time on target/day-time off target/target identifier/target type /desired mean point of impact/air support request number/target comments//

RECDATA/request number/mission priority/day-time on target/latest time information of value /reconnaissance mission type//

TRCPLOT/location of initial point/type area/trace point location//

CONTROL/type of control/callsign/(primary frequency) or (primary frequency designator) /(secondary frequency) or (secondary frequency designator)/report-in point/control comments//

FACINFO/callsign/primary (frequency) or (frequency designator)
/secondary (frequency) or (frequency designator)/report-in point/support unit identity
/control comments//

ELECMBT/aircraft call sign/priority/mission location/(altitude) or (flight level)/time on station
/time off station/primary (frequency) or frequency designator)
/secondary (frequency) or (frequency designator)//

REFUEL/tanker call sign/tanker mission number/air refueling control point
/(altitude) or (flight level)/air refueling control time/total off-load of fuel
/(primary frequency) or (frequency designator)/secondary (frequency) or (frequency designator)//

7REFUEL

/MSNNO	/ACSIGN	/NOTPAC	/OFF	/ARCT	/TNKR	/FUEL	/CMNT
mission number	aircraft call sign	number and type/model of aircraft	total off-load fuel	air refueling control time	tanker assignment	refueling fuel type	receiver comments//

AKNLDG/aknldg/(INST: aknldg instructions) or (force or unit required to aknldg)//

DECL/downgrading instructions//

NOTE: Sets PERID, AIRTASK, TASKUNIT, and MSNDAT are mandatory. You also must use one (but only one) of sets MSNLOC, TGTLOC, and RECDATA.

3. ENTRY LISTS

The ATOCONF uses the following entry lists.

LIST NUM	TITLE
11	Location
20	Target Type
107A	Mission Type
178	Reconnaissance Target Type
513	Aircraft Type
2005	Air Tasking Type

ATOCONF ATOCONF

```
PERID/300001Z/TO:302359Z/ASOF:010930Z//
      6       7       8
AIRTASK/PACKAGE/13//
        9      10
TASKUNIT/1TFW/KLBI/WEAPONS CONFIGURATION CHARLIE//
          11    12          13
MSNDAT/AF0001/1A/KILLER 10/4F111E/INT/45M/ACO1/ACO2/21111//
        14   15    16        17    18
```

THE ABOVE EXAMPLE IS NOT INTENDED TO DEPICT AN ACTUAL MESSAGE. USE IT AS A GUIDE FOR COMPLETING INDIVIDUAL SETS.

EX	SET NAME FIELD NAME	CAT S F	Number of Characters	EXPLANATION
		o	1-20X	Place name (town, terrain feature, etc.)
13	comments	o	1-68X	Enter additional comments concerning the tasked unit. If you need more space, add a free-text set. NOTE: Sets MSNDAT through 7REFUEL form a nested segment. Repeat them as a group to report multiple unit tasking. You must repeat the sets in theiroriginal order. You must include the mandatory sets in each repetition.
	MSNDAT	m		Use this set to give basic tasking/confirmation information for air missions.
14	mission num	m	1-8X	Enter the mission number.
15	package id	m	1-3ANS	Enter the package identification number for the assigned mission.
16	call sign	m	1-12X	Enter the call sign assigned to the mission aircraft.
17	notpac	m	3-8ANS	Enter the number and type of aircraft as follows:
			1-2N	• Enter the number of aircraft.
			2-6ANS	• Then enter the code for aircraft type/model. *ENTRY LIST 513*
18	mission type	m	2-5AN	Enter the type of mission. *ENTRY LIST 107*

EX	SET NAME FIELD NAME	CAT S F	Number of Characters	EXPLANATION
19	alert status	m	2-3AN	Enter the alert status from one of the following: ALERT STATUS — CODE Alert time — One-two digits followed by M or H to signify five -minute or one-hour intervals. Runway alert — RUN Battle stations — BAT Red (2-5 min for Marine units) — RED Yellow (15 min for Marine units) — YEL White (30-60 min for Marine units) — WHT Other (explain in a free-text set) — OTR
20	primary config code	m	1-5AN	Enter the primary configuration code for the aircraft.
21	secondary config code	m	1-5AN	Enter the secondary configuration code for the aircraft.
22	iff/sif code	m r	3-5AN	Enter the IFF/SIF (Identification Friend or Foe/Selective Identification Feature) mode and code as follows:
			1AN	⊗ Enter the mode (1, 2, or 3)
			2-4N	⊗ Then enter the code: 00-03, 10-13 through 70-73 for mode 1; 0000-7777 (omit 8's and 9's) for modes 2 and 3.
	MSNLOC	c r		This set is mandatory if TGTLOC or RECDATA are not used. Enter mission location information.
23	mstart	m	7AN	Enter the mission start time using two digits each for day, hour, minute and one letter for time zone.
24	mstop	m	7AN	Enter the mission stop time using two digits each for day, hour, minute and one letter for the zone.
25	location name	o	1-20X	Enter the name for the mission location.
26	ALT:	o	1-3N	Enter the field descriptor, then the altitude in hundreds of feet. OR

APPENDIX B THE TADIL COMMUNICATIONS LINK

A TADIL, according to Hill and Ulrich, is "a JCS approved standardized communications link suitable for transmission of digital information and characterized by standardized message formats and transmission attributes."36 Since these two factors are standardized, two or more operational centers, for example, weapon systems, can be connected. TADILS, utilizing computers, can pass the shared data in digital form among tactical forces C^2 units at or near real-time. Then the processed information can be shown on either symbolic situation or alphanumeric tabular displays.

Variations of TADILs that have been developed include:

- TADIL A, a secure, netted data link, used by the Navy primarily to exchange and broadcast, air, surface, and subsurface tracks between ships. It can also support electronic warfare. The architecture is many-to-many or one player can send and receive tracks to and from all players.

- TADIL B, a secure, point-to-point data link utilizing serial transmission frame characteristics and standard message formats. Its prime purpose is to connect tactical air defense and air control units. Being a serial system, it passes information from one player to another to another, etc. This one-to-one architecture differs from TADIL A.

- TADIL C, a time division multiple access data transmission (TDMA)[1] link between a control station and controlled aircraft. Used primarily by the Navy for automatic transmission of orders, status, and other information to interceptors. The link architecture is one-to-many and many-to-one or a message can be broadcast by one control station to many aircraft with all of the aircraft being able to respond to one control station.

TADILS A, B, and C offer proven advantages, as indicated above. However, none of them can be protected against jamming, and TADIL C is not secure. Also, processing time is somewhat limited as is the number of players per link: TADIL A, 20 players; TADIL B, two players; and TADIL C, eight players.

Voice systems are generic, common to all combat elements with many-to-many architecture if the players are tuned to the same

frequency. Typically they are not secure nor do they offer jamming protection. However the new Mark XV IFF system is designed to provide jam protection for the ETIDS identification system.[2]

IFF systems include interrogators, transponders, processing equipment, and related antenna systems enabling aircraft to identify themselves to air defense sites or other aircraft.

TACAN (Tactical Air Navigation) system provides an aircraft with a position location relative to a ground-based TACAN transponder. Once a position is determined, pilots using TACAN maps determine their grid location. Its architecture is many-to-one and one-to-many. Since the location is relative to the transponder for a particular aircraft, a common grid among aircraft may not be possible.

Eight criteria may be used for evaluating the components of an Existing Tactical Information Distribution Systems (ETIDS): (1) jamming protection; (2) security; (3) capacity, i.e., number of participants per link at any one time; (4) information flow, i.e., ability of system to deliver information from one person to another; (5) interoperability, i.e., ability of system components to talk and transmit information to each other; (6) common grid, i.e., the participants' common reference point; (7) survivability, i.e., the system's ability to continue providing users with information after the loss of a piece of the system; (8) coverage, the distance information can be transmitted.

None of the TADILS, Voice, TACAN, nor IFF systems meet all of these criteria or ideal objectives. Even considering interoperability, some services have some compatible equipment but they do not share common procedures and codes. Consequently, the TADILS had to be constantly refined to meet the objective of a joint control and identification system that allowed many users to participate over great distances with secure messages and jam protection. TADIL J was developed for these purposes.

NOTES

1. Time Division Multiple Access (TDMA) is the most popular method for separating channels or users on a common communication medium. Essentially, TDMA architecture provides time slots for message traffic. Assignments to the slots are accomplished by a Net Time Reference (NTR) terminal which also refers such assignments to the nodes.

2. Mark XV is also known as SINGARS (Single Channel Ground Air Radio), the standard radio system used by the Army and Marines.

McNairPapers

The McNair Papers are published at Fort Lesley J. McNair, home of the Institute for National Strategic Studies and the National Defense University. An Army post since 1794, the fort was given its present name in 1948 in honor of Lieutenant General Lesley James McNair. General McNair, known as "Educator of the Army" and trainer of some three million troops, was about to take command of Allied ground forces in Europe under Eisenhower, when he was killed in combat in Normandy, 25 July 1944.

1. Joseph P. Lorenz, *Egypt and the New Arab Coalition*, February 1989.
2. John E. Endicott, *Grand Strategy and the Pacific Region*, May 1989.
3.Eugene V. Rostow, *President, Prime Minister, or Constitutional Monarch?*, October 1989.
4. Howard G. DeWolf, *SDI and Arms Control*, November 1989.
5. Martin C. Libicki, *What Makes Industries Strategic*, November 1989.
6. Melvin A. Goodman, *Gorbachev and Soviet Policy in the Third World*, February 1990.
7. John Van Oudenaren, "The Tradition of Change in Soviet Foreign Policy," and Francis Conte, "Two Schools of Soviet Diplomacy," in *Understanding Soviet Foreign Policy*, April 1990.
8. Max G. Manwaring and Court Prisk, *A Strategic View of Insurgencies: Insights from El Salvador*, May 1990.
9. Steven R. Linke, *Managing Crises in Defense Industry: The PEPCON and Avtex Cases*, June 1990.
10. Christine M. Helms, *Arabism and Islam: Stateless Nations and Nationless States*, September 1990.
11. Ralph A. Cossa, *Iran: Soviet Interests, US Concerns*, July 1990.
12. Ewan Jamieson, *Friend or Ally? A Question for New Zealand*, May 1991.
13. Richard J. Dunn III, *From Gettysburg to the Gulf and Beyond: Coping with Revolutionary Technological Change in Land Warfare*,
14. Ted Greenwood, *U.S. and NATO Force Structure and Military Operations in the Mediterranean*, June 1993.
15. Oscar W. Clyatt, Jr., *Bulgaria's Quest for Security After the Cold*

War, February 1993.
16. William C. Bodie, *Moscow's "Near Abroad": Security Policy in Post-Soviet Europe*, June 1993.
17. William H. Lewis (ed.), *Military Implications of United Nations Peacekeeping Operations*, June 1993.
18. Sterling D. Sessions and Carl R. Jones, *Interoperability: A Desert Storm Case Study*, July 1993.