

NATIONAL DEFENSE UNIVERSITY
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

Lessons From Bosnia:

The IFOR Experience

Edited by Larry Wentz



DoD Command and Control Research Program

Assistant Secretary of Defense (C3I)
Mr. Anthony Valletta (Acting)
Deputy Assistant Secretary of Defense (C3I) Acquisition
Dr. Margaret Myers (Acting)
Executive Agent for CCRP
Dr. David S. Alberts
Mr. Larry Wentz* (Acting)

Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors. They do not necessarily represent the views of the National Defense University, the Department of Defense, or any other U.S. Government agency. Cleared for public release; distribution unlimited.

Portions of this publication may be quoted or reprinted without further permission, with credit to the Institute for National Strategic Studies, Washington, D.C. Courtesy copies of reviews would be appreciated.

Library of Congress Cataloging-in-Publication Data

Lessons from Bosnia / edited by Larry K. Wentz.

p. cm.

Includes bibliographical references.

ISBN 1-57906-004-8

1. Yugoslav War, 1991- --Participation, American. 2. Yugoslav War, 1991- --Bosnia and Hercegovina. 3. IFOR (Organization)--History. 4. National security--Bosnia and Hercegovina. 5. United States--History, Military. 6. Bosnia and Hercegovina--History, Military. I. Wentz, Larry K.

DR1313.7.F672U656 1997

949.703--dc21

97-38128

CIP

*as of January 1998



Lessons From Bosnia: The IFOR Experience

**Contributing Editor
Larry Wentz**



Contents

Foreword	xi
Acknowledgments	xv
Preface	xix
I. Introduction	1
II. Bosnia—Setting the Stage	9
III. Command and Control Structure	35
IV. Intelligence Operations	53
V. Civil-Military Cooperation	119
VI. The International Police Task Force	139
VII. Information Activities	167
VIII. Tactical PSYOP Support to Task Force Eagle	189
IX. Counterintelligence and HUMINT	225
X. Information Operations in Bosnia: A Soldier’s Perspective	255
XI. C4ISR Systems and Services	273
XII. NDU/CCRP Bosnia Study	379
XIII. Lessons Learned About Lessons Learned	397
XIV. Summary	409
End Notes	445

Appendix A: The Dayton Peace Agreement Summary	467
Appendix B: Chronology of IFOR Events	475
Appendix C: References	481
Appendix D: Acronyms	489
About the Contributing Editor	501
About the Authors	503

X. Information Operations in Bosnia: A Soldier's Perspective

Kenneth Allard

My arrival at the headquarters of the US 1st Armored Division in Tuzla, Bosnia, in May 1996 came some 5 months following its deployment as the principal U.S. peacekeeping force committed to *Operation Joint Endeavor*. As the senior NATO observer for that sector, I participated in field and aviation operations in four of the five maneuver brigade areas, observing U.S. and allied contingents comprising MND(N) of the IFOR and paying particular attention to command and control issues. While no outside observer could acquire the in-depth knowledge possessed by the dedicated men and women who had lived this mission from its inception, the tradeoff lay in the insights gathered from soldiers at many levels, from the division to the foxhole and from units deployed throughout the area of operations. While these observations were inevitably snapshots, the issues highlighted here seem especially relevant as lessons for the future.

In assessing these very preliminary findings, however, it is important to provide an operational context, since heat rather than cold, and dust rather than mud, now affected the missions of *Operation Joint Endeavor*. Even more remarkable were the “life support systems” which had transformed the primitive mud pits of

January into the elaborate base camps of May—some of which rivaled or surpassed the facilities in Germany from which the troops had come. Above all, the political and social atmosphere of Bosnia itself was the constant backdrop to the mission. An uneasy calm prevailed throughout the region, with shooting largely confined to occasional incidents of “celebratory firing” by drunken members of the local populace, factional demonstrations in the form of cemetery visits or soccer rallies, and constant tension over the issue of apprehending war criminals. All the forces participating in *Operation Joint Endeavor* supported the various international teams delivering humanitarian relief, investigating war crimes, supervising elections, and preparing for the long process of reconstruction. But the principal IFOR military functions were to provide the security forces that controlled the countryside, patrolling the zone of separation between the former warring factions, and carrying out the force demobilization and weapons cantonment provisions of the Dayton Accords.

Inspections of each declared weapons site were ordered in specific instructions issued to the brigades. The results of those inspections (and weapons totals) were tracked through databases maintained by the division G-2. Despite this systematic approach, there were almost daily instances in which weapons—sometimes major ones, like tanks and air defense guns—were discovered outside cantonment areas. Some of these occurrences appeared to be the result of honest mistakes, but in others there appeared to be either creative bookkeeping by the factions or outright attempts at concealment. The most consistent estimate was that possibly 70 percent of these weapons holdings had been accounted for, since Bosnia has a history, culture, and geography favoring concealment from outside powers.

In carrying out these missions, the U.S. force commander was explicit in ordering that “all operations be deliberate, coordinated and documented.” This guidance was strictly followed, with more similarities between the brigades than differences. Each patrol featured an effective combination of combat power, pre-planned air and fire support, multilevel communications, area knowledge,

and at least some effort to appreciate the situation of the local populace. The only real differences were in the application of the principle of force protection. The four-vehicle convoy rule was rigidly enforced in every U.S. unit, but somewhat more relaxed in the multinational units, where one- or two-vehicle administrative movements were the norm. On patrols, however, three-vehicle convoys regularly featured at least three armored vehicles for consistent firepower and personal protection. And in both the U.S. and the multinational units, patrols consistently wore Kevlar helmets, flak jackets, and personal sidearms with magazines inserted.

Reality Versus Perception

The military tasks flowing from the varied functions of IFOR underlined both the importance of information in modern military operations and the difficulties of adapting traditional structures to new missions and technologies. The reality of Bosnia presented an uneven picture of progress and problems that contrasted sharply with inside-the-Beltway perceptions. Defense trade publications regularly featured stories about the high technology supporting the Bosnian operation—complete with seductive images of electronic maps, gigabytes of computer-transmitted information, and live imagery from UAVs. As one Washington-based official exclaimed, “...with huge bandwidths and powerful computers, we can get intelligence to where it is needed—Humvees, cockpits, ships.”

Because information is the lifeblood of any modern military operation, an unprecedented amount of data indeed flowed from Washington to European headquarters and intermediate staging bases. A family of wide-area networks, for example, connected NATO headquarters with the IFOR in Bosnia, passing operational and intelligence messages to the 33 nationalities comprising the coalition. The Internet was also used for everything from “morale messages” exchanged between the troops and their families to home pages carrying frequent public affairs updates. A generation of painstaking efforts in the arena of NATO communications stan-

standardization had paid off as well, with systems that provided an essential baseline of interoperability for IFOR's coalition partners. In one memorable nighttime mission that I witnessed, a close air support mission over northern Bosnia featured British Harriers vectored by offshore NATO AWACS aircraft to Norwegian forward air controllers providing direct support to a Swedish-led brigade.

But elaborate information flows between higher command levels did not always translate into better support for the warfighter. In fact, life in Bosnia had not changed very much for the American soldier, because the information revolution largely seemed to stop at division level. Despite the techno-hype, subordinate brigades and battalions typically conducted operations much as they had 20 years before, with acetate-covered 1:50,000 maps, outdated communications gear, and only those sensor or reconnaissance systems organic to ground units. Unlike the popular image of a Tom Clancy "Ops Center," most tactical command centers (see figure 10-1) looked much as they had in other wars—usually housed in tents, semi-destroyed buildings, or the back ends of armored vehicles. To add in the effects of mountainous terrain (limiting line-of-sight communications), weather (either cold and muddy or hot and dusty), and computer viruses (sophisticated and ubiquitous) was to confront the new as well as the enduring qualities of military life in the field. In the apt summation of one U.S. Army general in Bosnia, "Soldiering is still an outdoor sport." And as always, the ingenuity and dedication of U.S. and NATO soldiers were critical in coping with these challenges.

Command and Control

It is important to recognize that the specter of the failed peacekeeping mission in Somalia pervaded much of what went on in Bosnia. In its aftermath, the fundamental question of "Who's in charge?" had become virtually synonymous with the dread specter of U.S. troops serving under foreign command. In practice, the 40-year history of NATO command arrangements had long since pro-



Figure 10-1. Tactical Command Center in MND(N)

duced the compromise of OPCON—a kind of leasing arrangement in which the designated NATO commander directed the actions of national elements while not interfering in their internal functions. NATO's first out-of-area operation nevertheless raised almost daily "rendering unto Caesar" questions as various national elements—the United States among them—carefully weighed alliance perspectives against national interests. But on the whole, these issues were well managed through military professionalism, with newly established soldier-to-soldier relationships being especially important in the integration of the Russian brigade attached to IFOR (see below).

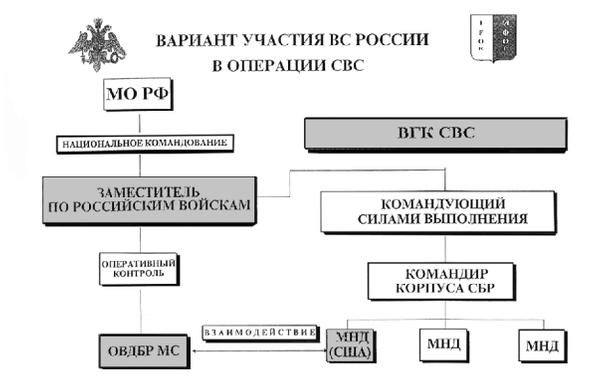
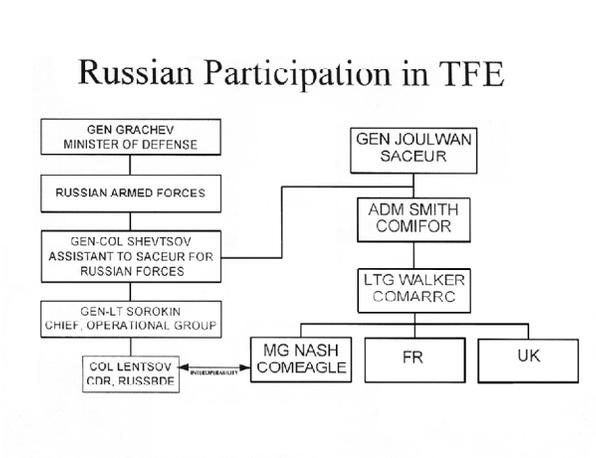
In contrast, the largest single command and control problem in Bosnia was the failure of the Dayton Accords to designate a single authority to synchronize the military, political, and humanitarian aspects of the mission. As shown in figure 10-2, the relatively clean lines of NATO command and control contrasted sharply with the complicated and ambiguous arrangements handicapping the already difficult tasks of reconciliation and reconstruction. Especially in the American sector, civil affairs units (largely drawn from Reserve components) were used to good effect by brigade and

battalion commanders whose culture emphasized initiative, accountability, and deadlines. Lacking either corresponding capabilities or these cultural attributes, their civilian counterparts were painfully slow in organizing the reconstruction efforts on which reconciliation ultimately depends. Not surprisingly, the humanitarian side of the mission consistently failed to keep pace with the improved security situation.

The Russian Brigade

I began an interview with the deputy commander of the Russian brigade by asking about the integration of Russian forces within IFOR. His indignant answer was, “What do you mean, integration?!” Rather than being integrated, the Russians regarded the formal relationship between the Russian brigade and the U.S.-led division as a friendly affiliation between equals. “They ask us to do things and we do them.” This comment illustrates a not-well-understood aspect of Russian participation. The accompanying illustration (see figure 10-3a) of the NATO version of those command relationships shows an OPCON relationship connecting the Russian brigade to the SACEUR through his Deputy for Russian Forces. The relationship between the brigade and the U.S. division was described in the NATO documents as TACON, essentially the authority to direct tactical movements and missions. Also shown, however, is the Russian version (figure 10-3b) of this same relationship. Their word for OPCON is “operativny kontrol”—the same term used in Soviet military science to define military control at the operational level, particularly the control of those formations known as “operational maneuver groups.” What NATO understands as TACON is translated by the Russians as “vzaimodestvya” or “interoperability”—connoting a relationship based on equality. As a practical matter, however, day-to-day operational matters were handled informally and effectively between Major General William Nash, the U.S. division commander, and Major General Alexander Lentsov—through a close personal relationship based on their com-

Figure 10-3. OPCON Relationships



mon professionalism as soldiers. More difficult questions, such as the assignment of Russian soldiers away from their assigned sector, were resolved through the illustrated command relationships.

Whatever term might have been strictly applied, there was a high degree of operational integration between the Russian brigade and other divisional units. Aviation support, intelligence, reconnaissance, and surveillance were tightly coordinated as well as requirements for inspections and other missions. The Russians appeared to respond best to written orders, which they considered more binding than verbal instructions. And while many NATO armies routinely perform “implied and specified tasks” in any mission, this was emphatically not standard Russian practice. From General Lentsov on down, there was a notably “strict construction” in the way the Russian brigade defined and performed its military tasks. Given this emphasis, there were some otherwise routine civil affairs functions that either were not performed or not reported because the Russians saw no reason to do so, including water supply, home reconstruction, and personality profiles of key local leaders. Indeed, the ubiquitous American reporting style (up to six daily medical reports, for example) and paperwork burden had to be greatly simplified for the Russians—something which their U.S. counterparts could only envy.

Because they were hand-picked for this mission, the Russian brigade projected themselves as a tough, competent force. Their base camps were invariably well-chosen with competently sighted weapons and comprehensive entrenchments. In the field, their tactical communications tended to be slow and unreliable. The FM radios were made compatible with the American SINCGARS system by the simple expedient of turning the squelch off, an arrangement similar to that used between the Army and the Marines during Somalia. Oddly enough, the Russians typically featured less frequent and more decentralized reporting requirements, so that it was standard practice on some key missions to deploy a U.S. liaison officer equipped with a TACSAT radio with a direct link to division headquarters. On joint patrols, Russian junior officers were well organized and tactically proficient (see figure 10-4). However, they



Figure 10-4. U.S. soldiers and Russian paratroopers conduct a routine joint patrol operation south of Brcko, Bosnia-Herzegovina, in the Russian Brigade's sector.

were often matter-of-fact about some things the United States takes more seriously: mission planning and briefings; delineation of specific objectives; integration of combined arms at the lowest levels; and after action reviews. Their cooperation and enthusiasm for working with NATO, were beyond reproach.

Use of Information

In both the NATO and U.S. contingents, reductions in headquarters and staffs have not matched post-Cold War cutbacks in force structures. While organizational featherbedding is often the first rule of combined operations, redundant hierarchies are no match for the speed and efficiency of decentralized electronic networks. Therefore, it was not unusual for information broadcast by these networks to be shared far faster than corroborating data succes-

sively reported through each layer in the chain of command. In a practice known as “skip-echeloning,” both Washington-based commands and IFOR headquarters elements occasionally used these networks to bypass intervening organizations in order to exchange information requirements firsthand—sometimes leaving the broader community in the dark. The Division Chief of Staff described how on several occasions watch officers at the headquarters were directly called by the White House Situation Room and other higher headquarters to confirm information apparently available at those levels but not until that moment known by the on-scene commander.

These hierarchical structures and the intensely political nature of *Operation Joint Endeavor* prompted floods of information at the operational level. Put simply, data was the preferred means of disciplining American forces, often to the point of micro-management. By the mid-point of the operation, some 1,200 “fragmentary orders” had been transmitted by the division to its subordinate units. And each evening at the U.S. headquarters in Tuzla, a “battle update briefing” prepared by the division staff covered the day’s events in excruciating detail. More than 120 PowerPoint slides were typically used to highlight the latest operational and intelligence developments as well as to pinpoint a host of administrative issues, such as the number of sandbags used to protect base camps. These briefings and the accompanying slides were regularly transmitted back to the higher U.S. headquarters monitoring the operations. These set-piece briefings, so reminiscent of the “Five O’Clock Follies” of the Vietnam era, promoted a ubiquitous and even hyperactive reporting regime which regularly led to cultural clashes, only some of which were a function of different nationalities. According to one harried executive officer at a U.S. brigade: “During the last incident in our sector, seven of our nine phone lines were tied up answering questions from the division staff.” Multiple taskings and overlapping reports were similarly cited as problems in both the U.S. and coalition brigades. However the multinational units at least found ways to cope with what they regarded as a uniquely American addiction to data requirements. “We take what we need,” one allied brigade commander pointed out with exquisite tact.

Media and Public Affairs

The media—the quintessential network—suffused the entire Bosnian mission, provoking ambitious efforts by NATO and U.S. public affairs officers to make full use of information as a weapon of peace. Especially in the U.S. sector, with its 12-nation contingent, the formation of a joint information bureau was an important step in using information as a means to provide timely and accurate information as well as to influence compliance with the Dayton Accords. Not only was this bureau run with an international staff, but its director became central to the functioning of the command group, providing daily advice to the division commander and operating in close partnership with the operations, intelligence, and civic affairs elements. The importance of these relationships could be seen in a June 1996 incident, when the Associated Press wrongly reported that Serb General Ratko Mladic (an indicted war criminal) had faced down IFOR soldiers, forcing them to withdraw. Within minutes of the story's filing on the AP wire, alarm bells went off at headquarters from Sarajevo to Washington. Although the U.S. commander in Tuzla and his public affairs staff were instantly besieged with phone calls, it took more than 24 hours to ensure that an accurate version of this event had been reported. Because such an act of deliberate or accidental “disinformation” could take on a life of its own through a tightly wired global information grid, the management of perceptions became an important and continuing mission. Precisely for that reason, hard-pressed U.S. commanders regularly sought out local media opportunities, including, in one instance, a regular guest slot on a Bosnian radio call-in show. The lesson learned: in peace operations, as in other politically charged conflicts, perception is the reality.

Communications and Automation

The Army communications system generally worked well in Bosnia, but only at great costs in manpower and effort. As in the past, radio transmissions dominated tactical communications. Because most Army tactical radios operate on line-of-sight transmissions, it was essential to place repeaters and relays on mountain tops. But with large numbers of radio nets required for the 15 brigades operating in the U.S. sector, there was a real problem with interference (“signal fratricide”). Ironically, even in one of the world’s most mountainous regions there was only so much high ground to go around. Since these critical relay sites had to be fortified and defended, support requirements typically consume 7-8 percent of combat manpower in addition to the U.S. signal brigade of over 1,100 soldiers. There was a sharp contrast between this “tooth-to-tail” ratio and the AT&T satellite phone system operated in U.S. base camps by roughly 24 company employees. Although the military communications system featured free morale calls, most U.S. soldiers phoned home with AT&T prepaid credit cards—expense outweighed by clarity and convenience. Their commanders often had similar feelings, in part because of the drain on already strapped combat manpower. “The former warring factions have better communications,” snapped one U.S. brigade commander, “because they have cellular phones and I don’t.”

The brigades and battalions in the U.S. sector—including the multinational units) were linked to the headquarters and each other by several baseline automation systems. The Maneuver Control System (MCS) is a vintage Army system that provided a secure means of transmitting orders, maps, diagrams, and classified e-mail. WARLORD, an intelligence terminal specially configured for this operation, handled most intelligence products, including imagery. However, a plethora of other automated logistical and administrative systems were also present, representing more a kludged-together operating environment than a “system of systems.” Such ad hoc arrangements made it correspondingly more difficult to maintain computers and electronic equipment or to defend them. Heat, cold,

humidity, and dust are traditional enemies of automation; but these challenges were magnified in Bosnia because there were so many computers, military supply lines were long, and there was little commercial infrastructure to take up the slack. A closely related and ominous development was the fast-growing problem of computer viruses. *While it is difficult to be precise, conventional wisdom among U.S. units was that 50 percent of their personal computers suffered from viruses of one kind or another.* Another problem was that large numbers of single-purpose, stand-alone databases made the integration of information incomparably more difficult, especially in the intelligence arena. Work-arounds were the order of the day, with heroic contributions coming from the most junior ranks, often augmented by technical virtuosos drawn from the Reserve components. The most common refrain: “Sir, this system was not designed for the job we’re doing here. So we messed around with it a little, and it’s not perfect, but we made it work.”

Support to the Warfighter

Despite the imperative of supporting the warfighter, the river of information available to U.S. military forces in Bosnia often diminished to a trickle by the time it reached the soldiers actually executing peacekeeping missions. In one operation, a brigade commander who had requested overhead imagery of his area complained that “the system” took 3 weeks to provide photographs that eventually turned out to be 6 months old. The reasons are many: communications pipelines too narrow for efficient digital data transmission to the lowest levels; outmoded tactical equipment; and automation resources easily overwhelmed by what data was available. But these were only some of the more pernicious effects of an unwritten but well-understood rule: the higher the headquarters, the more elaborate the information trappings and vice versa. Such priorities meant, for example, that the decision to deploy a state-of-the-art intelligence system known as Trojan Spirit with the U.S. brigades was delayed until shortly before those units left for Bosnia. Al-

though technology can provide a compelling way to enlarge the information highway to the lower echelons, such well-intended “fixes” must be balanced against the realities of Bosnia’s 24-hours-a-day operations. As one tactical intelligence officer said, “We just don’t have time over here for any more visits by the Good Idea Fairy.” The larger point is that advances in information technology are of military value only to the extent that they are accompanied by coherent doctrine, organizations, equipment, and people, to say nothing of the time needed to make them function as a team.

One of the bright spots in this picture, however, was the stunning success of Army tactical aviation in Bosnia. The helicopters of the 1st Armored Division’s Fourth Brigade combined speed and mobility in mountainous terrain—critical advantages in a region where every other factor conspired any external force. But innovations by Army aviation and intelligence soldiers also led to a new method of digitizing the Apache attack helicopter’s gun-camera footage—all for an investment of less than \$1,000 in commercial software and off-the-shelf equipment. The resulting photographs (see figure 10-5) documented Dayton Accord violations and—as unclassified imagery—were occasionally handed over to the former warring factions. Not only did these pictures display the exact time and location of such typical violations as tanks in the zone of separation, but they also featured targeting cross-hairs centered on the offending equipment—an unobvious but highly effective means of compelling compliance.

Conclusions

There can be no question that the military mission in Bosnia has been a success and that the American soldier, supported by his Air Force, Navy, and Marine counterparts, has been the primary reason why it has been so. But the Bosnian experience should also remind us that our worship of technology in warfare must be tempered by a stronger sense of the human factor. Information technology is uniquely affected by people, their training, their procedures,

Figure 10-5. Apache Gunship Camera Photo



and the time they take to perform them. But the combination of these factors in combat or operational settings is constantly and curiously underestimated. We have barely begun to address the organizational implications of modern information technology in synchronizing the political and military sides of a peacekeeping operation, in reducing top-heavy headquarters, and in substituting commercial products and services for outmoded military equipment and redundant support structures. These are daunting tasks; but until they result in unshakable leadership commitments, our hard-won progress in Bosnia will fall short of the “sensor-to-shooter” potential that Information Age operations will demand on other fields and in other years.

XI. C4ISR Systems and Services^{149,150,151}

Larry K. Wentz

The Challenge—Putting the Pieces Together

Effective C4ISR is a critical ingredient for the success of any military operation. Coalition operations such as *Joint Endeavor* present a complex set of challenges for the military C4ISR system planners, implementers, and operators. The most difficult challenge is the provision of integrated C4ISR services and capabilities to support the needs of ad hoc multinational military force structures and politically driven command arrangements. Although integrated C4ISR services are the desired objective, the realities tend to drive the solution to stove-piped implementations. In spite of technology advances, this will likely be the case for some time to come. There will continue to be uneven C4ISR capabilities among coalition members who will continue to rely on systems with which they are most comfortable—their own. For the IFOR operation, there were independent and separately managed NATO and national voice, message, data, and VTC networks; C4 systems and ISR systems; and so forth. This is simply the reality of coalition operations, with interoperability challenges and security disconnects that need to be dealt with. Agility and accommodation are truly keys to success in these types of operation.

In spite of formidable obstacles, NATO and its member nations were able to “put the pieces of the puzzle together” and installed and operated the largest military-civil communications and information system ever built to support a major peace operation—one of the success stories of *Operation Joint Endeavor*. The U.S. military CIS (communications and information systems) organizations (in particular, the U.S. Signal organizations such as 5th Signal Command) played a key leadership role in accomplishing the successful integration of the disparate NATO and national CIS systems. NATO, SHAPE, NACOSA, AFSOUTH, the IFOR CJ6, the ARRC, NC3A, and the United States, United Kingdom, and France all went through a very rapid learning curve, and many of the problems discussed herein were solved early into the IFOR operation by good will and good people working together for a common cause.

The U.S. Signal organizations also played a key leadership role in the establishment and staffing of the CJCCC (Combined Joint Communications Control Center) and the management of the IFOR CIS network. The United States provided 59 percent of the military communicators in theater at the peak of the operation. The prominent role of U.S. Signal officers in key positions in NATO, SHAPE, AFSOUTH, IFOR CJ6, EUCOM, DISA, USAREUR/5th Signal Command, USAFE, and other organizations was an important unifying factor. Many IFOR problems associated with system integration issues, ambiguous roles, incomplete doctrine, network and system management, and technical interoperability were successfully resolved through close coordination among these U.S. officers. The UK was also a key facilitator in this regard with important contributing players in NATO, SHAPE, NACOSA, AFSOUTH, the IFOR CJ6, the ARRC, and UK Signal units. The United Kingdom provided 32 percent of the military communicators in theater at the peak of the operation. NATO organizations such as AFSOUTH CISD (Communications and Information Systems Division), IFOR CJ6, SHAPE CISD, NACOSA, ARRC G6, and NC3A—the Hague rose to the occasion and provided untiring support to IFOR CIS installation, operation, and problem resolution activities as well.

Environmental Factors

In peace operations, it is necessary to be able to interface with the civil organizations such as the NGOs, PVOs, and IOs. In Bosnia there were more than 500 such personnel already operating in country when IFOR arrived and they relied on HF/VHF radios, regional Bosnia PTT telecommunications service where it existed, and to a large extent the UN VSAT voice network that supported UNPROFOR and other in-country UN elements. Some also had laptop computers, but none possessed the same level of communications and information system capabilities as the military.

The units deploying into BiH deployed into an area where the communication infrastructure had been destroyed and where the lack of cooperation among the former warring factions precluded the establishment of a BiH PTT-derived commercial communications capability to support or augment IFOR connectivity needs, especially cross-IEBL connectivity. In this regard, military owned and controlled primary connectivity was still a requirement for cross-IEBL and other essential C2 links.

The Bosnia population was literate and relatively well educated and was used to all forms of media that characterize an “information society.” The local and international radio, television, and print media were everywhere, operating independently of the military and reporting incidents almost instantaneously, sometimes before they were reported to IFOR. This created challenges for IFOR staff and placed added demands on the CIS network to be able to get the right information to the right place at the right time to meet not only the operational needs but to also accommodate the “CNN” effect (unsubstantiated media reports).

There were hazards and risks that had to be dealt with during *Operation Joint Endeavor*. The terrain and weather conditions were extreme. The commercial power was unreliable or in many cases did not exist. There was a lack of public water and space for housing C4ISR support personnel. Dust and dirt proved to be a challenge for the deployed commercially based, high-technology



PTT Damage

computer equipment that needed a relatively dust-free operational environment. Viruses also proved to be a problem for the computers and data networks, the main source being infected diskettes brought into the command centers by the staff. Minefields were numerous and added risk to all deployed C4ISR personnel. The force protection measures required soldiers to wear flack vests and helmets and travel in four-vehicle convoys, adding another challenge for those involved in the implementation, operation, and maintenance of the C4ISR systems.

There were other factors that influenced NATO and national activities in preparation for and execution of the IFOR deployment. The operation was occurring at a time when NATO and the nations were reducing force structures. Non-NATO and Partnership for Peace nations would be involved for the first time as well as the Russian Federation, and there was little guidance on how to proceed with these first-time events. In addition to the first out-of-area operation, it was also the first major ground operation ever. There were multiple OPLANs that added some confusion to the guidance for the CIS plans and management structure. NATO would be taking over from the UN and other peacekeeping agencies and this had some built-in uncertainties, including access to, integration of, and use of the already in-place CIS infrastructure of the UN, UK, and France. Deployment would take place in the depth of winter in an area of difficult terrain. The likelihood of hostilities was a major concern because of the fragility of the peace arrangements in Bosnia. There were effects on morale associated with deploying troops over the Christmas period. Therefore, one should not underestimate the degree of difficulty NATO and the nations faced as they prepared for and deployed to Bosnia in support of *Operation Joint Endeavor*.

Planning Considerations

CIS planning commenced more than 2 years prior to the Dayton Peace Accord being signed. Planning for OPLAN 40101 began in late summer of 1992 with the proposal of the Vance-Owens Peace Plan. The concept was to replace the UNPROFOR with

NATO forces. The ARRC was given the mission as the ground component commander and the responsibility to develop the scheme of maneuver. The plan matured and was re-designated as OPLAN 40103 in the fall of 1993, when it appeared that a larger replacement of UNPROFOR by a NATO force might be required.

In December 1994, members of USEUCOM staff met with AFSOUTH staff to discuss U.S. support for possibly assisting the UN in a withdrawal from Croatia and BiH. As a result of these discussions, preliminary planning for OPLAN 40104 began. By March of 1995, the political climate in Bosnia had deteriorated to the point that NATO planning for intervention resumed. OPLAN 40104 was developed for the sole purpose of withdrawing the UN from Bosnia and established the statement of requirements for the support of that operation. In September 1995, the political climate changed again; it appeared that peace was at hand in the region. As a result, in October 1995, NATO was directed by the North Atlantic Council to finalize plans for a peace-enforcement operation and AFSOUTH developed OPLAN 40105 to support this mission. NATO and national CIS organizations were thus left trying to hit a fast-moving political target and the changing operational plans did nothing to assist with the provision of “in time” CIS support. In fact, it made the situation more difficult.

Further complicating the planning was the fact that NATO had never attempted peace enforcement and it was its first ever out-of-area operation. Consequently, there was no doctrine, experience, or accepted practices to guide CIS planning and implementation—the NATO Combined Joint Task Force (CJTF) was just a concept and not doctrine. There were multiple NATO and national CIS organizations involved in the planning and implementation activities. The division of strategic, theater, and tactical CIS was less distinct for both NATO and national systems. AFSOUTH and SACEUR OPLANs reflected differing perspectives on CIS management and responsibilities. The Dayton Agreement assigned frequency management responsibilities to IFOR even though it had no established capability. These factors caused CIS organizational problems at the outset for IFOR CJ6. In order to address

the shortfalls, a Theater Frequency Management Cell (TFMC) was created and a Combined Joint Communications Control Center (CJCCC) was established to focus the theater-level planning and management of the CIS aspects of the IFOR operation. The CJCCC also facilitated coordination of NATO, national, strategic, theater, and tactical CIS activities.

The operational scenario for *Joint Endeavor* was unclear at the outset and national planning was being kept closely held. Hence, who was going where, when, and with what equipment were unclear to the NATO planners. Also, a lack of timely political planning guidance caused last-minute changes to bring the CIS plan in line with new policy decisions. For example, there was a requirement for COMIFOR to be in theater but AFSOUTH had no mobile headquarters capability. Thus it was necessary to look for a facility first in Zagreb and then at the last minute in Sarajevo. Neither in-country facility was configured as an operational headquarters from a CIS perspective, and because space was a premium in Sarajevo, it became necessary to locate part of the headquarters in the rear, initially in Zagreb. A comparable rear area capability was established in Naples at the same time as well. This added unanticipated last-minute requirements to the CIS plan. The ambiguities in C2 arrangements exacerbated the CIS planning problems.

Delayed political decisions prohibited forces from performing any real reconnaissance of the Bosnia area of operation, which prevented headquarters, communications, and command center site surveys prior to deployment. Some reconnaissance was possible in Croatia. Hungary was a different situation, where U.S. reconnaissance was possible to prepare for the deployment of U.S. support elements. NATO had never worked operationally with the non-NATO nations scheduled to participate and there was no doctrine on how their needs and CIS capabilities would be accommodated and integrated into the IFOR operational network.

In spite of the highly uncertain planning and operational environment and a lack of established CIS requirements, NATO, IFOR, and the nations still needed to plan for deployment. They had to anticipate potential requirements and provide a CIS capabil-

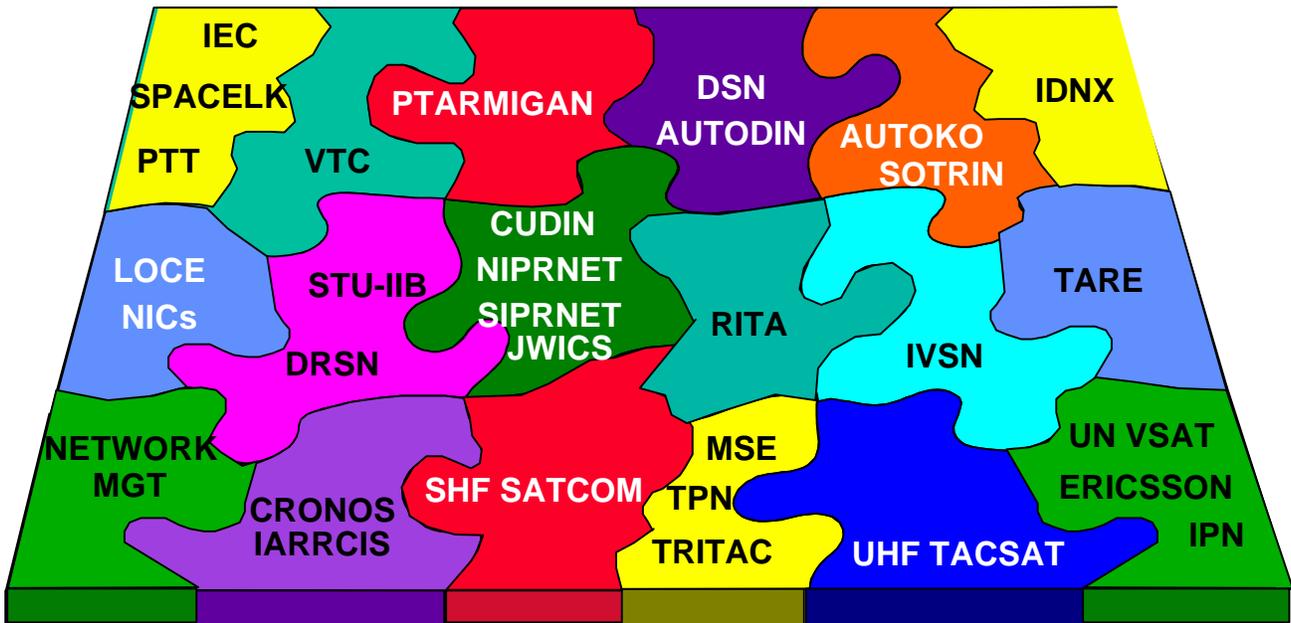
ity robust enough to accommodate unanticipated needs and surges should they occur. It was generally felt (at least by the United States) that it would be better to err on the side of providing too much CIS capability rather than not enough given the uncertainties of the operational environment. NATO was not fully supportive of an approach to “flood” with resources to overcome a problem.

Implementation and Operational Considerations

The NATO and IFOR framework member nation commands (i.e., NATO, SHAPE, AFSOUTH, ARRC, and the United States and United Kingdom, in particular) had to plan with a minimum of guidance and a lack of established requirements for the C4ISR capabilities to be deployed. The CIS contingency plans therefore had to be flexible enough to accommodate possible operational options ranging from assisting with the removal of the UNPROFOR, to peace enforcement, to peacekeeping, to war fighting. Furthermore, NATO lacked the CIS capability to deploy out of area. Limited military satellite bandwidth offered a major challenge as well. Two NATO satellites and one U.S. satellite were used but the bandwidth was still limited by space segment power and was inadequate to meet IFOR and national requirements. It was therefore necessary to rely on leased international vendor-provided commercial satellite services to fill the gap (e.g., IEC, SPACELINK, AT&T, and ITALIALINK).

The challenge facing NATO and the nations was to build a long haul and regional CIS network out of a mixture of military and commercial equipment that would vary widely in age, standards, and technology and would be built very quickly once given the order to deploy. Putting the pieces of the puzzle together (see figure 11-1) would most likely not result in a true “system of systems” for IFOR. Furthermore, there would be a need to interface systems that had not been planned or designed for interfacing. The independent national systems would be tied together, not engineered as a single system. Given the uncertainty of the situation it would most likely be a case of integrating what you get, not necessarily what

Figure 11-1. THE C4ISR Puzzle



you need, and then making the best of it. In addition, it would be necessary to support both mobile tactical command centers and fixed headquarters located in “buildings of opportunity,” such as the Annex to the Tito Residence (see picture) in downtown Sarajevo, hotels in Ilidza, the 1984 Olympic stadium and ice rink in Zetra, a factory in Banja Luka, office buildings at the airfields in Tuzla and Mostar, and Croatian military compounds in Zagreb and Split.

No single NATO or national organization was capable of providing the entire CIS infrastructure to support the operation. In addition, NATO took time to build up the organization and structure to plan, implement, operate, and manage the integrated strategic, theater, and tactical CIS capability required for such a large out-of-area coalition peace operation. NATO turned to the nations



IFOR Headquarters, Sarajevo

to assist in the form of experience, staff, and CIS capabilities and the United States, United Kingdom, and France played lead nation roles in this regard. The timely and effective response of these nations and 9 months of pre-planning by NACOSA allowed AFSOUTH to quickly react to the signing of the Dayton GFAP and rapidly deploy enough CIS capability to allow IFOR to take command and control of the operation.

The U.S. military strategic, theater, and tactical C4ISR systems and services provided critical communications and information systems and services in support of the IFOR operation, especially the tactical SHF SATCOM (the United States provided 76 percent of the tactical SHF terminals). The U.S. Tri-Service Tactical Communications (TRI-TAC) tactical systems formed the basis for the IFOR strategic- and theater-level network and TRI-TAC/MSE were used to support MND(N) and the national units assigned to it. The British tactical systems were the other major player in the IFOR operation. The PTARMIGAN tactical system supported the ARRC and its connectivity with the MNDs and supported MND(SW) and the national units assigned to it as well. The UK tactical SHF terminals were key contributors to the IFOR backbone connectivity (the VSC-501s provided 22 percent of the tactical SHF terminals). The French tactical systems supported MND(SE) and the national units assigned to it. The French tactical SHF terminals only supported national connectivity needs. NATO-acquired CIS and leased commercial services provided a key portion of the rest of the IFOR capabilities extended into Croatia and Bosnia. The NATO TSGT (Transportable Satellite Ground Terminal) provided military SHF SATCOM access to the IFOR headquarters in Sarajevo.

Deployment into urban facilities provided interesting challenges for the implementation teams since they were required to wire these facilities for voice and data services from scratch. This included installing LANs and telephone lines; removing tactical equipment from their shelters and installing them in fixed facilities; installing cables in buildings and on compounds; installing VSAT terminals; and performing numerous other non-tactical installation functions. The installation activities stretched the abilities of the

multinational teams deployed and required personnel with broad skills and training in order that they could be used for more than one task. The extensive use of commercial products (e.g., VSATs, IDNXs, routers, and ERICSSON telephone switches) meant that the military personnel needed additional training to engineer, install, and maintain this equipment as well. An IDNX course was set up at the NATO Latina, Italy, training facility to meet the IFOR need for installers and maintainers of this equipment. There were no “Tandy/Radio Shacks” in Bosnia so this put additional pressure on the support system for commercial equipment spares, repairs, and contractor assistance.

For any military operation, a certain amount of “learning on the job” is expected. However, the deployment into a generally urban environment (using office buildings for command centers), coupled with the extensive use of commercial products and services, created a need for more intensive on-the-job-training (OJT) than had been anticipated, both for the providers and users of the information services. OJT training programs were set up by the CIS providers not only to train their staff but also to teach command center staff how to use the information systems in the centers.

The proliferation of different information systems resulted in a situation where no one person was cross-trained to operate or maintain all of the systems in the command centers. Furthermore, the information system capabilities deployed were not being exploited due to the fact that the users lacked training and adequate understanding of the full potential of these systems. In many cases, information systems were simply used for word processing, e-mail, and PowerPoint briefings. SOCIFOR/JSOTF2 reported that the systems under their control could best be characterized as “too many, too duplicative.”

There was a significant lack of trained data systems and network administrators. They were constantly in high demand and there were simply not enough of them to adequately meet the needs of the information networks deployed. The military also lacked experienced, system-level maintenance and network management personnel in theater to troubleshoot the complex information net-

works deployed. Contractor support and the professional skills of those at the SHAPE Technical Center (now the NATO C3 Agency, the Hague) and national elements such as 5th Signal Command and DISA had to be brought to bear to help solve complex system-level problems.

Training needs were not limited to information systems alone; there were shortfalls in the military SATCOM area as well, e.g., the ARRC lacked trained NATO Airbase System (NABS) SATCOM terminal operators and maintainers and had to be supplemented by USAFE technicians.

U.S. PSYOP and CIMIC operations experienced problems in communicating between headquarters and the deployed tactical teams. The tactical teams had to rely on services provided to them by the units they supported. In many cases, the supporting units did not have spare capacity to offer them, and therefore had to share access to the voice and data services. Such shared access was frequently not high on the priority of the supporting units, limiting the ability of the PSYOP and CIMIC teams to communicate effectively. In some cases, the teams deployed with laptops but could not access the U.S. tactical packet network due to the lack of Tactical Terminal Adapter (TTA) interface devices. The shortage of TTAs was only one aspect of this problem, and not the most important. The use of TTAs was also limited by a shortage of voice channels over the U.S. MSE. Finally, there were also problems experienced in the timely distribution of PSYOP products to the deployed tactical PSYOP teams since there was no automated PSYOP-provided information system dissemination capability to specifically meet these needs. Vehicle transportation means were relied upon to bulk deliver products (e.g., *The Herald of Peace*, handbills, and posters) to the MNDs for local distribution. Some transcripts for radio and TV broadcasts were sent electronically to the deployed tactical PSYOP teams.

The shortage of TTAs proved to be a broader U.S. Army problem since Combat Support Systems such as STAMIS (Standard Army Management Information System) deployed without appropriate interface devices and there was a general shortage of

TTAs in theater to support the demand for access to information services. It was reported that Task Force Eagle was short more than 300 TTAs and an average request of 3 users per week were being experienced at D+65. TTAs were used on an exception basis in MND(N). The preferred connectivity was via the Network Encryption System (NES) into the Tactical Packet Network that provided a security solution and concentration. The U.S. Army STACCS system also experienced some deployment problems as a result of the deploying units not providing the necessary modems for tail circuits off the NES—equipment was left in garrison.

Although there were high expectations that the soldier on the ground would benefit more from advances in information technology, this was not necessarily the case for IFOR, despite efforts to equip them with the latest capabilities. From a coalition operation point of view, however, significant progress was made in moving the “information revolution” to lower levels of the command hierarchy. In most instances, the IFOR CIS network provided better service and more capability than that available at NATO and the major NATO Command headquarters and at many of the IFOR troop contributing nations’ home stations.

Unanticipated Requirements

The communications and information needs of operations such as the IFOR Public Information Office, IFOR Information Campaign, Engineers, PSYOP, CIMIC, Counterintelligence, and HUMINT were not completely formulated or necessarily fully understood at the outset of the operation. The need to be able to interface with and provide some limited support to the NGO/PVO/IO community was also underestimated. Therefore, the requirements were not adequately articulated to the IFOR and national CIS planners and providers so that the necessary service could be made available at the outset of the operation to support these activities. As an example, the IFOR CJCIMIC headquarters operation in the Burger building in downtown Sarajevo only had a few local telephone lines to conduct business in the early stages of operation. If they needed

information services or a broader IFOR communications capability, they had to go to IFOR headquarters at the Tito Residency. The CIMIC and some HUMINT vehicles lacked radios for communicating while operating in the countryside. The engineers also generated a requirement for force protection communications since they too were frequently scattered throughout the country. The PIO needed more effective IFOR communications and information services at the Holiday Inn in Sarajevo and while traveling around the countryside in order to be able to quickly inform the chain of command of media-related, time-sensitive events and issues.

The IFOR engineers and legal and medical personnel needed to use the Internet to access reference material. The PIO also needed Internet access for media interaction. The Internet could be used to get English translations of Croatian and other international press releases and news articles. NATO policy at the outset of the operation did not support the use of commercial Internet services. NATO policy makers were often slow in accepting reality and the need for pragmatic change. The use of the Internet in NATO was an example of such a phenomenon. In contrast, Internet access was available to U.S. elements at almost all locations, even remote base camps in MND(N).

A significant change to the earlier OPLANs was abandoning the concept of a combined logistic support arrangement and making logistic support a national responsibility. This resulted in the establishment of three NSEs: the United States in Hungary, the British in Split, Croatia, and the French in Ploce, Croatia. The ARRC COSCOM commander was designated COMMZ Forward commander and located in Split, Croatia. He was given the responsibility of reporting movement into theater to the IFOR Commander for Support who was located in Zagreb, Croatia. This meant that providing communications between COMMZ Forward and the NSEs was a theater responsibility. For the United States it also added the requirement to support a U.S. NSE in Hungary.

Early Interoperability Considerations

Interoperability became a major concern when the total scope of the engineering effort for the IFOR network was realized. No one nation had committed to the integrated network engineering task that included terrestrial and satellite transmission systems; commercial PTT networks; and diverse systems of voice, video, and data of NATO and national strategic, theater, and tactical systems. It was decided to conduct a major interoperability exercise, called *INTEROP 95*, to get a better insight into the system integration and interface issues and solutions. *INTEROP 95*, held in April 1995, included more than 250 participants from 8 nations and tested all anticipated interfaces necessary to execute the AFSOUTH and ARRC OPLANs. System interfaces tested included the UN Ericsson commercial switch, the Olivetti commercial switch, the Italian tactical system SOTRIN, the U.S. tactical systems TRI-TAC/MSE, the UK tactical system PTARMIGAN, the U.S. strategic system DSN, and the NATO voice network IVSN. The N.E.T. commercial IDNX, the SHAPE TSGT and deployable reach-back communications capability REPLICA, the USAF TSSR (TROPO/Satellite Support Radio) LOS radio, and NATO and national tactical satellite terminals (U.S. TSCs, UK VSC-501 and NATO Air Base SATCOM (NABS) (USAFE deployed)) were tested as well. The results of *INTEROP 95* were so overwhelming that the U.S. Joint Interoperability Test Command (JITC) certified a number of the interfaces and published a NATO Interface Guide as a reference book. Lessons learned have shown that despite “standard NATO interfaces,” interoperability trials still have to take place to reduce interface problems.

Exercises such as *INTEROP 95* and subsequently, *Mountain Shield I* and *II*, served to refine concepts of operation and work out many system integration and interoperability issues among various commercial and NATO strategic and national tactical switching and transmission systems. Among the 5th Signal Command learning experiences were difficulties in acquiring the NATO IVB satellite and poor-quality NATO satellite links (plagued with system hits). Subsequent U.S./NATO satellite testing revealed that

BPSK rather than QPSK transmission needed to be used on the NATO IVB to achieve the desired link performance. Unfortunately, BPSK requires more bandwidth so the satellite planners had to reengineer the planned satellite network that was already bandwidth constrained. This problem may also have been a training-related issue as well, in that the U.S. personnel may not have been adequately prepared for accessing the NATO satellite system. Pre-deployment exercises serve to help resolve problems such as these. They also provide excellent training for the participating coalition organizations that end up supporting the actual operation.

Based on field tests and exercises involving U.S., NATO, and allied communications systems, EUCCOM J6 developed a EUCCOM U.S./NATO/Allied Communications Systems Automated Interoperability Handbook. The handbook is on a laptop computer and is used to document known interoperable configurations that work. It provides a wiring diagram of the configuration, technical details, and other relevant information necessary to guide interface implementation in the field. An operator simply enters the configuration to be set up and if it has been accomplished before and documented, the computer provides the details necessary to implement, test, and operate the requested interface arrangement.

Evolution of the CIS Capabilities

One distinct advantage enjoyed by AFSOUTH was the time allowed in the lead up to the IFOR operation. During the planning of OPLANs 40103 and 40104 there was time to do some limited site surveys in Croatia and Bosnia and to coordinate CIS planning with NATO, SHAPE, and likely key participating nations such as the United States, United Kingdom, and France. It should be noted, however, that although there was a lot of time to plan the NATO CIS network to support the withdrawal of UN forces, there was little time to develop the theater contingency option to support the last-minute change to deploy into Bosnia for the IFOR peace-enforcement mission.

Fortunately, NATO had already taken action to extend its strategic CIS network into Croatia in anticipation of having to support the extraction of UN forces. The UN also had a fairly extensive network in place in Croatia and Bosnia to support UNPROFOR C2 needs. In addition, at the TOA (transfer of authority) from UNPROFOR to IFOR, there was also a considerable advantage in that the United Kingdom and France, two of the framework nations, were already in place as part of UNPROFOR. The fact that they were already in theater meant that they also had their CIS infrastructure operating in theater, including links back to their national support elements. These networks therefore became major players in facilitating the extension of NATO and national CIS capabilities to support the initial IFOR C2 needs in Bosnia.

The United States, on the other hand, was at a disadvantage in that it was required to essentially deploy its CIS capabilities from scratch when IFOR was activated. The establishment of the Headquarters IFOR, the C-SUPPORT Headquarters, and the ARRC CIS capabilities also experienced similar challenges at the outset of the operation.

The IFOR network implemented in Bosnia was basically a tactical military network which relied heavily on the tactical assets of the United States and the United Kingdom. Over time, the military network was augmented with commercial products and services. The IFOR plan was to phase out the military assets as soon as possible and rely more extensively on commercial services with a military overlay to support essential C2 needs. The commercial capabilities implemented were viewed as leave behind when IFOR withdrew and were therefore an integral part of the CIS exit strategy. When the decision was made in late 1996 to extend the NATO presence in Bosnia, the commercialization of the NATO CIS network in Bosnia and Croatia continued as a big element of the CIS strategy and the establishment of the so-called IFOR Peace Network.

TOA from AFSOUTH/IFOR to LANDCENT/IFOR occurred on 7 November 1996. The ARRC TOA to LANDCENT/IFOR occurred on 20 November 1996 and the TOA from IFOR to SFOR occurred on 20 December 1996. These TOAs were accompanied by a large personnel change and changes in the NATO and national CIS infrastructure. For the strategic and theater CIS connectivity, a rationalization and re-balancing of the networks was necessary to reflect the move of the IFOR operational center to Sarajevo and then to Ilidza where SFOR headquarters was established. Accompanying the reconfigurations were a greatly reduced role of AFSOUTH and downsizing of the CIS support to them.

LANDCENT had been planning for the transition for several months with “right seat” hand-over training initiated in late September 1996. In spite of an attempt to get up on the learning curve, LANDCENT still experienced many of the CIS implementation and procurement challenges seen in IFOR’s initial deployment.

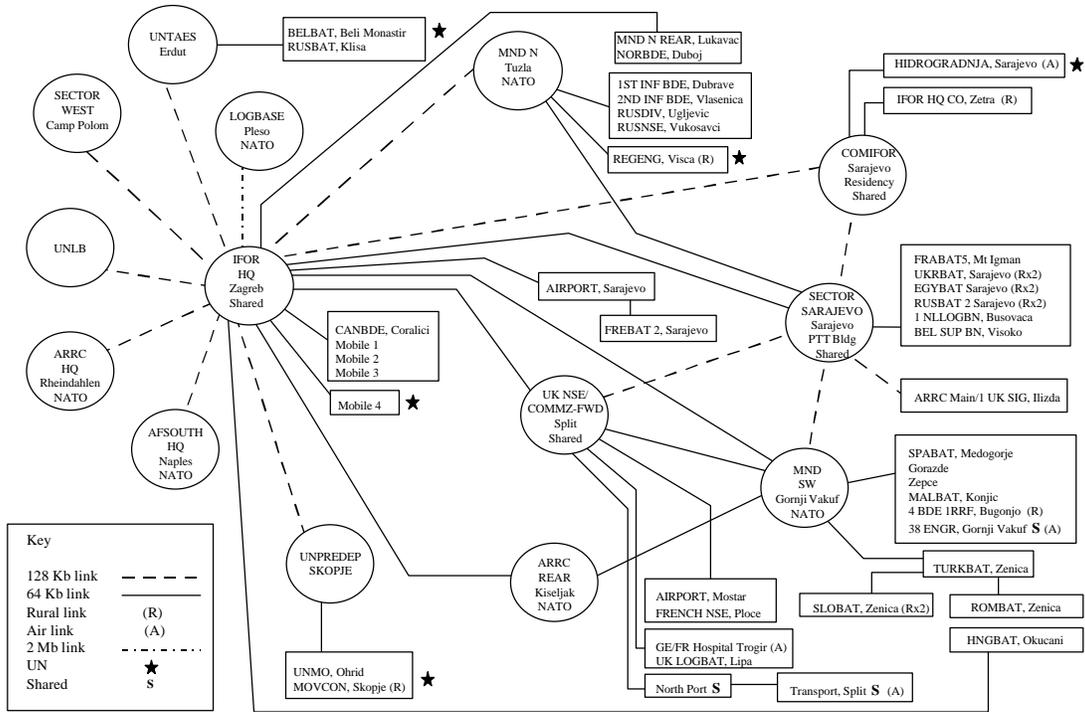
For the United States, there were also some unintended CIS reconfigurations as well. For example, due to the fact that Commander LANDCENT/SFOR was also Commander USAREUR, U.S. national CIS support systems had to be added to meet his U.S.-only requirements. The force structure downsizing associated with the IFOR TOA to SFOR also resulted in a major reconfiguration of the U.S. tactical satellite and switched networks supporting the NATO operation.

The UN Network

Prior to the IFOR operation, UNPROFOR had been operating in theater with a CIS network which consisted of VSAT, voice, secure and nonsecure fax, HF/VHF/UHF radios, and a system for convoy tracking and communications called LOGTRACKS. These assets were in place and some were available to support the IFOR deployment.

The UN VSAT network, depicted in figure 11-2, was already in place and provided voice connectivity to key locations to which IFOR deployed. It played a critical support role in not only

Figure 11-2. UN VSAT Network



the deployment phase but also throughout the operation. The network consisted of ERICSSON switches interconnected by a commercial VSAT network. There were four standard access packages available: CORPS level—8 trunk lines and 80 extensions; division level—8 trunk lines and 30 extensions; brigade/battalion level—4 trunk lines and 10 extensions; and local access to 2 lines from local VSAT facilities. NATO leased the service from the UN.

The UN VHF radio network (Motorola) consisted of 40-watt base stations, 25-watt vehicle mounted sets, and 5-watt handheld sets. There were repeater stations throughout Croatia and BiH. ARRC-Main established a VHF “network of networks” to monitor election supervisor activity for the September 1996 national elections. The MND brigade operations centers performed the monitoring. The network was a combination of IPTF and UN assets with NATO-funded ARRC-Main assets used to fill in the gaps.

The NATO Network

In preparation for the execution of OPLAN 40104, the extraction of UN forces, a data network based on leased E1 (2mb/s) transmission bearers and using NATO-purchased IDNX smart multiplexers was extended by NACOSA and the United States into Croatia. The seven-node network connecting SHAPE, AFSOUTH, Vicenza, Brindisi, Zagreb, Pleso, and Split was approved and funded by NATO on 8 February 1995. Installation (with some assistance from DISA) began in March and was completed on 13 April 1995. In April 1995, the NAC approved the first-ever NATO out-of-area operation and authorized the deployment of up to 80 military personnel to install, operate, and maintain the E1/IDNX-based information network. The operation was dubbed “Mini-STEP 2” of a three-step process to extend NATO strategic communications and information services into the theater. On 26 April 1995, the first soldiers of the Southern Region Signal Regiment, AFSOUTH, began to deploy to Zagreb, Croatia. In addition to installing the interfaces to the E1/IDNX network, an operational WAN was established

between the sites and LANs at Zagreb, Pleso, and Split. The plan also included pre-wiring and interconnecting designated buildings to be used by IFOR staff to permit rapid occupancy if the need arose. By the end of May 1995, the E1/IDNX-based strategic backbone information network was fully operational.

The NATO Transportable Satellite Ground Terminal (TSGT) was deployed to Camp Pleso (a UN compound collocated with the Zagreb international airport) and was used to provide a military path for the E1/IDNX network in the event of political instability in Croatia. The TSGT also supported the extension of SHAPE headquarters voice, message, and data services to the Zagreb area through the use of the SHAPE-provided REPLICIA system. The REPLICIA system was based on a prototype developed by the SHAPE Technical Center (now the NATO C3 Agency) and provided a reach-back service to SHAPE headquarters.

IFOR and Framework Nations Networks

With the signing of the Dayton Peace Agreement on 14 December 1995, the mission changed and Croatia and Hungary became the embarkation points for NATO troops deploying into the region. OPLANs 40105 and 10405 provided the guidance for the deployment of these forces and the supporting CIS infrastructure. However, because of C2 differences, the OPLANs were never harmonized and this led to disruption and discord between AFSOUTH and SHAPE staffs.

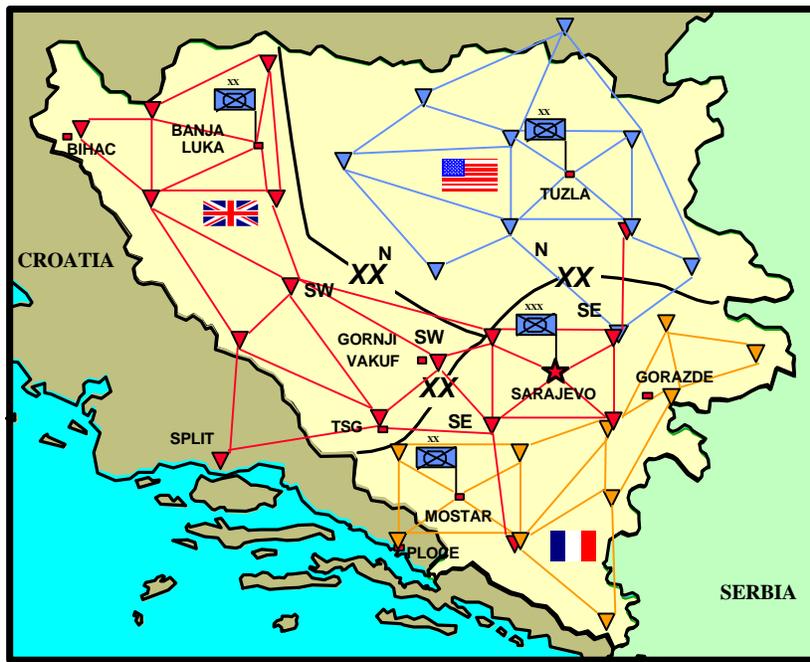
The CJCCC started to deploy elements of its organization to Zagreb in early December 1995 along with the main staff elements of the IFOR C-Support. By 17 December 1995, HQ IFOR JOC operations were being conducted out of Zagreb with a HQ IFOR (FWD) JOC at the Residency in Sarajevo. On 18 December 1995, the NATO TSGT and REPLICIA were moved from Camp Pleso (Zagreb) to Sarajevo. The TOA from UNPROFOR to IFOR took place on 20 December 1995. At this time the Residency in Sarajevo had the following systems operational: UN VSAT, TRI-

TAC, REPLICA, DSN, PTARMIGAN, Defense Red Switch Network, WAN, Video Teleconferencing (VTC) (connecting the Residency, AFSOUTH, and Zagreb), TARE, Recognized Air Picture from the CAOC, and LOCE INTEL access. The ARRC too was up and operational at this time with connectivity to its MNDs, the NSEs (National Support Elements), and IFOR Headquarters.

The IFOR CIS network (figure 11-3) was based on a strategy to use national military tactical systems to extend the NATO strategic CIS network into the area of operation. When a period of stability was achieved, the plan was to replace the tactical systems with commercial capabilities. It had to be kept in mind that the IFOR mission was to be completed within a year. Therefore, the IFOR CIS infrastructure would need to be replaced, in any case, by commercial capabilities as part of the mission completion.

In addition to supporting the IFOR CIS network, the framework nations (the United States, United Kingdom, and France) also provided capabilities that would support their own forces committed to *Operation Joint Endeavor* (figure 11-4). These capabilities included strategic to tactical C2 and mission support networks, as well as national intelligence capabilities and supporting ISR networks that would provide intelligence support to the national commanders and provide IFOR-releasable intelligence to IFOR and the ARRC through the NICs (National Intelligence Cells). Tactical systems indigenous to the units deployed, such as the U.S. MSE, single channel TACSAT, and Combat Net Radio, were employed at division and below. The United Kingdom deployed SCRA, VHF, UHF, VSAT, leased PTT, and INMARSAT capabilities to support division to battalion voice and data services, including access to MENTOR, their strategic-level network (DSN equivalent). The French deployed a number of different capabilities to support division to battalion voice, telegraph, and data services: the SPARTACUS TACSAT, the SICILE/TANIT network that supported HF/VHF/UHF/PTT/INMARSAT and PTARMIGAN interfaces and services, and the SYRACUSE SHF SATCOM. The RTY network also provided telegraph services down to the battalion level. Ac-

Figure 11-4. Framework Nations Network



cess to the French strategic-level system RITTER (DSN equivalent) was provided as well. The French tactical system RITA was not deployed until the March 1996 time frame.

The IFOR implementation strategy would undergo some change, however, with the fall 1996 decision to extend the NATO involvement for an additional 18 months and transition IFOR to LANDCENT/SFOR. Commercialization of the military network through the establishment of a commercial services-based, end-state network, the IFOR Private (Peace) Network (IPN), continued to be the strategy followed by IFOR and subsequently LANDCENT/SFOR. The replacement of IFOR with SFOR and the movement of SFOR headquarters from the Residency in Sarajevo to Ilidza (outside of Sarajevo) extended the reliance on military tactical systems beyond the time frame anticipated and also required the acquisition of additional NATO CIS capabilities to accommodate this change. Furthermore, the United States had to provide additional national communications to support a four-star general, who while serving as the LANDCENT/SFOR commander in Sarajevo also retained command of USAREUR.

IFOR C4I Systems and Service

Since NATO had no in-place ability to deploy forward its strategic C4I capabilities, IFOR had to rely heavily on the national tactical assets of the framework nations, the UN VSAT networks, and commercial products and services to extend connectivity into Bosnia and to provide information services to the deployed headquarters and forces. The pervasive use of commercial-of-the-shelf information products and services propelled NATO and IFOR into the Information Age.

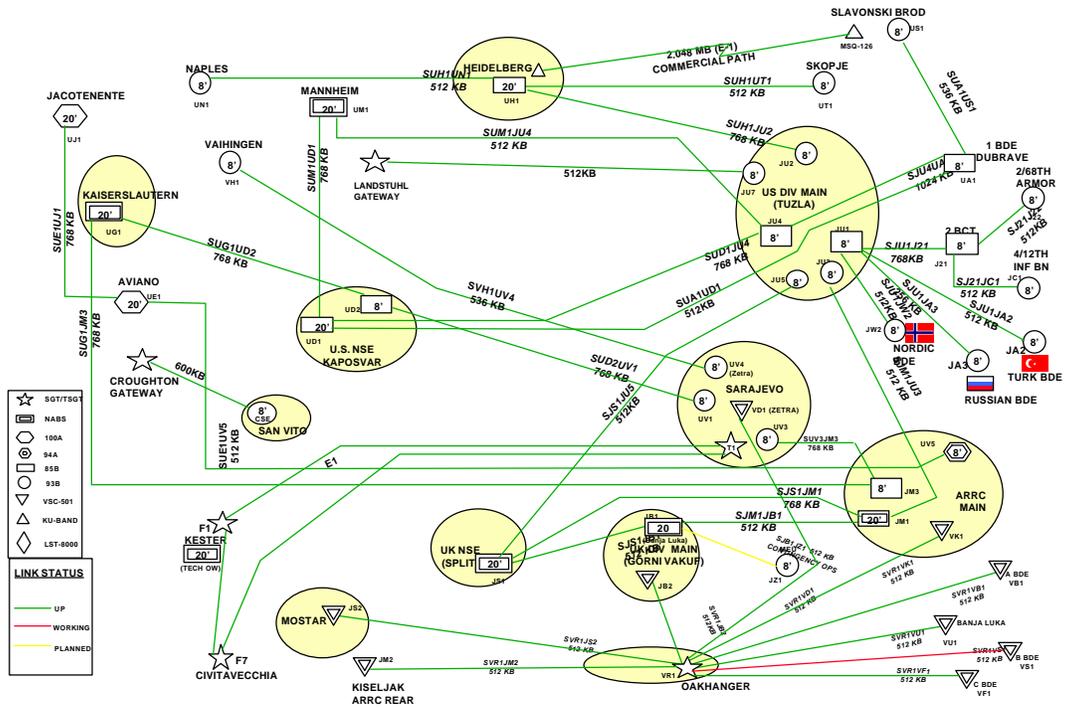
Military and Commercial SATCOM

Due to the lack of Bosnia telecommunications infrastructure (and in particular, cross-IEBL connectivity), mountainous terrain, and the high cost of force protection for radio relay sites, national military SHF SATCOM was used extensively. It was used not only to provide the transmission bearers for the initial deployment but also to support connectivity throughout the IFOR operation (figure 11-5) as well. NATO only had one TSGT and it was deployed to Sarajevo to support IFOR Headquarters reach-back connectivity to SHAPE. Because NACOSA had SHF SATCOM expertise and NATO had SHF space segment capacity, it was possible for NACOSA to design and the CJCCC to implement a large and complex SATCOM network using the NATO and U.S. DSCS satellites and national tactical SATCOM terminal assets. The United States and United Kingdom provided the bulk of the military tactical SHF SATCOM terminals (U.S.: 35 TSCs and 5 NABS, UK: 9 VSC-501s) supporting IFOR, ARRC, C-SPT, the NSEs, and the MNDs. In order to achieve the desired bandwidth on key links, it was necessary for the U.S. Regional Space Support Center (RSSC) to engineer the U.S. loading of the satellite based on the use of 20-foot dishes (these dishes were in short supply).

The French provided military SATCOM (the SYRACUSE, TANIT, and SPARTACUS tactical satellite terminals) connectivity but only for the MND(SE) area of operation and connectivity to France. The SYRACUSE network used the French TELECOM II A and B satellites.

By late summer 1996, although the original NATO TSGT (designated T1) was still operating well in Sarajevo, there was increasing concern about the ability to keep the terminal operational (overdue for an upgrade) and spares to support it. Therefore, it was decided to deploy several of the newly acquired NATO TSGTs to Sarajevo to replace the old equipment. The first TSGT was deployed in September 1996 to replace the aging T1. Three more terminals were deployed over the next 3 months. Adding the new

Figure 11-5. SHF Architecture

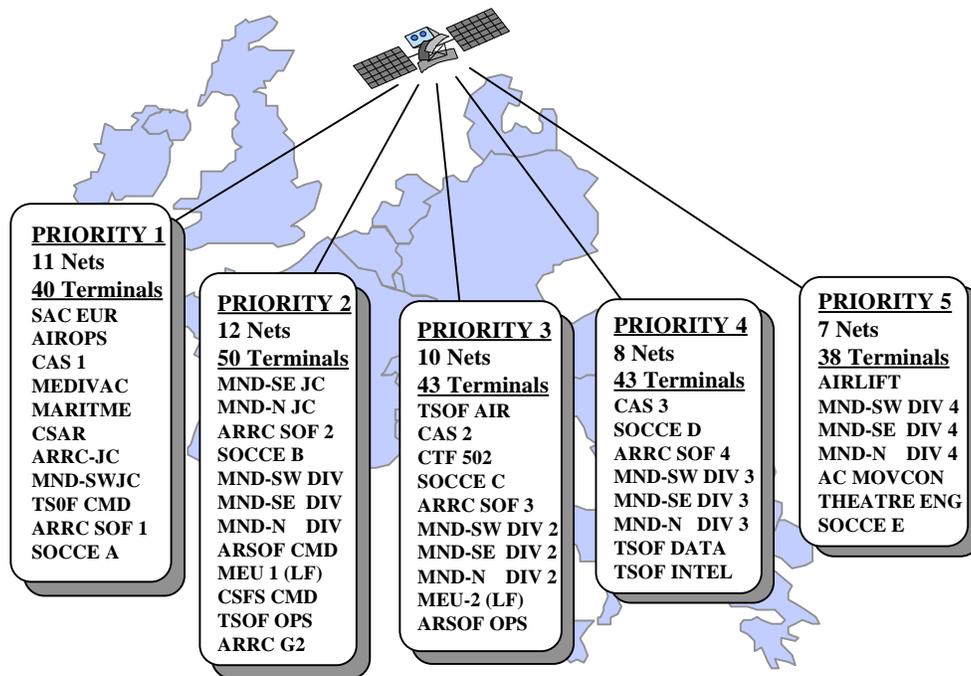


terminals also increased capacity and provided more robust NATO SATCOM connectivity in the area in anticipation of the transfer of authority to LANDCENT/SFOR.

The USAF terrestrial TROPO/SATELLITE Support Radio (TSSR) provided a 2mb/s line of sight (LOS) capability that was quite flexible and easy to set up. The TSSR was used to establish local connectivity where it was not possible to acquire PTT service. For example, it was used from the roof of the Tito Residency annex to Zetra stadium to link IFOR headquarters with the NATO satellite ground terminal and by the ARRC in Ilidza to connect to the UN VSAT network in Sarajevo.

Single-channel UHF SATCOM allowed commanders to overcome terrain and distance restrictions for broadcast radio networks. In particular, at the tactical level this capability allowed formations and units to operate voice nets over wide areas without deploying VHF FM rebroadcast stations. The distance, terrain, and ground security environment that the forces needed to operate over often did not allow the deployment of rebroadcast stations. TACSAT had the efficiencies of a broadcast network, allowing stations in the net to hear and respond simultaneously. The terminals were small and easily portable and allowed maneuver commanders to quickly establish communications. UHF SATCOM was a major player throughout the theater with 37 networks active out of a planned 48 (see figure 11-6). Establishing UHF access and allocation procedures was a first for NATO. Problems were worked out jointly between AFSOUTH, NACOSA, and USEUCOM. NATO leased 32 UHF channels from the U.S. satellite network (at a very high price from the NATO point of view). NATO also initiated action to procure 212 UHF TACSAT terminals (half LST-5E [wide and narrow band capable] and half PRC-117D [narrow band capable only with a separate crypto add-on]). The CJCCC established the initial set of UHF access and allocation procedures and closely managed the emerging network. The number of UHF channels available on the satellite limited the capability over a particular region. Addi-

Figure 11-6. UHF SATCOM



tionally, there were some long lead time items in re-supply and repair because the UHF terminals were low-density items. This had some operational impact implications.

As the operation evolved, commercial VSAT services were extended into the area through contract services provided by IEC, SPACELINK, and HARRIS TELEDATA. IDNX smart multiservice bandwidth managers were interconnected by the military and commercial bearers and used to provide a robust transmission infrastructure that provided connectivity for the voice, data, and VTC networks. In fact, the combined IFOR and U.S. IDNX network was the largest military IDNX-based network ever implemented. The E1/SATCOM/IDNX network proved to be a flexible and capable system for *Operation Joint Endeavor*. Figure 11-7 shows the status of the NATO IDNX network at the end of *Operation Joint Endeavor*. The network supported communications services for 18 different geographically dispersed locations. A leased 2mb/s commercial SATCOM link, ITALIALINK, connected IFOR headquarters in Sarajevo with AFSOUTH headquarters, Naples. Commercial INMARSAT terminals were also used by IFOR, the ARRC, the MNDs, C-SPT, the NSEs, and national command elements.

Military Voice and Commercial Services

National tactical voice equipment was used to establish the IFOR Voice Network (figure 11-8). The U.S. TRI-TAC system provided a large portion of the strategic- and theater-level telecommunications infrastructure supporting organizations such as SHAPE, AFSOUTH, IFOR, C-SUPPORT, COMMZ, and the NSEs. NATO also provided some. The UK tactical system, PTARMIGAN, provided the telecommunications support for the ARRC (CORPS level) and between the ARRC and the MND headquarters. The United States, United Kingdom, and France used their tactical systems to support division-level communications including service to those forces assigned to their divisions. TRI-TAC/MSE equipment was employed in support to MND(N) and the U.S. NSE in Hungary. PTARMIGAN was used to support MND(SW) and the UK NSE in

Figure 11-7. IDNX/IEC/SPACELINK/ITALIALINK Network

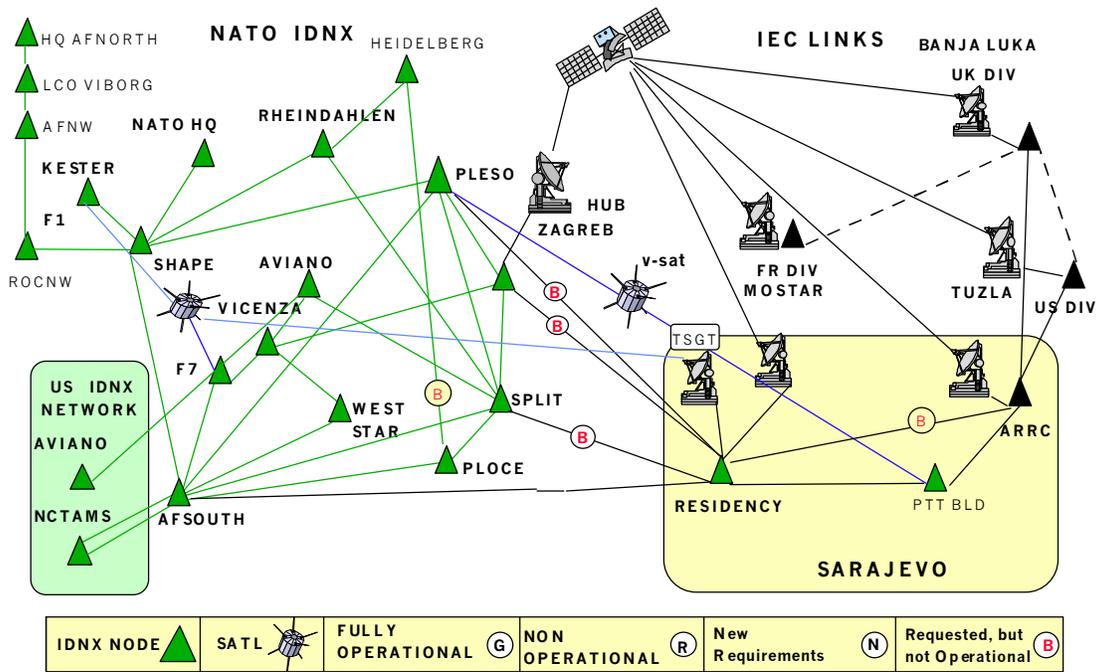
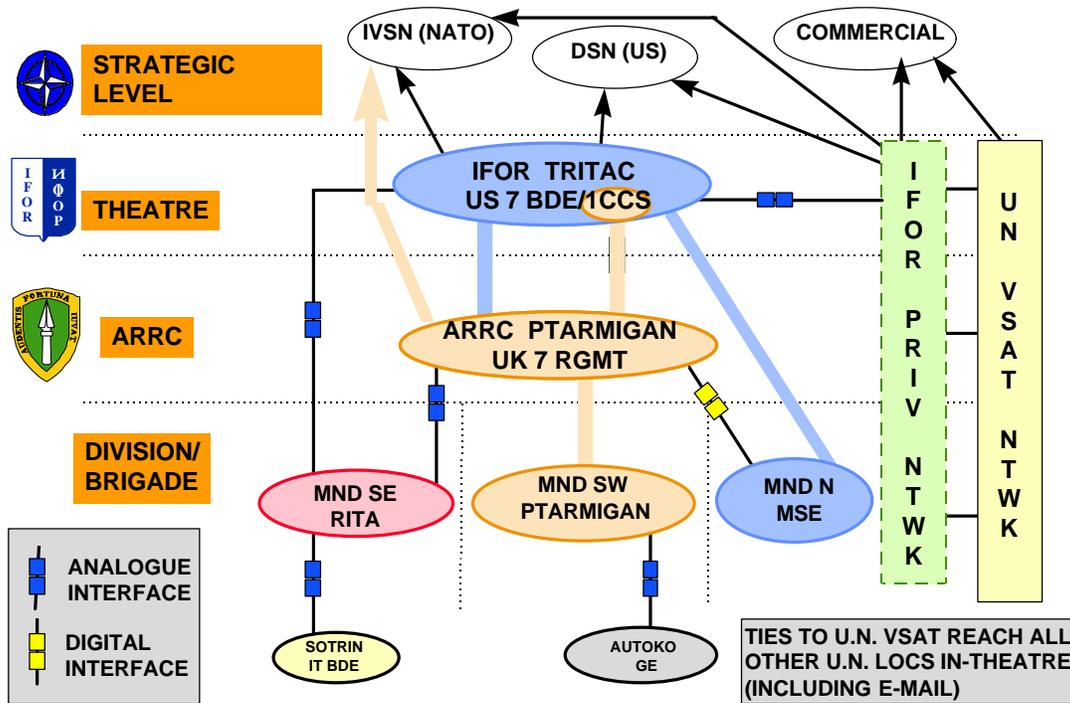


Figure 11-8. IFOR Voice Network



Split. French tactical systems already in place were used to initially support MND(SE). The tactical system RITA was deployed in the March 1996 time frame to provide additional support to MND(SE) and its NSE in Ploce. The Italian system, SOTRIN, supported the Italian brigade in MND(SE) and the German tactical system, AUTOKO, supported the German contingent in MND(SW). STANAG 5040 was employed to provide an analogue interface between the national, tactical, and strategic voice networks; between TRI-TAC and the NATO strategic voice network, IVSN; and between TRI-TAC and the commercial networks such as the UN VSAT and the Bosnia and Croatian PTTs where available. The Interim Digital Interface PTARMIGAN (IDIP), designed by the United Kingdom for this operation, was used to provide a digital interface between PTARMIGAN and the TRI-TAC/MSE systems. STANAG 5040 was used for the TRI-TAC to RITA interface as well as SOTRIN and AUTOKO interfaces with RITA and PTARMIGAN, respectively.

The OHR (Office of the High Representative) had a terrestrial UHF Motorola network that was installed to link major Bosnian cities. IFOR headquarters obtained a channel on this network to provide force protection communications for CIMIC and IFOR Information Campaign personnel in the field.

The Republika Srpska (RS) and the Federation telecommunications infrastructure were severely damaged as a result of the war. Some damage was also caused by the allied bombing campaign. Before the war, there were about 4,000 international lines but in December 1995 there were only 400. There were some 30,000 Federation and 27,000 RS trunks before the war but in December 1995 there were 8,000 and 4,000 respectively. As a result, only limited local and regional services were generally available. The international call completions went from a pre-war percentage of 35 percent to 2 percent in December 1995. There was no operational cross-IEBL connectivity even though physically some connectivity existed. For example, RS and Federation trunk switches were interconnected but software code blocks prevented dialing between the two networks. Commercial cellular communication was

available in some areas of Croatia and towards the end of the IFOR operation, a limited coverage commercial cellular capability was implemented in the Sarajevo area.

AT&T and British Telecom provided a soldier Call Home commercial service as part of the military MWR (morale, welfare, and recreation) support initiatives. MCI also showed an interest in providing service, but due to the contract arrangement with AT&T this did not happen. AT&T implemented roughly a 20-node commercial satellite-based network to support the MWR service and to support other U.S. military needs in Bosnia, Croatia, and Hungary. The AT&T implementation at the outset was slower than the U.S. military would have liked it to be and DSN was used to provide limited support for MWR needs. In the case of AT&T there was a Military Saver Program under a contract with AFFEES that soldiers could join in order to get reduced rates. During the 1995 Christmas holiday period there was a promotion sponsored by AFFES, VFW, and AT&T that provided every U.S. soldier a free \$20 calling card donated by these organizations.

There were various morale-call policies in place for NATO and national military personnel. The United States allowed deployed military to use the DSN for this purpose. There was, however, an IFOR-related unintended consequence associated with this practice. For U.S. personnel assigned to IFOR organizational elements, the only access to the DSN (at least in the Sarajevo area) was through the UN VSAT network. There was no NATO policy that prevented the use of the UN VSAT network for this purpose. As a result, the UN VSAT network, which was already overloaded with operational traffic, experienced additional loading from morale calls that interfered with the operational use of the network. The French used RITA to call back to France. The British forbade morale calls over their military networks. It was reported that staffs of all nationalities used the IFOR commercial access at the Residency in Sarajevo to make direct-dial international calls home. This too had IFOR-related unintended consequences. The calls interfered with bona fide mission traffic (since the commercial access could be used when UN VSAT and other networks were having problems or loaded with

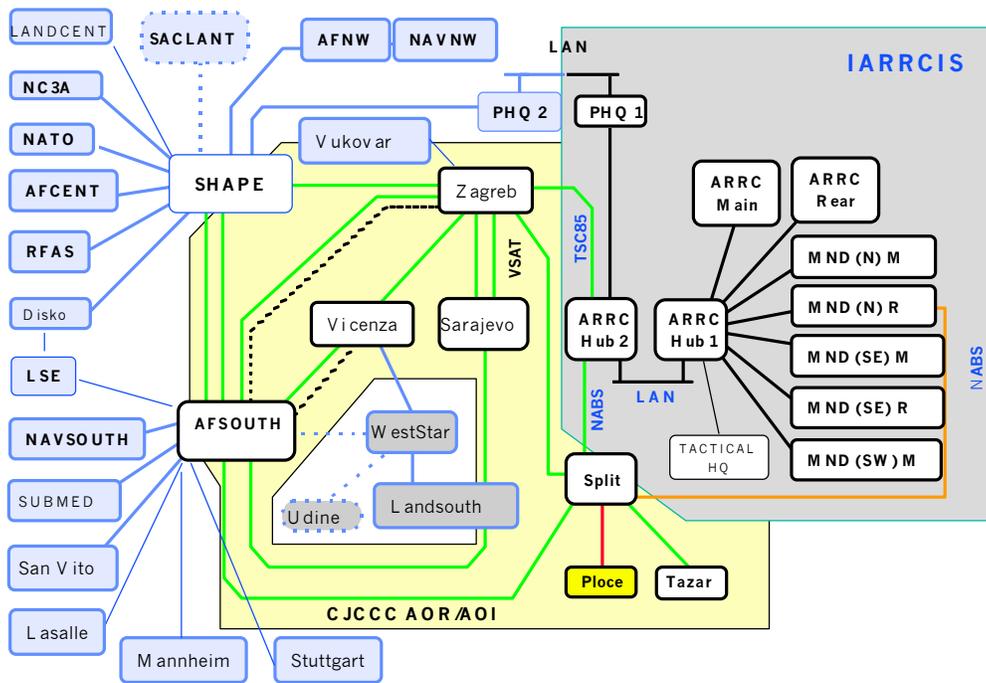
operational traffic). In addition, this service was expensive. NATO, which leased the service and ran the switch at the Residency, did not enforce a policy on use of this service and usage accounting was not performed on the switch in Sarajevo to check for abuse of the service.

IFOR Data and Messaging Services

IFOR data network service was provided by extending the AFSOUTH information system prototype designed by the SHAPE Technical Center (now the NATO C3 Agency, the Hague). The prototyping activities were carried out under project ECHO (Evolutionary Capability for Headquarters Operation). At the end of 1993, ECHO was a four-node commercial client-server-based architecture interconnected by a X.25-based Wide Area Network. The interconnecting links operated at 2.5kb/s. By February 1994 the network was expanded and migrated from X.25 to TCP/IP with enhanced security features (authorized to operate NATO SECRET system high). In May 1995, the functionality was further expanded and the network was declared operational and re-named CRONOS. The interconnecting links were upgraded and varied in bandwidth between 9.6kb/s and 64kb/s. The network supported Microsoft Office and e-mail services along with some functionally specific C2 applications such as the PAIS, CRESP, Allied Deployment and Movement System (ADAMS), and the RAP from the CAOC. The CRONOS network was extended to support NATO and IFOR strategic- and theater-level needs. The CRONOS LAN at IFOR headquarters had to be upgraded to switched Ethernet technology due to the volume of traffic received and generated by the Joint Operations Center.

UK CIS support to the ARRC included a tactical information system, the Interim ARRC Information System (IARRCIS). IARRCIS was a ruggedized equivalent of CRONOS and was used to support the ARRC and the data services between the ARRC and the MND headquarters. The CRONOS and IARRCIS networks (figure 11-9) were interfaced to provide seamless data and e-mail service between the NATO and IFOR strategic, theater, and tactical

Figure 11-9. CRONOS/IARRCIS Network

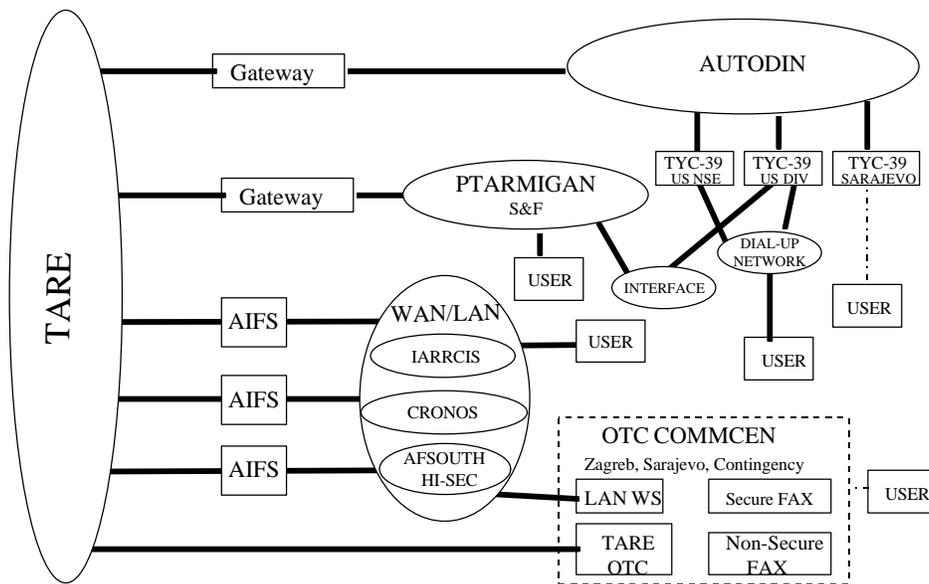


headquarters and support organizations. There was no interface between the IFOR/ARRC data networks (CRONOS and IARRCIS) and the strategic, theater, and tactical data networks of the MND nations and other participating nations.

The ADAMS, also developed by STC (now the NC3A), was used to coordinate and track NATO and national deployments. The ADAMS provided three main elements: the network for secure communication and data exchange; the software to support the analysis, planning, and management of the actual deployment process; and the databases describing the forces, transportation assets, and mobility infrastructure. NATO and national access to the ADAMS hub at SHAPE were provided through the public ISDN network via a router, a NATO approved encryption device, a terminal adapter, and an ADAMS workstation located at the appropriate NATO and national movement staff headquarters. At the outset, the initial users were the three framework nations, SHAPE, and the NC3A but soon grew to accommodate all NATO troop-contributing nations. The SHAPE Allied Movement Control Center in Mons, Belgium, and the IFOR Joint Movement Control Center in Zagreb, Croatia, coordinated the detailed deployment plans (DDPs) inputted from the nations and monitored and reported on the actual deployment. DDPs were text files describing what, where, when, and how things were moving. By the end of the deployment phase a total of 217 DDPs from 20 nations had been processed. The frequency of updates varied greatly between nations. Most of the nations provided updates only in response to significant events or changes to the plan. The United States on the other hand used a software interface between its JOPES and ADAMS to provide daily updates whether or not there were significant changes. This proved to be especially helpful for reporting actual movements.

The decision was made early not to extend the NATO strategic message network, the TARE, into theater. Instead, it was decided to provide an interface between the NATO data network, CRONOS, and the TARE and wrap the formal NATO messages (ACP 127 format) in an e-mail and send them via the interface (figure 11-10). There was one exception to this policy; a TARE termi-

Figure 11-10. Message Network



nal was provided at the Residency in Sarajevo for messages of higher classification than NATO SECRET and to be used as a backup in case the CRONOS LAN failed. The CRONOS LAN was unstable for the first several months of operation and did fail frequently. The United States extended a limited Automatic Digital Network (AUTODIN) capability into theater. The fact that the NATO TARE and the U.S. AUTODIN systems were interconnected at the strategic level made it possible to support some over-the-counter NATO messaging services for IFOR in Zagreb and Sarajevo.

Internet Service

Unclassified Internet was used frequently and demands for service increased throughout the operation. IFOR use of the Internet was not planned; its use simply grew with user demand. In MND(N) and the U.S. NSE, Internet access was provided via the NES and Tactical Packet Network (TPN), and via Point of Presence (POP) routers. Internet access was more widely available to U.S. forces than to NATO elements.

A limited theater-level Internet access was provided by the U.S. Army to IFOR, but IFOR really needed its own access that made Internet services more readily available to a broader IFOR community. The Public Information Office (PIO) used it for media interactions and home pages were created to inform the press and public about the operation in general. The intelligence community used it for open-source assessments; legal and medical personnel used it as a reference tool; and the engineers used it for activities such as predictions for the height of the Sava River to adjust the pontoon bridges. Deployed military personnel used it to maintain contact with their home organizations. It also had value as part of the MWR support—e-mails to home.

Internet access allowed the staffs to obtain information directly from sources around the world. As a result of the demand for Internet services by IFOR, NATO reviewed and revised its policy on restricted NATO use of the Internet. Users accessed the Internet by dialing through the U.S. DSN and the UN VSAT network to

gain access to the U.S. NIPRNET that had a gateway to the Internet. Access was also possible through other dial-in servers in Germany and in other locations. Later in the operation, the CJCCC provided an IFOR dial-up service to an Internet server connected to the Sarajevo UN telephone switch, which had a positive effect in off-loading the long data calls on the DSN and UN VSAT systems. Direct IFOR access to the Internet using the public network and commercial providers also became available.

IFOR Video Teleconferencing Service

Two Video Teleconferencing networks (figure 11-11) were established to support IFOR C2 decision making and to facilitate coordination, one for Commander IFOR and his command elements and the other for the Commander ARRC and his MND commanders. The ARRC also had a secure voice conferencing capability provided by the PTARMIGAN system. VTC was an essential element of the NATO command and control operations. The NATO VTC at the Residency in Sarajevo was booked regularly for most of the day. By August 1996, the network included Naples, Split, Zagreb, the USS *LaSalle*, ARRC-Main, SHAPE headquarters in Belgium, and LANDCENT headquarters in Germany. The United States also deployed an extensive VTC capability, it was the U.S. Army's C2 system of choice.

IFOR Intelligence Services

The overall intelligence architecture to support IFOR is depicted in figure 11-12. The figure shows the NATO, national, and lower level connectivity. The U.S. LOCE system was extended to division level to support IFOR intelligence needs. Nations also provided national intelligence support and services to IFOR through liaison officers and NICs. An ICC (Intelligence Coordination Cell) was also established at the Joint Analysis Center in Molesworth, England. The cell consisted of a number of different national representatives who helped respond to theater requests for information

Figure 11-11. IFOR VTC Network

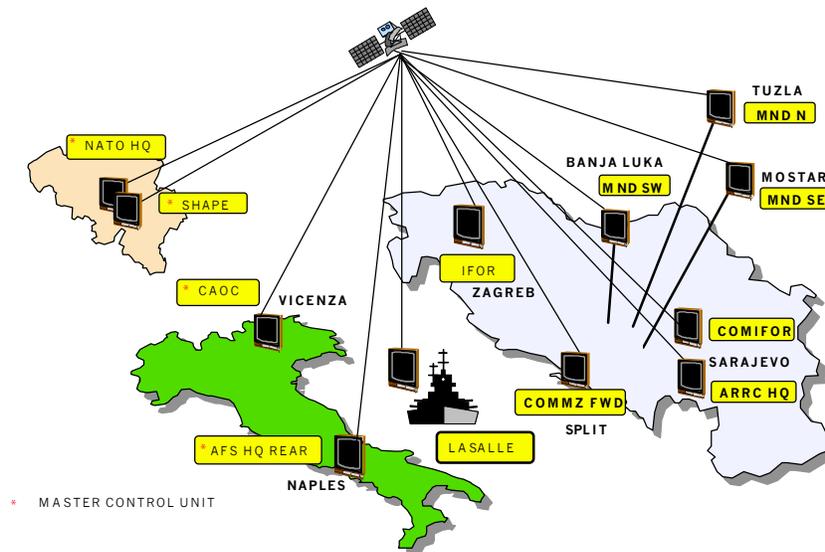
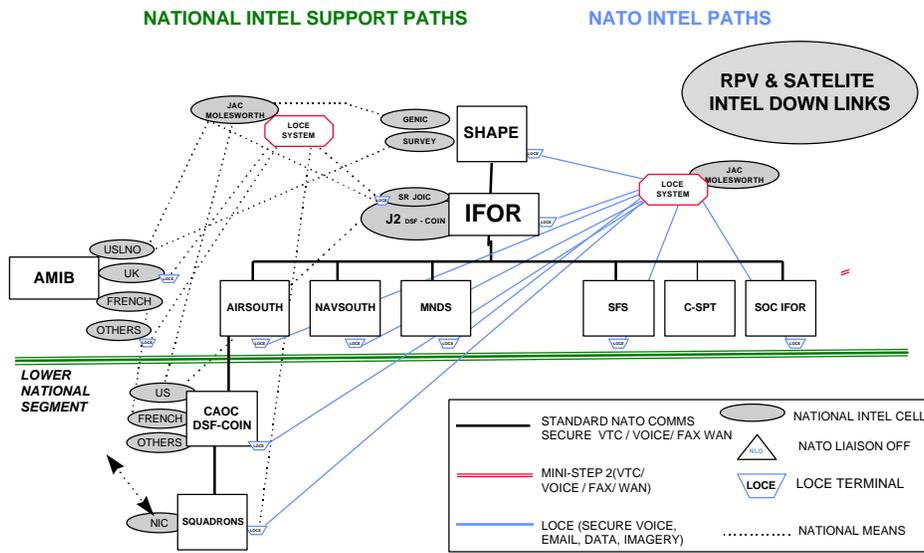


Figure 11-12. IFOR Intelligence Architecture



via the LOCE system. They also helped to clarify requests (language differences) from members of their national forces deployed in theater. The national representatives had direct communications access to their national intelligence sources for obtaining additional information to respond to specific requests from the theater and to add to the LOCE database for use by IFOR in general. The ICC was essentially a coalition “intelligence help desk.” The LOCE network provided the means for initiating the requests and disseminating the packaged results, including populating the LOCE servers with national data released to IFOR.

The multinational coalition operation, which included members from non-NATO countries, required the establishment of an IFOR Releasable category for classified information to be shared with IFOR and its partners in the operation. In terms of sharing, the United States extended access to some of its national intelligence capabilities, such as ASAS WARLORD workstations, to units assigned to MND(N) like the Russian brigade.

IFOR Air, Naval, and Special Operations Support

CIS support for air and naval operations remained in place following *Deny Flight*, *Decisive Force*, and *Sharp Guard* and did not require special efforts to integrate them into the IFOR operation. Although a reserve force was never allocated to IFOR, the Marine Expeditionary Unit offshore remained an option and had to be considered in the development of the CIS architecture. The Special Operations Forces CIS support consisted of both IFOR and nationally provided C4ISR capabilities. For example, the Joint Special Operations Task Force, also known as the Special Operations Command IFOR, located on the San Vito Air Station in Italy had a number of different C4ISR systems serving the operation. They had IFOR and national voice, message, and data services including for the United States, both collateral and SCI LANs for access to national capabilities. They had access to LOCE. U.S. systems such as JDISS, ASAS-Warrior, TRRIP, SOFPARS,

JSTARS, TIBS, and SOCRATES METOC were provided. In fact, there was a significant overlap in capabilities deployed to support SOCIFOR operations.

IFOR Non-NATO Nations Support

The non-NATO troop contributing nations did not have direct access to the IFOR CIS network. In order to facilitate communications between and among NATO and the non-NATO troop contributing nations (e.g., Austria, Czech Republic, Hungary, Russia, and others) who supported the IFOR operation, it was necessary to set up a special network using the public switched network. The U.S. supplied secure telephones (KY-71E) so that these nations and NATO could communicate securely either by voice or fax. In order to participate in the IFOR operation, the non-NATO units were required to provide funding and security assurances to NATO and to allocate their units to one of the IFOR MNDs.

IFOR Election Network

The High Representative, Mr. Carl Bildt, stated that free and open access to the media had to be provided as one of the 12 conditions for establishing a framework for free and fair national elections. Very few independent broadcasting stations were operational in Bosnia with virtually all of them being controlled by either the governments or entities. To circumvent this, two projects were considered: (1) a nationwide television broadcasting network called the Open Broadcast Network and (2) an FM broadcasting network called the Free Elections Radio Network (FERN). Both the Republika Srpska and Federation governments were unwilling to cooperate. Of the two projects, only the FERN was implemented. The project was realized mainly due to the drive of the Swiss government and the Office of Security and Cooperation in Europe, for which Switzerland was chairman. To implement FERN, IFOR compounds were used since other locations for transmitters were most likely mined. In addition, the UN had experienced theft problems

for radio sites that were not provided force protection. HQ IFOR, CJCCC, CIMIC, and IIC personnel were also utilized extensively for consulting, obtaining site access permissions, and verifying coverage patterns, frequency management support, and other services. In support of the elections, IFOR was responsible for protecting the election supervisors and IPTF personnel. As noted earlier, to accommodate this requirement ARRC communications personnel patched together a nationwide VHF Motorola network using IPTF, UN, and their own assets—if a nationwide cellular telephone network had existed in Bosnia, it would have been possible to provide communications to all election monitors.

IFOR Security Considerations

Security for the IFOR CIS network was provided through the use of approved NATO and national security devices. The CRONOS, LOCE, Tactical Voice, ADAMS, and VTC networks operated SECRET system high. STU-IIB secure voice units were available for use over the non-secure UN VSAT and PTT networks and on INMARSAT. Although the information networks were operated system high, other information protection measures, including network-level virus protection and intrusion detection and protection, were slow in implementation.

COMSEC management proved to be a challenge. Two theater distribution accounts had to be established to provide COMSEC support to IFOR forces—one to support Italy-based operations and one to support forces deployed to Croatia and Bosnia. The purpose of the accounts was to issue NATO material to those units who had no national distribution pipeline established in theater, to issue NATO crypto to national accounts, and to support national distribution in the event that national pipelines were not able to issue NATO cryptos to their deployed units. Normally crypto distribution is via the national pipelines to national units only. National regulations prohibit the issue of NATO crypto to other nations. The establishment of the special accounts was an attempt to streamline the process and ensure that cryptos would be distributed in a multinational environ-

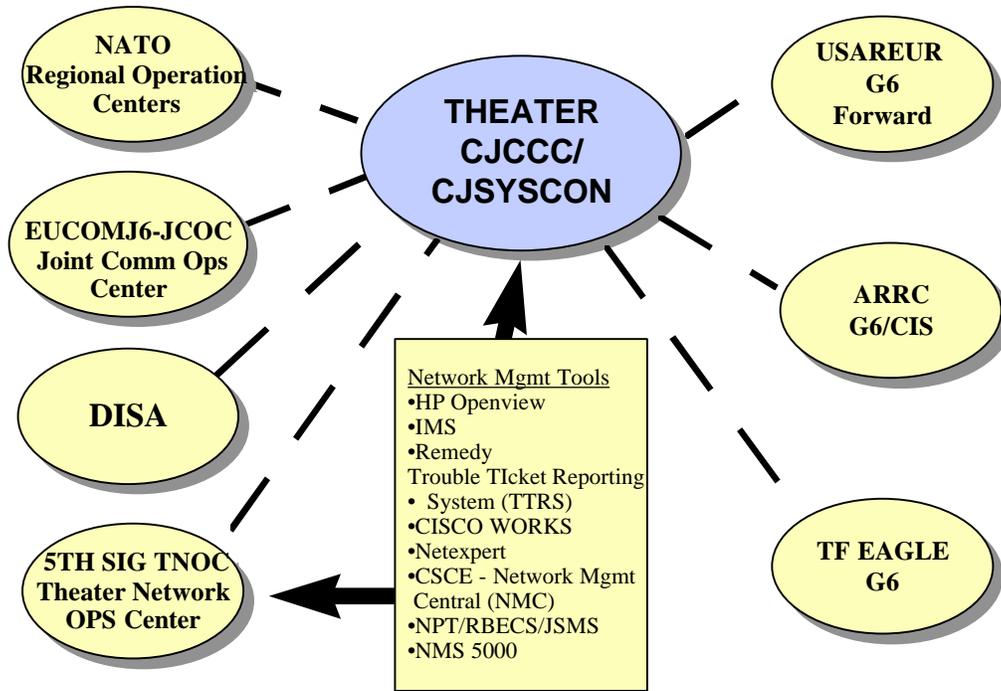
ment to NATO users. STU-IIBs were used to electronically distribute key material. This worked reasonably well but was limited by the availability of data transfer devices and the quality of the Croatian and Bosnian phone lines. In the future, NATO needs one crypto pipeline that is capable of distributing NATO crypto throughout the force; can electronically transfer key material; is rapid and secure; and can ensure that the key will get to where it needs to go.

IFOR Network and System Management

In order to pull the CIS planning, implementation, and management together, the IFOR CJ6 established a new organizational element, the CJCCC, to work with NACOSA, the ARRC G6, the MND G6s, the C-Support G6, and the national control centers (figure 11-13). The CJCCC (first located in Zagreb, Croatia, and then moved to AFSOUTH headquarters in Naples, Italy) was also responsible for managing the IFOR theater-level CIS network. NACOSA (located in Mons, Belgium, at SHAPE headquarters) had the responsibility for managing the NATO strategic-level CIS network. The Kester, Belgium, NATO satellite control center supported NACOSA in the management of the NATO IV satellite system. There were overlaps in the responsibilities of the CJCCC and NACOSA because of the blurring of the boundary between strategic- and theater-level systems. These differences needed to be sorted out early in the operation but the SHAPE/AFSOUTH C2 differences precluded this happening quickly.

The CIS organizational elements supporting the IFOR operation exceeded 4,000 personnel at the peak of the operation and the CJCCC alone approached 300 personnel. The CJCCC and IFOR CJ6 set up operation in Zagreb in early December 1995 but the IFOR CJ6 moved to Naples in January 1996. The CJCCC did not move to Naples until May 1996 where it managed the theater CIS network for the rest of the IFOR operation. On 4 November 1996, command of the CJCCC was transferred from AFSOUTH to LANDCENT in preparation for the 7 November TOA from AFSOUTH/IFOR to LANDCENT/IFOR and the TOA of the ARRC

Figure 11-13. Network Management



to LANDCENT/IFOR on 20 November. On 20 December 1996, TOA from IFOR to SFOR was accomplished and as part of this transfer, plans were initiated to move the SFOR CJCCC to Sarajevo. The CJCCC was subsequently renamed the Communications Information Systems Control Center (CISCC) and moved to Ilidza to be collocated with SFOR headquarters.

In response to the Dayton Accord frequency management tasking to IFOR, a Theater Frequency Management Cell (TFMC) was established in Zagreb at the outset of the operation. The cell deployed from Naples with little information on units to be supported, their number (ORBAT), their locations, their requirements, or their equipment in theater. The only available database was that of ongoing operations for *Deny Flight* and other UN missions. There was no information on the available spectrum and no Status of Forces Agreement. UN units transferred to IFOR were already using frequencies and would either continue to use them or change to other frequencies because of location changes and operations under different commands. The Sarajevo area also presented a problem because of the large concentration of units and associated communications equipment. The ARRC collocated its Field Management Office with the TFMC to coordinate and manage the frequency requirements in BiH for all land forces. The TFMC used automated tools provided by the United States and NATO. A TFMC Forward was eventually established in Sarajevo to act as the agent for day-to-day coordination within BiH and with the ethnic factions. The TFMC and ARRC FMO were relocated to Naples with the CJCCC move in May 1996. Over time, the TFMC was able to manage the use of the spectrum quite well. Most of the problems faced were caused by the lack of information on unit deployments, by organizations not being aware of the TFMC and the need to coordinate with it, by poor planning, and by late entries of frequency requests. On the civil side, there were problems because the RS was using Belgrade as their recognized frequency management authority, not the BiH. For instance, Belgrade TV was being relayed

illegally by RS transmitters. Also, the records of stations operating in BiH were inaccurate—few stations listed were still in operation, and many of the ones that were in operation weren't registered.

Logistic support under OPLAN 40104 was conceived as being a combined operation but because of national difficulties, it evolved into framework nations supporting their own forces and those allocated to them. Thus, the role of the Commander for Support became one of coordination and deconfliction and required changes to the CIS concept. A dedicated CIS logistics organization was established based upon the Southern Region Communications Logistics Depot in Lago Patria, Naples, which executed all logistical requirements in conjunction with forward sites in Zagreb and Sarajevo. Air transportation was provided by the IFOR shuttle flights and was a key element in the CIS logistic plan.

U.S. C4ISR Systems and Service

The C4ISR infrastructure provided by the United States to its deployed forces exceeded current Army doctrine. Capabilities included TRI-TAC/MSE, commercial telephone services at every base camp, and both secure and non-secure data network services at all base camps. MSE to DSN connectivity (more than 3 million calls completed), single channel TACSAT (supported operational, administrative, and logistic networks), INMARSAT for worldwide commercial telephone access, facsimile at base camps, and VTC to brigade headquarters were also provided. The MCS (Maneuver Control System), the ASAS WARLORD (intelligence), the WAN/LAN networks using Windows NT servers, and MSE communications connectivity formed the backbone information system for the division in MND(N). MCS was distributed to every major subordinate command element including the multinational units assigned to the division. The presence of MCS at each brigade level of command made the dissemination of information such as FRAGOs and OPORDs timely and efficient. MCS was also capable of providing multiple broadcasts of information to several C2 nodes using its

FTP capability. MCS was, however, somewhat complicated and not particularly user friendly. Furthermore, because of the inflexibility of its tools (e.g., mapping and word processing) to tailor the capabilities to meet needs particular to this mission, it was used predominantly as a communications hub rather than in its traditional role as a maneuver C2 system.

The U.S. communications and information systems deployment set a new standard for division and below. Doctrinally, only the brigade and separate battalions had voice and data capabilities. During the operation, all base camps had this capability and, in some instances, remote camps for isolated companies had the same level of support.

The 5th Signal Command was fully deployed by mid-March, with almost 700 personnel in country. *Operation Joint Endeavor* used the entire USAREUR theater-level multi-channel tactical satellite and large switch assets and still required augmentation with USAFE and commercial satellite and switching equipment.

U.S. Data and Messaging Services

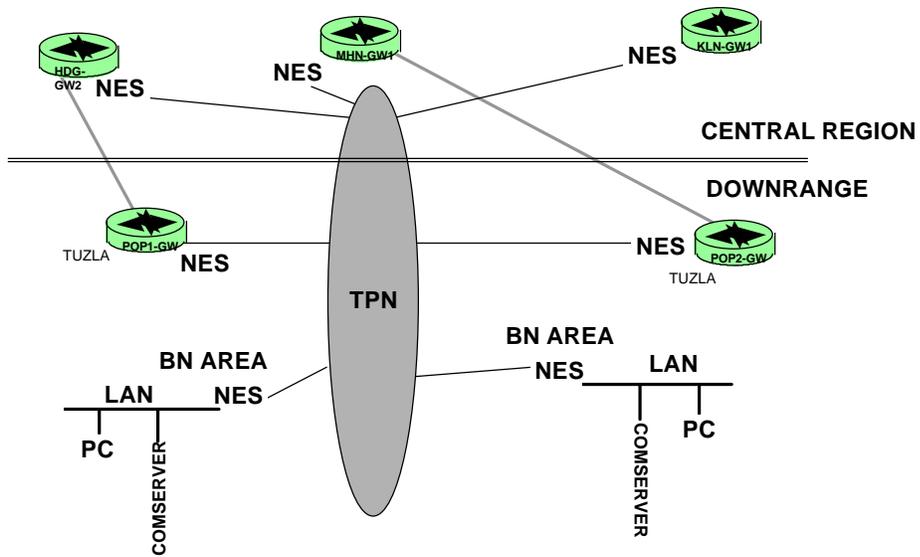
Most of the messaging requirements, both administrative and C2, were satisfied with unclassified TCP/IP Internet-like networks connected with routers and hosts. E-mail could and did carry AUTODIN messages. Classified traffic was handled through AUTODIN and SIPRNET to TPN to C2 systems such as STACCS, MCS, and SIPR LAN servers at major headquarters (figure 11-14).

Especially innovative was the use of the IDNX equipment, routers (CISCO Series), NES, and other COTS technology to establish a network that provided Internet, NIPRNET, and SIPRNET access via the TPN to every base camp. The 5th Signal Command anticipated that the data needs of the operation would exceed the capabilities of the TPN planned and that it would be necessary to augment the TPN. The 5th Signal Command developed and deployed the Deployable Automation Support Host (DASH) to the U.S. NSE at Kapsovar, Hungary, to facilitate the augmentation of the TPN. The DASH included NIPRNET and SIPRNET routers,

Figure 11-14. TPN/NES



Network Encryption System (NES) (for 17 Battalion Areas)



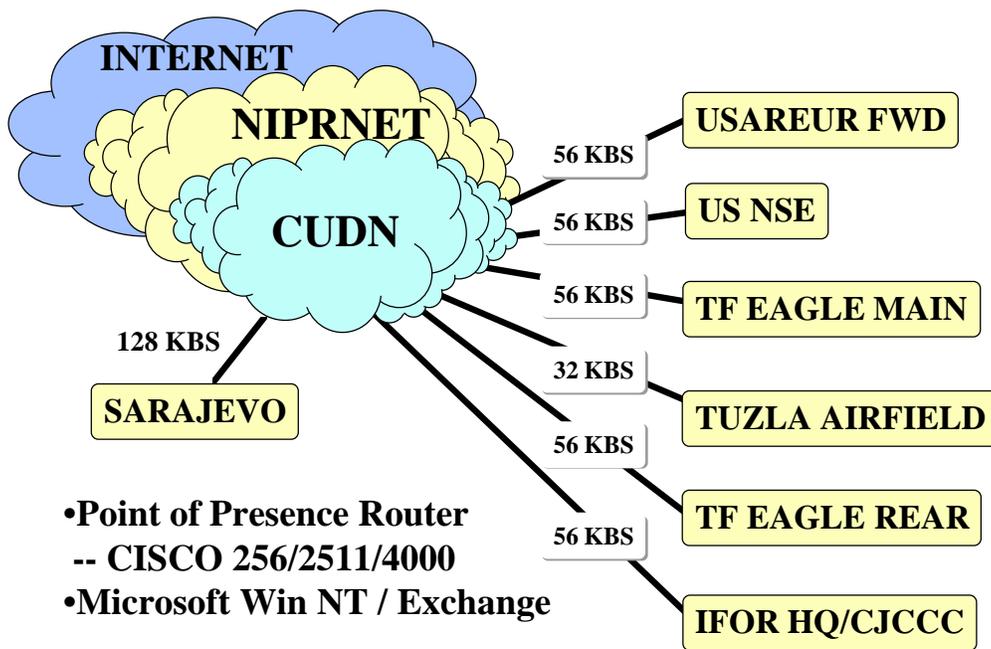
hubs, direct-connect/high-speed modems, cables, small routers, TTAs, and other equipment and installer kits necessary to support implementation.

A POP router network augmented the DASH and incorporated both dial-up and LAN subscribers. The routers were networked through 56kb/s links. The POP and DASH router network was interfaced to the Common User Data Network (CUDN) via 256kb/s access links (figure 11-15). The CUDN provided NIPRNET connectivity to Army customers in Germany. Through CUDN gateways to NIPRNET, the deployed users had access to the worldwide NIPRNET, including access to the commercial Internet. The transportable command post, the MSQ-126 (borrowed from CINCPAC assets), was deployed to Supply Area Harmon in Slavinski Brod, Croatia, and provided NIPRNET access through a 128kb/s link with the Heidelberg, Germany, gateway node. USAREUR (FWD) in Tazsar, Hungary, was provided access to the Heidelberg gateway through a POP router and 256kb/s link.

The POP router network employed the use of the NES to encrypt unclassified but sensitive traffic for transmission over the SECRET high TPN, thus protecting the TPN SECRET accreditation. The use of NES obviated the need for firewalls to allow unaccredited systems (e.g., used to overcome systemic problems of STAMIS accreditation) processing unclassified data to traverse the classified network, the TPN. The capability was fielded with nearly every Small Extension Node down to battalion level. Hence, the POP and DASH capabilities provided deployed users with a wide area network access through an Internet Protocol environment—another *Joint Endeavor* success story.

In the dynamic environment of *Joint Endeavor*, users arrived with a variety of operating systems and e-mail clients and different methods for accessing the network (e.g., dial-in and LAN). The Post Office Protocol-3 compliant server proved to be the most flexible and universal mail server standard available to deal effectively with the mix of capabilities deployed. Although this capability was not used for mail access, it was being considered for use in the future.

Figure 11-15. CUDN



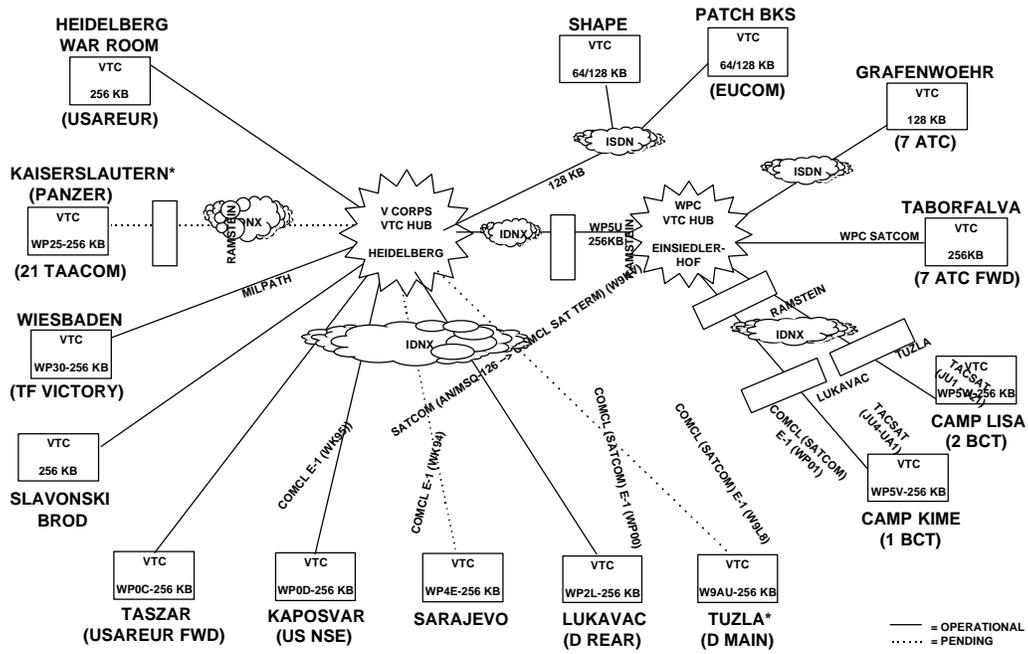
U.S. Video Teleconferencing Service

The United States deployed two different VTC networks (figure 11-16) to support U.S. needs—an SCI level for intelligence operation use and a collateral level for V CORPS. VTC became the command and control system of choice, especially for the U.S. Army. LTG Abrams (Command, V CORPS and USAREUR (FWD)), the Commander MND(N) and Task Force Eagle, and the three allied brigades were tied together over the U.S.-provided VTC network prior to the NATO system coming on-line. LTG Abrams, who pioneered the active use of VTC in theater, pushed this particular arrangement. He created a “virtual headquarters” that linked the ISB in Hungary with the rear area operations in Germany (four locations) and CONUS, as well as with Task Force Eagle, its brigades, and the Sava river crossing site. The combination of e-mail, the file transfer of PowerPoint slides, and the VTC to discuss both command and staff decisions was a look into the future of a “virtual” command post, a key element of command posts of the future. LTG Abrams stated that e-mail and VTC made the difference in a successful deployment and execution in Bosnia. He compared them to the use of TACSAT and GPS (Global Positioning System) in *Desert Shield/Storm*.

U.S. Reach-Back Service

The use of an Army-provided Reach-Back capability to the Central Region proved effective in providing access to a broader range of voice and information services available through gateways with the U.S. strategic network, the Defense Information Infrastructure. The capability provided good access to Army activities in the Landstuhl, Kaiserslautern, Mannheim, and Heidelberg areas where a lot of the deployed active duty forces came from. It also served the needs of a large number of the CONUS-based deployed forces,

Figure 11-16. U.S. VTC Network
JOINT ENDEAVOR VTC NET
 (PLANNED CONFIGURATION*)



such as the Civil Affairs and PSYOPS units. There was also a single-node Air Force Reach-Back capability to Ramstein AB, Germany.

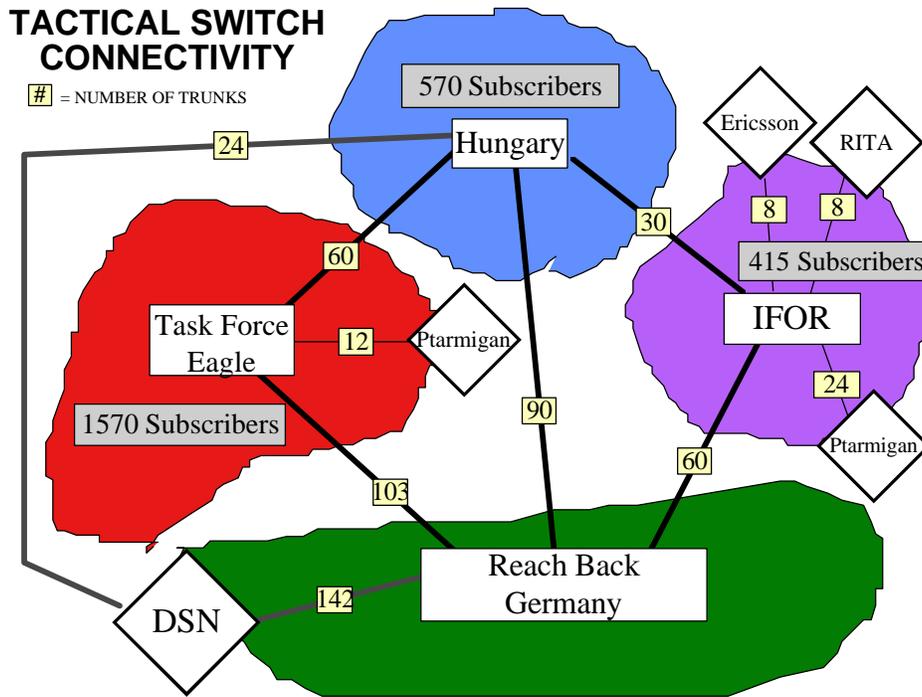
The Army Reach-Back nodes (figure 11-17) were set up in Germany several days prior to the deployment of the tactical equipment to Bosnia, Croatia, and Hungary. Upon arrival in country, the first priority was to establish connectivity with the Reach-Back nodes. Tactical satellite assets were used for this purpose and enough assets were also deployed to ensure that dual and triple connectivity could be established to other TRI-TAC switches as well. The tactical networks were interconnected with the U.S. strategic network at three locations in Germany—Heidelberg, Mannheim, and Kaiserslautern. At the peak of the operation there were 228 trunks connecting the tactical voice network to the Defense Switched Network (DSN) alone.

Other U.S.-Provided C4 Services

The Global Positioning System (GPS) continued to be an important military capability and was used for marking of the IEBL and the ZOS, vehicle tracking, asset tracking, and precision navigation and position identification.

At the outset of *Operation Joint Endeavor*, almost every Air Mobility Command location reported inadequate communications capability to include the transmission of classified information. The operating units at both Rhein-Main and Ramstein ABs, Germany, were unable to communicate with the CAOC in Vicenza, Italy, on a required basis during the first several weeks of the operation. This resulted in frustration, as tasking was not received in a timely manner. Questions concerning missions and/or operations could not always be answered directly without extended delays. For example, at Vicenza it took weeks to get a STU-III in the Regional Air Movement and Coordination Center (RAMCC). The RAMCC also did not have a classified e-mail capability. The working environment needed to safeguard operationally sensitive information, especially when participating in combined operations.

Figure 11-17. Reach-Back Capability



The Air Force C2 systems, the Global Decision Support System (GDSS), and the C2 Information Processing System (C2IPS) were undergoing upgrades when the operation was initiated. The systems were neither reliable nor user friendly. There were problems with the old and the new GDSS passing information to the old and new C2IPS. Some of the basic flight information was passed between systems, but remarks and comments were not. As a result, information about mission success, diversions, and cargo delivery was not always passed. The deployed operators also lacked adequate training to update and use the C2 systems and there were not enough trained personnel present and designated for ensuring that data was entered correctly and updated regularly.

Additionally, AMC resources were diverted from mission-specific tasks when duplicate requests for information were received from numerous agencies. There was a perception that the information being requested was for general information briefings and not decision making. For example, a request for a certain piece of information concerning aircraft reliability may have been pursued by three different divisions within the same directorate at AMC headquarters, as well as the TACC, the Air Staff and Joint Staff, and a variety of other organizations from the theater and throughout the DoD. As a result, deployed and headquarters personnel spent a great deal of time gathering and disseminating data and information instead of running the operation. This was a problem that was not unique to the Air Force but was pervasive across all IFOR and national organizational elements. Information requests must be managed carefully because they have the potential to grow and become more than just a burden on a given staff or organization.

The Air Force Mission Support System (AFMSS) was deployed to Rhein-Main AB. The AFMSS consisted of a deployable ground mission planning system and a portable system. The ground system was used for aircraft flight planning at the main operating base and the portable laptop system was used to plan missions at remote locations. The system deployed to Rhein-Main supported C-17 operations into Bosnia, including President Clinton and Secretary of Defense William Perry's visits to Bosnia. The C-17 crews

planned and built their missions, downloaded the information, and then loaded it into the C-17's onboard computer. The aircrews cut the mission planning time to less than an hour. The use of high-resolution imagery and digital terrain elevation data allowed aircrews to fly their missions on the computer. The system also provided airfield orientation, high terrain, and threat awareness and tactics analysis. AMC's Tanker Airlift Control Center used charts and maps produced by the AFMSS system at AMC headquarters to plan the initial routes used in the Bosnia airlift operation. AMC aircrews used AFMSS in daily operations between Rhein-Main and Bosnia. Additional support was given in providing joint operations graphics and charts to the JSTARS operations.

The late and somewhat fragmented arrival of the Army Combat Service Support (CSS) elements, coupled with the arriving users being unprepared to set up their communications and automation equipment (the long-haul communications at the NSE were up and operating), put them at a disadvantage at the outset. March and April 1996 were spent establishing support areas and finally in May the logistics communications were established, supply support areas became operational, and supply backlogs were diminished. The Standard Army Management Information Systems (STAMIS), such as SAMS, ILAP, SARSS, SIDPERS, SPBS-R, ULLS, TAMMIS, and SAAS, supported the operation. Logistics also became a proving ground for advanced technology and concepts for developing automated systems to support force projection. Systems such as Total Asset Visibility (TAV), Intransit Visibility (ITV), Automated Manifesting System (AMS), Objective Supply Capability (OSC), Exportable Logistics System (ELS), and others were deployed to help improve the operation. An interesting Internet aspect was the use of the World Wide Web by ITV to determine locations of parts shipped in containers marked with RF tags. The ITV Home Page allowed managers to use a requisition query process imbedded in the Website. This helped managers estimate when parts arrived, thus preventing duplicate requisitions and setting priorities for receipt processing on arrival. The downside of deploying the prototype information systems was that the advanced

technology outpaced the ability of the O/M support force to maintain the systems. The systems were also subject to environmental and human vulnerabilities that influenced their ability to provide reliable service, e.g., RF tags and bar codes missing, unauthorized software loads, untrained personnel trying to fix problems, freezing temperatures, high humidity, dust, and dirt.

U.S. ISR Systems and Services

U.S. intelligence, surveillance, and reconnaissance (ISR) support was the best that could be provided anywhere in the world. The United States leveraged its SIGINT, CI, HUMINT, OSINT, IMINT, and MASINT disciplines and capabilities and brought both its operational and advanced technology prototype systems to bear to provide the commander with “Information Dominance.” Also key to the operational success was the contribution of many different intelligence organization elements—EUCOM J2; the analysis centers such as the JAC, UCIRF, and FOSIF; support activities such as the NICs and the National Intelligence Support Teams; and the CI/HUMINT teams on the ground in country to name a few.

Historically, weather has had a significant impact on military operations and *Operation Joint Endeavor* was no exception. The Balkans lacked a modern meteorological system and indigenous weather data was sparse. The 7th Weather Squadron and USAREUR weather staff provided accurate, timely, and relevant weather intelligence. The SWO provided numerous briefings and products that included satellite weather imagery of the Central Region and the area of operation, 24- and 48-hour forecasts, and weather impacts on operations. Thanks to the use of a German satellite communications weather broadcast system, the amount of real-time useful weather data to the troops in the field was the best in the history of the U.S. military. Weather personnel were deployed to IFOR, the ARRC, USAREUR (FWD), MND(N), and several base camps, but lacked sufficient manning to provide observers to other key lo-

cations. Remote weather support required more reliable communications from both the Air Force and Army to ensure climatologic data was received by supported units.

The JWICS (Joint Worldwide Intelligence Communications System), JMICS (Joint Military Intelligence Communications System), and Trojan Spirit systems were used to extend wide-band intelligence services into theater supporting SCI and collateral secure voice, data, facsimile, video, secondary imagery dissemination, and other intelligence-oriented information services. The Trojan Spirit extended 128kb/s service to the brigade level, 32 to 64kb/s for SIPRNET, and the remaining bandwidth for JWICS (DISNET-3) and for secure telephones. This in itself was a success story. It was not, however, envisioned that Trojan Spirit would be used to support a broader set of C3I needs. The capability was limited in the number of terminals and capacity per terminal and was really designed as an intelligence community asset. INTELINK and LOCE information networks were used to support intelligent dissemination of intelligence and other information. The U.S. INTELINK and INTELINK-S also provided Internet-like Web services and Netscape browser tools to facilitate collaboration, coordination, and search capabilities for improved information retrieval and dissemination.

The JDISS, DISE, TRRIP, and other intelligent workstations provided access to a core set of intelligence databases and applications. JDISS was the theater link to the rest of the intelligence world. TRAP, TIBS, and TRIXS broadcast and intelligence exchange services were provided. The ASAS-WARLORD workstations that supported all source data processing and manipulation formed the backbone of the division intelligence architecture and were used extensively. Access to ASAS-WARLORD was provided to the NORDIC and Russian brigades and the Turkish battalion supporting MND(N). UAVs, such as Predator and Pioneer, were used extensively for monitoring important areas of interest. NATO AWACS, JSTARS, U2, and other capabilities were employed to provide information that could be used to demonstrate to the FWF

that they could be seen any time of the day or night and under all weather conditions. The message was clearly sent to the FWF that compliance would be closely monitored and enforced by IFOR.

There were innovative uses of deployed capabilities to meet operational needs. For example, the AH-64 gun camera tapes were processed through the MITT, which is normally a CORPS-level asset but was deployed to the division for this operation. Using the MITT frame-grabber capability and annotation software, it was possible to select an image or frame and exploit the still image. Hence, exploited unclassified images could be produced within 12 hours and given to the allies and the FWF. It was easy to convince the FWF to move tanks out of the ZOS when you could show them a clear picture with the AH-64 crosshairs on the side of the tank. Interestingly, in a 1992 Army after action report for *Desert Storm* it was noted that better use should be made of the helicopter gun cameras for intelligence purposes in support of the ground commander. It took a couple of innovative enlisted men several years later on the ground in Bosnia to recognize and use the new technology deployed for other purposes in a different way to bring it to a reality. The capability was also used with Combat Camera footage and amateur handheld video camera tapes.

Timely transmission of Combat Camera and CI/HUMINT digital camera products and the integration of these products into the information operations network were challenges faced early in the operation. Adjustments had to be made to accommodate these needs. One of these adjustments was the integration of the U.S. CI/HUMINT commercial notebook computer-based data acquisition, management, and communications system into the SIPRNET. The capability is referred to as TRRIP (Theater Rapid Response Intelligence Package). Linking the U.S. MSE network with the SIPRNET via Trojan Spirit provided connectivity to the battalion level for TRRIP users and significantly enhanced the operational effectiveness of the CI/HUMINT teams—a real success story. MSE in MND(N) was also linked to SIPRNET via the reach-back locations and this offered an opportunity to access a much greater capacity than the Trojan Spirit linking.

Another innovation based on commercially developed and available technology occurred in February 1996, when the CI/HUMINT team in Tuzla realized that the TRRIP too could play a role in exploiting Apache gun camera and other video sources to obtain images for the brigade commanders. By using the SNAPPY commercial freeze-frame product plugged into the back of the TRRIP, they could view video and do frame grabbing. The TRRIP lash-up did not have the annotation capabilities of the MITT but it could give the commanders snapshots of violations or other insights that they could then use with the FWF or otherwise. In this case, several SNAPPYs (high 8 video cameras, small-screen viewers, batteries, a freeze-frame printer, and power packs) were purchased by OSD(C3I) Office of Special Technology and provided to CI/HUMINT teams within 1 week of identifying the requirement. This COTS solution significantly enhanced the CI/HUMINT team capability at the brigade and battalion levels.

There were numerous other strategic and tactical ISR and communications capabilities deployed to support intelligence operations. Many of the systems deployed were stand-alone, and it was not clear to personnel in theater whether adequate consideration had been given to the integration of these capabilities in the operational environment. Division personnel felt that the burden of integration was placed on the units rather than having been done in advance of deployment as part of an integrated intelligence architecture. As a result, there were duplications and inefficient use of scarce bandwidth. This situation also contributed to training, maintenance, and logistic support problems as well as system performance and responsiveness to user needs. Furthermore, there was no one computer system that effectively balanced power, flexibility, and user-friendliness. The units had to determine the best machine to build a particular database on and the best format to put it in.

Bandwidth Limitations

In spite of the enhanced capabilities and broadband systems extended into theater, the warrior on the ground and on the move was still operating in the range of kb/s. Some were getting access to 64kb/s but most were still limited to something less than this and in many cases had to operate in the 2.4kb/s to 9.6kb/s range. The JSOTF2 was allocated 32kb/s access, which in their assessment was insufficient to meet the intelligence systems communications needs. The Task Force Eagle G2 After Action Review noted that the MSE was not powerful enough to handle the division intelligence dissemination needs and this impacted their production and dissemination operations. The Task Force's 26 WARLORD terminals were interconnected via the MSE packet switch network. The graphic presentations, maps, and images produced could not be easily disseminated to the brigades over this network because the interconnecting communications pipes were too small. Instead, the production method had to be tailored to meet dissemination needs. If products were to receive wide dissemination they would be produced in textual format to ease dissemination problems. If the products were to receive limited and specialized dissemination then graphics were the medium of choice. In either case, production and dissemination operations were being affected by the size of the communications pipes. DISA-Europe lessons learned also noted that the military tactical systems were unable to fully support the bandwidth demands (e.g., VTC, SIPRNET, NIPRNET, and telemedicine) and leased commercial service was the only way to provide the deployed commanders the same service they were used to in garrison. It was also necessary to use contractor personnel to fill the gap in trained military O&M personnel in country. The use of commercial products and contracted O&M personnel added training demands for both the military and the contractors.

U.S. Advanced Technology Systems

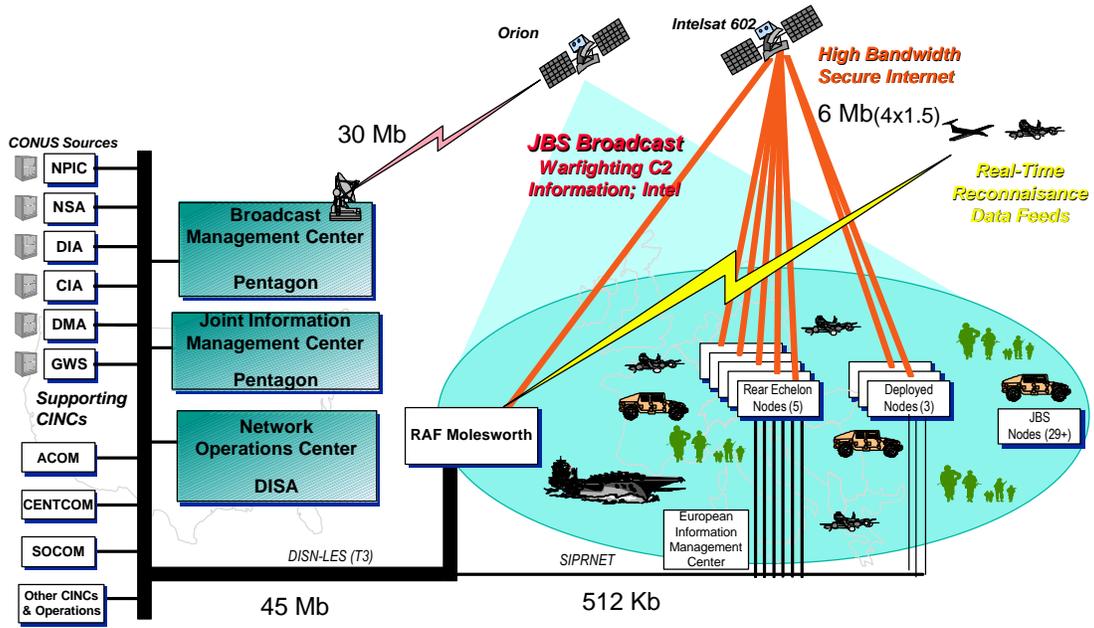
The advanced technology community stood poised to offer enhanced C4ISR capabilities for U.S. national and selected IFOR use. A wide range of the U.S. military's advanced technologies were deployed to the Bosnia theater which, among other capabilities, allowed the troops in MND(N) to electronically reconnoiter the landscape with a thoroughness that essentially allowed them to see day or night, in all weather, and in real time. The surveillance capabilities ranged from satellites in orbit to remote sensing devices buried in the ground, with an array of air and ground systems in between. If within an "area of interest" a phone call was made, a radio message was sent, or something moved on a Bosnia highway, the odds were it was known to the commanders and tracked by the systems.

Some of the advanced technologies were used before the IFOR deployment. For example, the PowerScene, a 3-D terrain visualization simulator (designed by Cambridge Research Assoc.) using computer-enhanced composites of satellite imagery, maps, and photographs, provided access to a "virtual Bosnia" that could be used to "fly" over the entire country and see realistic details down to one-meter resolution. The system was used for preflight rehearsals during the 1995 NATO bombing attacks and it was also a critical component of the Dayton peace talks. Tactically, the 1st AD used it to plan troop movements through a potentially hostile Bosnia countryside.

The Bosnia C2 Augmentation System/Joint Broadcast System (figure 11-18) was deployed in spring 1996 to provide improved wide-band connectivity and broadcast information services. These services accommodated intelligent push and pull of critical C2 information and services, such as intelligence, weather, broadcast news, and GCCS services to IFOR, the ARRC, and the MND headquarters. JBS was also used for real-time Predator video distribution.

The Army fielded the most advanced telemedicine system in history to provide medical care to U.S. forces in Bosnia, Croatia, and Hungary. The high bandwidth system supported applications

Figure 11-18. BC2A/JBS



such as telesurgery, telemedicine, telepsychology, and teledentistry. The Landstuhl Regional Medical Center in Germany, the Combat Support Hospital (CHS) in Tszar, Hungary, and the 212th Mobile Army Surgical Hospital (MASH) in Tuzla were linked to each other and to medical centers in the states. Internet access was also provided. It was reported by DISA that about 10 percent of the U.S.-provided bandwidth in the operational area was allocated to telemedicine activities. This focused attention on the need to reexamine the priorities for circuit preemption, since traditionally higher priority C2 and mission support users preempted telemedicine consultations either in progress or scheduled to temporarily restore failed circuits supporting their operations.

The Joint Total Asset Visibility (JTAV) system was another advanced capability deployed to Hungary and Bosnia to track assets on order from a supplier, in transit, or in storage. JTAV was not the only asset visibility system deployed. A system was developed by the Volpe Transportation Center that used RF tags and GPS, and the International Transportation Information Tracking (In-transit) system was also deployed. The Army also used a number of tiered logistics systems such as the Unit Level Logistic System, the Standard Army Retail-Level Supply System, and the Department of the Army Movement Management System.

U.S. Network and System Management

Network and system management was the glue that held all of the U.S. C4ISR pieces together. There were a number of different players on the U.S. side. The Joint Staff (J6Z) managed UHF and SHF SATCOM allocations and coordinated Joint Staff responses to CINC requests for additional contingency asset support. USEUCOM (J6) established a Joint Communications Operations Center to monitor and coordinate theater CIS activities. DISA-EUR managed the European theater Defense Information Infrastructure and extension of its capabilities such as DSN, NIPRNET, SIPRNET, and the IDNXs into Croatia and Bosnia. DISA and the Regional Space Support Center managed the DSCS satellite sys-

tem. The DIA managed the Joint Worldwide Intelligence Communications System (JWICS) and its extension into the area of operation. USAFE established a network operations center in Ramstein, Germany, to manage Air Force assets supporting the operation. USAREUR/5th Signal Command managed the Reach-Back and the deployed voice, data, and VTC tactical networks from their Theater Network Operations Center (TNOC) in Mannheim, Germany. They were the principal provider of staff and expertise to the CJCCC and they also had network management capabilities and staff at USAREUR (FWD) in Hungary, Task Force Eagle in Bosnia, and other brigade and battalion network management operations. There were other organizations managing mission support systems for logistics, medical, personnel, and other activities. The intelligence community had a number of different organizations managing the numerous ISR systems and services supporting the operation, including the Joint Analysis Center in Molesworth, England, and the USAREUR Combat Intelligence Readiness Facility in Augsburg, Germany. Finally, DISA established a Joint Information Management Center in the Pentagon to manage the BC2A/JBS.

The Defense Information Systems Agency (DISA) reported that they processed more than 1,400 Telecommunications Service Order (TSO) requests for extension of Defense Information Infrastructure (DII) connectivity and services into the theater. Over 740 of these requests were urgent, with 400 of them being requested within the first month of the deployment.

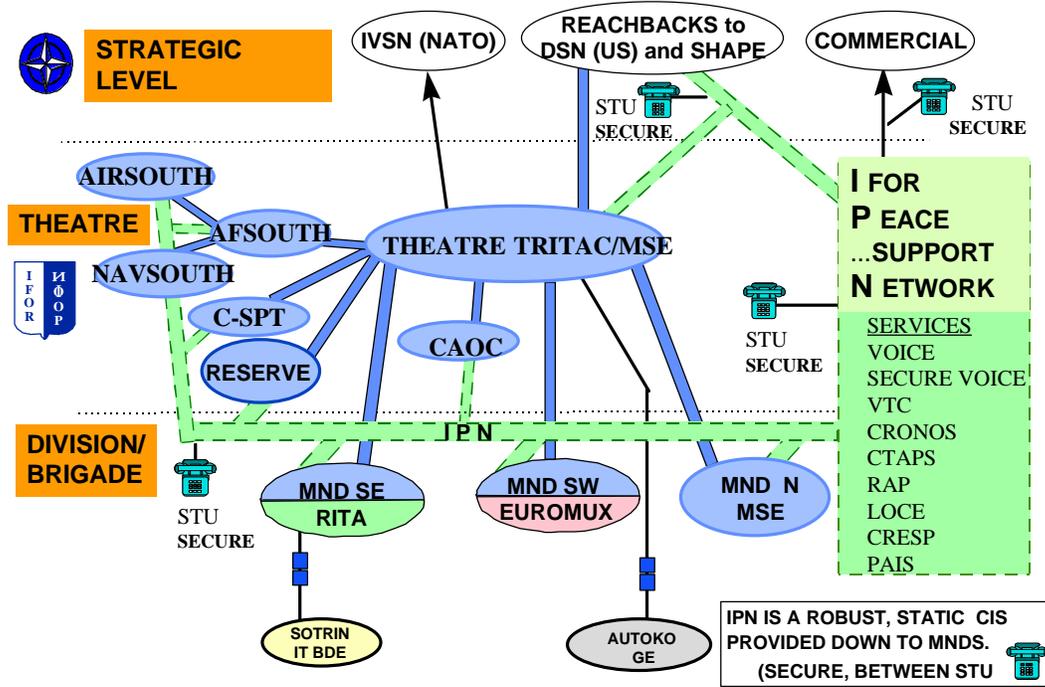
Transfer of Authority—CIS Implications and Unintended Consequences

The redeployment of the ARRC was accompanied by the redeployment of the UK Signal Regiment (the United Kingdom was the framework nation supporting the ARRC) with its PTARMIGAN and IARRCIS CIS systems, including some other C2 capabilities. The U.S. TRI-TAC/MSE network was expanded to replace PTARMIGAN at the corps level and to provide connectivity to the

SFOR Multinational Forces. The IFOR CRONOS system replaced the IARRCIS as the C2 capability for SFOR. The EUROMUX system was deployed by the UK in MND(SW) to replace the PTARMIGAN system at the division level. The replacement of PTARMIGAN with the EUROMUX resulted in some interoperability problems between the EUROMUX and MSE and the TTC-39D that needed to be resolved. For example, at the conclusion of the IFOR operation, the EUROMUX interface to the U.S. systems was only working in one direction. Calls could be initiated from EUROMUX to the U.S. network intercept operator but calls could not be completed from the U.S. systems to EUROMUX. EUROMUX was a newer version of PTARMIGAN but with less functionality. EUROMUX had fewer switching capabilities than PTARMIGAN but was much more suitable for a smaller user base such as the new operation. The EUROMUX had an advantage over PTARMIGAN in that it was more modern and required much less manpower to operate. The SFOR configuration resulting from the redeployments is depicted in figure 11-19.

In addition to the withdrawal of the ARRC framework nation CIS systems (i.e., the UK PTARMIGAN and IARRCIS), the TOA to LANDCENT/SFOR also required some reconfiguration and redeployment of the IFOR-procured CIS infrastructure, some of which was destined for AFSOUTH's use. Part of the reconfiguration included accommodating the move of the headquarters SFOR from the annex at the Tito Residency to Ilidza and the modernization of the SFOR command center CIS support. Therefore, CIS equipment essential to the headquarters of the LANDCENT Component Commander and Commander SFOR had to be replaced in some cases and added to in other cases to meet SFOR requirements. In regard to the latter, the CRONOS local area network (LAN) established at the SFOR headquarters was extensive. Its LAN featured a 100mb/s backbone, 10mb/s links at the staff level, fiber optic links to the workstations, connections to 13 external wide area circuits, and a substantial population of workstations. Although most of the information distribution was by e-mail, automated data replication using the Public Folder tool and access via

Figure 11-19. SFOR CIS Network



Web-based tools were also introduced. Expanded functionality for CRONOS applications such as PAIS and CRESP was included as well.

NATO HQ staff needed to be convinced that equipment already procured for IFOR could not be used in toto to meet LANDCENT/SFOR requirements. This raised the significant and ongoing challenge of equipment accountability. Despite the questions of eligibility, NATO common funding of CIS infrastructure was approved and procurement initiated to support the LANDCENT/SFOR requirements.

There were unintended consequences associated with the TOA to LANDCENT and the removal of the ARRC and the PTARMIGAN, IARRCIS, and other ARRC-provided CIS capabilities. EUROMUX and MSE did not entirely replace the functionality of PTARMIGAN. For example, there was no replacement for the PTARMIGAN secure voice conference capability and secure SCRA. The UK THISTLE system, which was used by the ARRC to build and distribute the ground order of battle, was pulled out. The ARRC's geographic support, which provided the map and boundary databases used by all IFOR command elements, was not removed but arrangements had to be made with the UK to lease the system to NATO. And finally, the CIS capabilities of the Allied Military Intelligence battalion were also impacted by the withdrawal of ARRC equipment. These capabilities either required replacement or enhancements to support the SFOR operation adequately. As a result, some confusion, difficulty, and expense caused a delay in providing minimum essential CIS to the new HQ SFOR in Sarajevo.

The TOA to LANDCENT/SFOR also had some unintended consequences for the U.S. military CIS providers. Since the commander LANDCENT/SFOR was also the commander USAREUR, it was necessary to provide additional CIS capabilities to support his national responsibilities. Some of the services that had to be extended to the new headquarters facility in Ilidza (outside of Sarajevo) were secure and nonsecure (including Internet) data network and e-mail services, extensions off the Red Switch in Stuttgart,

U.S. Secret mobile radio communications, and numerous DSN secure telephones. TACSAT and line-of-site communications, secure facsimile, U.S. television, and video teleconferencing were other capabilities that had to be provided. Simultaneously, Task Force Eagle downsized and transitioned from the 1st Armored Division to the 1st Infantry Division. The tactical network changed from the 22nd Signal Brigade and 141st Signal Battalion to the 121st Signal Battalion. The NATO and associated MND(N) downsizing (60,000 to 30,000 troops) and leadership change resulted in a major reconfiguration of the U.S. tactical satellite and switched network support to NATO throughout the area of operation as well.

Commercialization—A Key Player

Commercialization came in several forms. First, commercial products and services were used to augment the military systems deployed, as was the case with the IDNX and VSAT. In some cases, such as the NATO CRONOS network and U.S. NIPRNET and SIPRNET, they provided the strategic- and theater-level information services required for command and control operations. Commercial products and services were also an integral part of advanced technology capabilities deployed to theater, e.g., the U.S. BC2A/JBS information services and broadcast network. Commercialization played a role in the exit strategy when used as a means to replace tactical telecommunications systems with commercial capabilities such as the IPN for the IFOR telecommunications network and the Sprint contract to replace U.S. tactical systems in Hungary and Bosnia.

Use of commercial, off-the-shelf (COTS) desktop and laptop computers and use of Microsoft Office Professional and MS mail were crucial steps in achieving information standardization for the IFOR operation. Microsoft Mail was not a universal platform that lent itself well to a dynamic environment such as *Joint Endeavor* where different e-mail clients and operating systems were employed.

The only operating system that could be used to access Microsoft Mail remotely was Windows 95. Some users had to purchase Windows 95 so that they could access the system.

Information was easily exchanged using MS Word, PowerPoint, and Excel. MS Word was used by MND(N) to write FRAGOs, which were sent using FTP through the MCS to the subordinate commands. No comprehensive software users training was provided and so many operators had to learn on the job. Advanced training would have made it easier and faster for all users to learn MS Office Professional.

Using non-ruggedized hardware required special consideration. Daily cleaning and use of protective covers and power surge protectors were a must in the Bosnia environment. Handling of 3.5-inch diskettes and other removable data sources had to be done carefully as well. Disks needed to be kept clean to avoid loss of data. Double sources of storage when practical and disk covers and protective cases were also measures used.

The commercialization of IFOR communication systems was one of the goals for the overall improvement of the CIS architecture. The timing for withdrawal of the tactical systems was very much related to the success of the commercialization process. Tactical communications systems provided the advantages of mobility, flexibility, and security. Mobility and flexibility for communication systems became less important considerations as the operation continued and the headquarters remained almost entirely static. Security for the commercialized network could be met by means such as STU-IIBs for the voice network and operation of the secure data networks CRONOS and LOCE and the secure VTC network SECRET system high. Hence, it was possible to withdraw tactical systems once the commercial network was capable of satisfying the IFOR operational needs.

The military commercialization strategy must, however, take into account the disposition of the entity one plans to lease from or have a contractor operate in—both the political disposition (willingness) and the technical disposition (enough infrastructure to provide the service). PTT commercialization worked well in Croatia,

but they were really “in the rear.” In the Federation, the PTT was fairly cooperative, but didn’t have the infrastructure. Contractor-provided service in these two areas worked fairly well, but was slow to deliver, especially since the bandwidth requirements were raised during and after acquisition of services. In the RS, nothing worked—PTT or contractor. Contractor support outside of IFOR compounds in RS areas was not obtainable because of lack of cooperation.

The IFOR plan for the commercialization of their communications network was also aimed at reducing the costs to NATO and reducing the IFOR dependence on the UN VSAT network. The plan was to install ERICSSON MD-110 digital switches at the major headquarters, expand the commercial VSAT/IDNX network, and lease E1 connectivity including cross-IBEL connectivity from the BiH and Croatian PTTs. The evolution of the commercial network, the IFOR Private (Peace) Network (IPN), was slower than IFOR would have liked. The main difficulties centered on the slow reconstruction of the BiH PTT infrastructure and the continued unwillingness of the FWF PTTs to provide cross-IEBL connectivity.

The United States also had major commercialization efforts in Tazsar and Kaposvar, Hungary, and Tuzla, Bosnia. A 5th Signal Command contract with Sprint (supported by Lucent and MATAV) was used for this purpose. The voice part of the Tazsar/Kaposvar effort was completed in two parts, approximately 50 percent in December 1996 allowing a return of 163 signal soldiers and the rest in February 1997 allowing the return of the remaining soldiers. The data part was finished in April 1997. The reduction in CIS personnel in MND(N) was a result of downsizing and to a lesser degree commercialization. The commercialization of seven base camps in Bosnia (completion scheduled for the spring of 1997) and the NATO force downsizing (about a 50-percent reduction) under *Operation Joint Guard* would contribute to a further reduction in the U.S. military CIS personnel in theater. It was estimated that the U.S. CIS military support personnel in country would be reduced from a high of more than 2,200 at the peak of the operation to just over 300 personnel upon completion of these actions.

There were some important lessons learned in the Army's commercialization efforts. First, the vendors could not respond quickly. One needs to plan on 120 days to contract and 5 to 6 months after that for the vendor to become fully operational. The problem is that vendors are not prepositioned or prepared to send mobile systems to operate in a field environment with an inadequate support structure. Second, the vendors are unable to hire technical personnel who are willing and able to match military personnel or DoD civilians in the field in technical expertise, dedication, and sense of urgency. This observation may run counter to conventional wisdom, but technical skills are in short supply in the workforce and commercial vendor personnel are not accustomed to the demands of the military in the field.

Contracting—Unexpected Challenges

NATO and national acquisition of products and services for use in the IFOR operation was not strictly centrally controlled, so there were inconsistencies in costs, spares, support arrangements, training, and documentation. For example, USAREUR did not coordinate its contracting with NAMSA (NATO Maintenance and Supply Agency), the NATO contracting authority in country; they used their own contracting officer. This required USAREUR contracting personnel to come from Germany and Hungary to accomplish the contracts mission when in-country NATO contracting officers could have accomplished the mission if an agreement with NATO had existed. There were few standing contracts to support contingency acquisitions. For example, at the outset DISA had a contract in place for use of the commercial space segment (the CSCI contract for transponder leasing). However, there was no DISA or other contract vehicle in place for providing earth terminals and for the installation of other equipment such as IDNXs, routers, and the O&M of installed equipment. The CSCI concept placed the responsibility for user access on the end users' CIS support organiza-

tion. They were to provide the access arrangements such as a SATCOM terminal and access equipment to extend the service to the end user location.

Control of PTT costs was also a serious problem. There was no mechanism for logging commercial calls or recording usage of PTT access. Extensive operational use was made of available commercial PTT access. This was extremely expensive, but an essential way to do business, especially during the early phases of the operation. It is difficult to control the use of commercial PTT and prevent abuse, but some form of call logging and usage tracking would help.

Competitive bidding did not always realize the best product for price and in some cases did not work for IFOR. A lowest cost bid for a computer mouse bulk purchase resulted in the delivery of poor-quality equipment that failed after several weeks of use. A similar problem was experienced with the acquisition of tape for marking the minefield areas. It was also felt that the competitive bid for the NATO UHF TACSAT terminals led to different quality products (purchased 106 Harris PRC-117D and 106 Motorola LST-5E). The LST-5E narrow band performance was much better than the PRC-117D. In addition, the warranty repair cycle was much more responsive for the LST-5E (the theater experienced a period of 2 months of no spares for the PRC-117D before repaired sets were received through the warranty program, but did not have any spares problems for the LST-5E). Competitive bidding also did not necessarily work when dealing with the Serbs, since frequently there was only one source and price.

Vendor quality was also important, especially considering the environment in which IFOR operated. Vendor services and products did not always meet expectations. For some vendors, such as IEC, this was a new experience for them as well as NATO, so both were on a learning curve. NATO and national acquisition processes had to be streamlined in order to meet the time-sensitive needs of the deployment. Use of the U.S. FMS process was attempted to ac-

quire IDNX equipment for NATO, but the process in the end proved to be too slow and cumbersome to achieve rapid acquisition. A contract between NATO and N.E.T. was used instead.

Spares and Repairs—A Steep Learning Curve

Providing spares was also an issue. Inadequate spares were purchased for equipment procured under emergency acquisitions. There were no Radio Shacks or Tandy's in Bosnia to buy spare parts or other emergency off-the-shelf products. Vendor maintenance personnel of the right ethnic group did not always exist in the region of operation and special measures were necessary to get access to such personnel. Such a case was reported in MND(N) where a repairman was a Croatian and the U.S. military had to be used to get him through Serb territory to fix the equipment. In Bosnia, and the Sarajevo area in particular, all transactions were in cash and German DMs were preferred. Most vendors wanted hard cash up front and many preferred not to have formal contract arrangements.

Repair of commercial and military CIS equipment that failed in country presented some interesting challenges. Identification and evaluation of failed equipment was a problem, sometimes due to a lack of experience with the commercial equipment and in other cases due to inadequate training, documentation, and test equipment. There were warranty issues; for example, who does what repairs where? Most ADP equipment was under warranty and therefore no maintenance could be performed on it. Specific examples were computer hard drives and memory chips. Those used on SECRET LANs, for example, could not be sent back to the manufacturers for repair. For the LST-5E UHF TACSAT equipment, the antennas and handsets were not under warranty and could be repaired using operational spares; otherwise, the equipment had to be returned to Motorola for repair. There were issues related to getting the failed equipment out of theater to repair facilities and then back in country to the user, including tracking of the status of the repair process; shipping

delays; repair turnaround time; and slow and often unreliable Customs processing. The repair turnaround times for assets under warranty were in many cases excessive and impacted mission capabilities.

Although USAREUR had done some thinking in advance of deployment, contractors as well as the military still found themselves on a steep learning curve once they deployed. There were issues related to where repair facilities should be located, e.g., at vendor repair facilities, at government repair facilities in Germany, at the Intermediate Staging Base in Hungary, or at facilities in Bosnia. The NATO supply system did not support NABS and TSSR equipment and special arrangements had to be made with the CJCCC to establish logistic support procedures. In this case, the equipment was sent to the 1st Combat Communications Squadron deployed in Tuzla, which then forwarded it to the Air Force repair facility at Ramstein AB, Germany. The U.S Army experienced problems with some 6,000 pieces of CIS equipment during the first 6 months of the deployment. These problems included software glitches, hardware failures, integration problems, crushed computers, dirty line printers, and computer mouse problems. Many of the issues were pervasive and difficult to solve in an operational environment.

Interoperability—Making Progress

Historically, interoperability has been one of the most difficult areas to deal with and this operation was no exception. Integration and interoperability of commercial and military systems were not always straightforward either. The IDNXs and VTCs required special interfaces with the military, PTT, and UN VSAT networks.

The analog-based STANAG 5040 was still the norm for interfacing strategic, theater, and tactical voice systems. The interface was slow, inefficient, and lacked functionality to effectively integrate the strategic and tactical voice networks to accomplish a true “system of systems.” No digital interface existed for interfacing strategic and tactical digital networks. The TTC-39D experi-

enced interface problems with the ERICSSON MD-110 switch used by the UN and IFOR. The Interim Digital Interface PTARMIGAN (IDIP) was designed by the United Kingdom specifically for this operation and was used to provide a more effective digital interface between the UK PTARMIGAN and the U.S. TRI-TAC/MSE tactical systems. Marc Space, a U.S. company, designed a special interface box to allow the PTARMIGAN store and forward to interface with the U.S TYC-39 tactical message switch—the interface was demonstrated at *INTEROP 95*. The EUROMMUX that replaced PTARMIGAN in the MND(SW) was not capable of accommodating a STANAG 5040 interface. Therefore, there were problems interfacing it with the TRI-TAC TTC-39D which replaced PTARMIGAN at the CORPS headquarters level (i.e., SFOR headquarters and its interfaces with the three MNDs) and the interface between MND(N) and MND(SW).

The IDNX deployment required the certification of some 50 different interface arrangements. There were no automated interfaces between the IFOR data networks (CRONOS, IARRCIS, and LOCE) and national data networks, such as the U.S. NIPRNET and SIPRNET. The CRONOS was not interfaced with LOCE or the ADAMS networks even though information was manually transferred between the systems. Network applications were not interoperable. The ADAMS movement control system and JOPES required a manual interface for exchanging information. The NATO and national intelligence systems were not directly connected and had to use manual exchanges to share information from one system to the other. For example, a correlation center was established at the JAC to populate the LOCE server with information from the United States, United Kingdom, France, and other national sources for distribution to IFOR elements. The STU-IIB, the NATO-approved secure voice equipment, was used extensively by IFOR, but a large number of the U.S. forces deployed to Bosnia with STU-IIIs that were not interoperable with the STU-IIB.

The U.S. intelligence processing system used at Echelons Above Corps (EAC) did not “talk” to the Echelons Corps and Below (ECB) systems such as JDISS. To fix the problem, an EAC

processing system such as JDISS had to be deployed to ECB intelligence centers. The lack of connectivity between EAC and ECB systems was caused by security restrictions on certain intelligence information being processed with other kinds of intelligence information. Different levels of classifications and security accesses accompanied this information. Different kinds of intelligence data were compartmentalized and communicated to higher and lower users within their own stove-piped arrangements. This was a root cause of the proliferation of intelligence processing systems.

Liaison became a very important interoperability issue in IFOR. With 34 participating nations, it is easy to see that not all assigned personnel understood or spoke English, although English was the language of the operation. Therefore, liaison personnel were used to bridge the communications gap and facilitate coordination between organization elements. There were liaison cells in the CJCCC for representatives from the MNDs, ARRC, NACOSA, DISA, EUCOM, USAREUR, and USAFE. The intelligence and Special Operations Forces communities used and provided liaison personnel. The MNDs used liaisons with the forces assigned to them, such as the Russian brigade in MND(N), and between themselves and with IFOR and the ARRC.

Although interoperability is continuing to improve, there is still a long way to go to achieve seamless integration of NATO, national strategic and tactical, and commercially provided CIS systems and services.

NATO CIS Contingency Assets and Acquisition

The shortfalls in the existing NATO CIS infrastructure were known at the start of IFOR. The mechanism for overcoming the shortfalls was already in place and identified within the NATO CIS Contingency Assets Pool (NCCAP) concept. The NCCAP concept combined the Allied Command Europe (ACE) CIS Contingency Assets Pool, mainly for land and air users, with the Maritime CIS

Contingency Assets Pool, which was for naval users. Under the NCCAP concept, a pool of deployable CIS equipment would be procured and maintained for NATO and made available for contingency operations and exercises. Some equipment (new single- and multi-link TSGTs) was already being procured, but not delivered, when the operation started. In NATO, advance procurements are not generally planned for equipment with short manufacturing time scales in order to take full advantage of the latest commercial hardware and software technology. Contingency funding authorization is given to support rapid implementation on a need basis. The pool is enhanced where necessary with deployable assets made available by the nations. The provision of CIS assets for Bosnia was consistent with the NCCAP concept. Although the NCCAP concept was in place, there was initially very little equipment actually on hand. Furthermore, the detailed operational procedures for its use had not been finalized. Heavy reliance was therefore placed on the framework nations' national CIS assets, particularly those provided by the United States, and on leased PTT/VSAT/IDNX connectivity provided by NATO. In addition, greater reliance had to be placed on emergency procurement.

Generally speaking, NATO committees proved to be responsive and reacted flexibly to emergency CIS requests. There were some instances where the NATO CIS procurements failed to arrive in time to meet the operational commanders' requirements. In these cases, the NATO procurement cycle was too slow or unable to meet emergency requirements. In some cases, the contractor was unable to deliver and this resulted in failure to meet the operational requirement. One particular case in point was the failure of FLEXLINK to provide commercial SATCOM services. Due to the financial collapse of the FLEXLINK Company, it became necessary to find another vendor to provide the service. The Interstate Electronics Corporation (IEC) ultimately took over the contract from FLEXLINK and was responsible for providing an extension of NATO's E1/IDNX network into Bosnia to connect key IFOR locations via commercial SATCOM exclusive of the host nation's infrastructure. Because of the need to re-let the contract, the operational

capability was implemented late. The implementation delay severely limited IFOR's ability to satisfy the bandwidth requirement for the operation. In May 1996, the IEC network became fully operational and provided the key services and necessary bandwidth down to the IFOR, ARRC, and MND levels.

International competitive bidding was only really imposed by the NATO Infrastructure Committee for the acquisition of the TACSAT terminals. Almost all other procurements were through Basic Ordering Agreements set up by the NC3A and AFSOUTH with a range of suppliers. In some cases, market surveys were employed before deciding on the most cost-effective provider. The time pressure imposed by the operational situation mandated a pragmatic balance between cost and delivery time in all cases.

For the IFOR operation, NATO authorized over \$100 million dollars for CIS expenditures. More than \$60 million was spent on communications alone, the major items being UHF/SHF tactical satellite terminals, UN VSAT service leases, commercial E1 leases, the IEC commercial SATCOM/IDNX network, and the UHF SATCOM channel lease from the United States.

C4ISR Performance

The pervasive use of COTS information products and services propelled NATO and IFOR into the Information Age and a new way of doing business. There was extensive use of e-mail and a reduced reliance on formal messaging systems. The formal message traffic (the NATO TARE message network) by volume (megabytes per day) was less than 10 percent of the total IFOR daily data network traffic. PowerPoint briefings were used to inform and were readily distributed over the data networks. The data networks were also used for collaborative planning and distribution of wide-band information such as images, although at times this was slow due to the limited bandwidth of the interconnecting links (64kb/s or less).

The bandwidth limitations were driven by NATO constraints on minimum cost solutions and unavailability of NATO-approved crypto equipment to run the links at higher rates.

Secure VTC was used extensively by IFOR and the ARRC for collaboration and coordination and as time went on, it became the medium of choice for conducting business. The VTCs were also used by subordinate IFOR elements to conduct day-to-day business. The VTC systems performed reasonably well when operating, but they were subject to outages due to SATCOM link bit error rates, crypto synchronization problems, and PICTURETEL software lock-outs. Numerous maintenance problems occurred and when they did, there was a lot of high-level pressure put on the maintenance staff to get them repaired quickly. Such pressure may have led to addressing the symptom and not necessarily the problem in many instances.

During the early deployment phases, different telephone handsets were present in command center locations. In some cases, it was reported that as many as seven different handsets were provided due to the multiple NATO, UN, and national voice networks. Although the various networks were interfaced and it was possible to progressively navigate through them, the networks were not integrated as a system with common numbering, routing, and signaling plans and directory services. Because of manpower shortages, time constraints, and constant change, telephone book and number management was a problem. There were multiple phone books at any one time (e.g., at least three phone books existed for the U.S. network: AFSOUTH, USAREUR FWD, and Task Force Eagle) and production coordination was sporadic. Phone book and dialing instruction distribution was a problem as well. As a result, calling from one network to another required some knowledge of the operational characteristics of each of the tactical systems, how they were interconnected, and the correct dialing sequence to progress from one network to the other. People frequently carried a dialing plan on a 3"x5" card in their pockets when traveling in Bosnia or found such a plan posted near the telephones.

The military tactical voice networks also were not very user friendly. The variety of multinational users at the theater and strategic levels found them difficult to use. The end-to-end network performance was also marginal, so users tended to default to using the UN VSAT network to do business since its operation was similar to a commercial telephone system. Unlike the military networks that were end-to-end security protected, the UN VSAT was not. One could use STU-IIBs on the UN VSAT but they were in short supply. Over time, a number of the tactical phones were removed, but there were still several different types of telephone handsets in the command centers.

The leased service offered by the UN to IFOR did not meet IFOR expectations. The UN VSAT network could not handle the load IFOR put on it. There were problems in getting priority responses from the UN to provide service for new IFOR subscribers/users and to take maintenance actions to resolve performance problems. There was no single UN focal point for actions in response to IFOR requests for service—the CJCCC element in Zagreb established a UN liaison position to facilitate working with the UN.

The new data network capabilities provided IFOR the opportunity to share information more efficiently and quickly (nearly simultaneously) at all levels of the command structure. This was a vast improvement over the previous procedures requiring the corroboration of data successively reported through each level in the chain of command. It was also possible to exchange information that bypassed (“skip echelon”) intervening levels of the command structure. The ability to electronically bypass levels of command to obtain information firsthand was occasionally used in the interest of expediency and providing information up the chain of command, but sometimes at the expense of leaving others in the dark. Towards the end of the IFOR operation, the problem was not one of a lack of information but rather one of finding the useful details among the wealth of information available.

The CRONOS LAN and WAN management was evolving with the operation and had been the source of some problems during the early phases of the IFOR operation because of the need for

SOPs and trained network management and administration staff. There was also a conflict in the management responsibilities of the CJCCC and NACOSA caused by the SHAPE/AFSOUTH C2 differences. The NC3A, the Hague, maintained a CRONOS help desk that was connected to the network and was available to support requests for assistance from the theater.

Managing all of the information available to the commander and his staff was a difficult problem. Users lacked adequate tools to search for available information. Likewise, there were inadequate tools for managing information collection, storage, and sharing. This was particularly true early in the operation in the areas of coordinating, integrating, and fusing intelligence, surveillance, and reconnaissance capabilities and making this information available to the user. A mixture of NATO and national prototype and operational systems were used in an attempt to fuse various land, sea, and air pictures into a common tactical picture. The maritime and land pictures provided to the tactical commanders were of good quality. The air picture in the CAOC, made up from a variety of sources, was of particularly high quality. However, there was no overall integrated maritime/air/land picture provided to the commanders.

There were other sources of information such as the Internet and local and international media that needed to be incorporated into the IFOR information base. In terms of sharing classified information, security releasability was also an issue that needed to be addressed to ensure that information was put in the hands of those that needed it in a timely way without revealing sources and methods, but stringently protecting highly sensitive information.

Although extensive use was made of e-mail, VTC, and data network services, voice communications still played a major role in conducting the IFOR operation. This was true in spite of a grade of service that, at times, could exceed a 20-percent probability of blocking for call attempts during the early phases of the IFOR operation. The end-to-end voice quality was marginal especially if the call had to be routed through several different tactical switched networks. The UN VSAT network performance proved to be marginal, espe-

cially for calls out of the area of operation. Voice network performance improved towards the end of the IFOR phase of the operation, especially with the implementation of the IPN.

IFOR estimated that about 91 percent of the network capacity was dedicated to voice services, 6 percent for VTC, and 3 percent for data services. On the other hand, 5th Signal Command estimated that about 50 percent of the U.S. network was dedicated to voice services and 25 percent each for VTC and data services. If the U.S. intelligence network capacity were added to the U.S. statistics, data would certainly exceed 75 percent of the overall network capacity.

There were high hopes for extended use of cellular services in Bosnia, but effective coverage from the commercial networks could only be achieved in some parts of Croatia. A number of offers were made by cellular vendors to implement cellular services in Bosnia but were met with political opposition by the FWF PTTs. There was a proposal to operate from IFOR compounds. This had the added advantage of physical security. ARRC-Main was opposed to taking on such a responsibility because of the additional support and manpower implications. There was also a question regarding the effectiveness of the coverage of such a system. By the end of the IFOR operation, the PTT implemented a limited coverage cellular capability in Sarajevo.

Problems with viruses were experienced not only with the CRONOS and IARRCIS but also with most computers brought into the theater. The Center for Army Lessons Learned reported that within the first 60 days of operation nearly every Army computer brought into theater had been infected. Infected diskettes brought into the command centers and the swapping of diskettes (including infected ones) between the unclassified and classified systems were major sources of the problem and its proliferation. There was also a lack of personal discipline and standard operating procedures. Virus detection and correction measures were put in place along with a user information awareness campaign. Laptop computers were placed at the entrance to command centers with virus scan programs and a notice posted that all diskettes had to be

scanned before being taken into the command center. Use of games on the command center computers—another source of viruses—was forbidden. C-Support in Zagreb used a diskette color-coding scheme to prevent confusion regarding classified versus unclassified. They also developed a set of operating instructions. Neither of the C-Support approaches were implemented IFOR-wide.

While most of the detected viruses were relatively benign, their ubiquitous presence underscored the vulnerability of the computers and data networks to systematic hostile attack. There was a need for improved intrusion detection capabilities for the data networks. A related issue was the lack of adequate data network configuration management and control. The CJCCC needed better configuration management tools and procedures. Security was an ongoing responsibility for which improvements were made over the duration of the operation.

Dust and dirt caused problems with disk drives and servers, creating the requirement for protective measures such as covering up computers when not in use and vacuuming the work areas and the computers themselves more frequently. Commercial power failures and fluctuations caused major CIS outages for those sites that did not have a UPS backup capability and power-line surge protectors. Sometimes the power failures were a result of planned outages. For example, the commander of the Croatia compound in Zagreb, where the UN and the IFOR C-Support were located, performed an unannounced base power outage. The interruption shut down the UN and C-Support CIS capabilities. Needless to say, swift action was taken to acquire a UPS capability to support the UN and IFOR C-Support CIS systems. Power was a serious problem that required high-level attention to get the necessary UPS capabilities deployed.

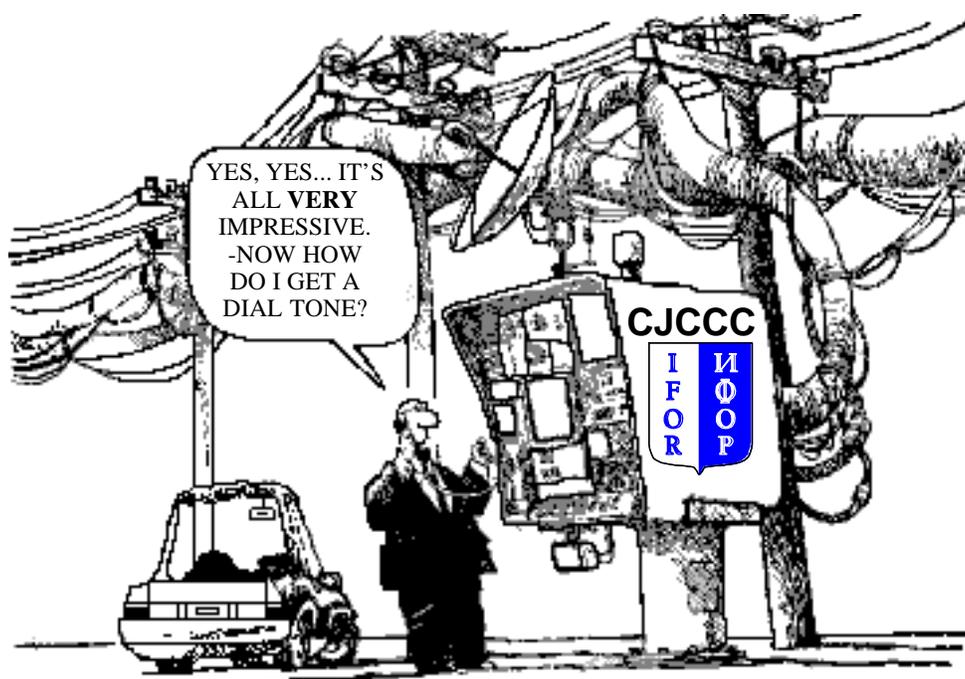
The extension of secure services to non-NATO coalition partners was also an issue that had to be dealt with by IFOR. Security policy modifications were required to accommodate the release of classified information and liaison teams were provided to non-NATO units assigned to IFOR, such as the U.S. INTEL team with the Russian brigade and the U.S.-provided narrow-band voice ter-

minals for the PfP nations supporting the operation. IFOR CJ6 suggested that NATO might consider the use of commercially available security products to facilitate secure communications with non-NATO troop contributing nations in support of future peace operation security needs.

Network and system management of IFOR's communications and information network proved to be a major challenge (figure 11-20). An IFOR organization structure had to be created, agreed upon, and staffed quickly. The U.S Joint Pub 6-05 provided the basis for the establishment of the CJCCC to manage IFOR's network. System tools had to be acquired to monitor and manage the networks. There were multiple NATO and national players, such as SHAPE's NATO CIS Operating and Support Agency (NACOSA), the AFSOUTH CISD, the IFOR CJ6, the CJCCC, the ARRC G6, the MND G6s, and the national J6s. The roles, relationships, and activities of these organizations needed to be established and coordinated. Furthermore, overlaps in organizational responsibilities needed to be worked out since the distinction between strategic, theater, and tactical became blurred. SHAPE and AFSOUTH OPLANs and C2 differences did not help the staff attempts to resolve these overlaps. NATO communications and ADP were managed separately, and this needed to be accommodated by the CJCCC. Over time, these issues were resolved and the CIS system provided reasonable services. However, the CIS system for the most part was never heavily stressed during the IFOR operation. Therefore, the performance of the networks and the supporting management organization were never tested under more hostile or stressful conditions.

The management of the U.S. C4ISR networks was a challenge as well. C4 and ISR were managed separately as well as communications and ADP. The ISR systems were managed by different organization elements. The blurring of the strategic, theater, and tactical boundaries was a problem for the United States too. There was no doctrine defining the demarcation point between U.S. strategic, theater, and tactical systems. This had to be dealt with at the outset of the operation since strategic- and theater-level capa-

Figure 11-20. CJCCC



bilities were deployed into the tactical area, resulting in overlapping responsibilities for the management organizations and no clear definition of who had end-to-end assured service responsibility.

The use of e-mail, PowerPoint briefings, PCs, and video teleconferencing not only dominated the mode of operation at division and above but was also beginning to penetrate below division as well. Tactical systems, however, still dominated at division and below. The maneuver units relied on tactical line-of-site communications. The use of non-tactical communications was at the commander's discretion. Commercial systems such as INMARSAT with STU-III and STU-IIB were used. There was also a desire for broader access to commercial services such as cellular and commercial SATCOM. Desktop and laptop computers were based throughout the tactical area. Early on these were 286 and 386 machines but it soon became necessary to deploy 486 and Pentium machines to handle the volume of data and accommodate the RAM needs of storage-hungry programs such as MS Office. Rotation of troops also added some unintended consequences. The arriving units would at times bring with them the latest version of software applications, contributing to some interoperability problems when trying to share products from different versions of software applications.

The IFOR information revolution largely stopped at the division headquarters level in Bosnia. In some cases such as MND(N) and the U.S. forces in Croatia and Hungary, higher bandwidth services were extended to the battalion level. Every U.S. base camp had telephone service and secure and non-secure data and e-mail capabilities. However, the communications and information system support to the IFOR warfighters changed very little, and the warfighters continued to operate much as they had in the past. Operations were conducted using acetate-covered 1:50,000 maps (see picture), outmoded tactical equipment, and sensor or reconnaissance systems organic to ground units.

The use of TCP/IP-based networks is proliferating for the unclassified military and commercial networks (the NIPRNET and Internet) and for the classified military networks (the NATO CRONOS and LOCE and the U.S. SIPRNET and INTELINK).

Furthermore, the data networks are increasingly being relied upon by the military for supporting operational C2 and intelligence traffic. Although the IFOR and national networks performed reasonably well overall, there were problems with congestion and assured service when equipment failures and traffic-loading situations were encountered at major nodes or operations centers. Under the stress of real hostilities, where one or more operations centers or nodes are attacked or destroyed or extreme traffic overloads are encountered, the networks could gridlock or fail, catastrophically denying service to essential C2 users. The redundancy, robustness, and resiliency of the IFOR network design and supporting network and system management structure were never really tested operationally. The IFOR network and system management capabilities and structure to support C2 traffic under extreme hostile conditions were not part of the design criteria, nor was such a capability implemented. It was tough enough to create a capability to manage the integrated peace operations network derived from NATO and national systems. Alternative (low bandwidth) fall-back systems (TARE/AUTODIN and C2 voice networks) were not implemented as a reconstitution or continuity of service capability even with the danger of open hostility, as was the possibility with the RS faction. The VTC network had similar weaknesses and was a “bandwidth hog” as well. If one or more nodes or operations centers were attacked, the bandwidth to support or reconstitute VTC service would most likely not have been available. Voice conference systems such as that provided for the ARRC by PTARMIGAN could have been used as a limited conferencing backup capability. There were a couple of satellite failures that highlighted the vulnerability of the IFOR network. Actions were taken to build in some additional redundancy and establish contingency plans for reconstitution of critical C2 links.

Technology Insertion

Although the deployed high-technology systems generally supported the headquarters far more effectively than they supported the soldier on the ground, there were, of course, exceptions. Many innovative uses were made of the U.S. military's array of advanced technologies (mainly in the area of ISR) to more effectively support the headquarters and the soldier on the ground. In fact, Bosnia (mainly MND(N) and the CAOC) became a model for the U.S. doctrine known as "Information Dominance" and technology test beds.

U.S. commanders, in particular, reported that a virtual flood of new technologies followed their deployment to Bosnia. These technologies were generally inserted incompletely and imperfectly. Many of the new systems and technologies were deployed without doctrinal support, concepts of operations and training, and logistic support packages. As a consequence, they could not be fully employed. Moreover, because they had not been through full and systematic development and testing, trained military operators were not available. Initial operations and maintenance had to be provided by contractors or the government development team personnel. Even so, these new technologies reportedly still made excessive demands on military operator personnel who had to find the time to train, learn to maintain the equipment, and develop concepts of operation. In many cases, this meant that new systems were underutilized because their full functionality and potential were not understood.

The advanced technology capabilities deployed in Bosnia were essentially stove-pipe systems and capabilities that were overlaid on the operational networks. Hence, one of the major challenges the United States and IFOR faced was the integration of these capabilities and systems into the operation and then being able to exploit them to the maximum extent possible.

Air Force and Army initiatives were directed at trying to put discipline into the technology insertion process and facilitate the deployment of advanced technologies to the theater. In January 1996, the Air Force Electronic Systems Center at Hanscom AFB

established a *Joint Endeavor* Laboratory, now the C2 Unified Battlespace Environment (CUBE). The laboratory replicated the C3I functionality of the CAOC in Vicenza, Italy, and was used for rapid problem solving and system integration testing of new capabilities before operational deployment to the theater. A 24-hour hotline was established to support technical assistance requests from the field. ESC also deployed technical assistance teams to the CAOC to help resolve on-site integration and configuration management problems. In December 1995, the Army Materiel Command established a Bosnia Technology Integration Cell (BTIC) to serve as a clearinghouse for critical technologies and the “nerve center” for tracking and integrating the technology community’s efforts to support U.S. soldiers in Bosnia. The BTIC focused its efforts on prospecting for systems that would provide American forces with a technological advantage for operations such as anti-mine, anti-sniper, communications, and surveillance.

NATO too established an advanced technology laboratory to facilitate the introduction of new capabilities and functionality into the NATO CIS systems such as CRONOS and ADAMS. The laboratory facility at the NATO C3 Agency, The Hague (NC3A) replicated the NATO CIS systems deployed in support of IFOR and was used for rapid prototyping and system integration testing. A CRONOS Help Desk was established and manned 24 hours a day to provide on-line technical assistance and answer requests for help from the field. The NC3A also deployed technical assistance teams to help resolve problems in the field.

There were concerns expressed by other nations such as the United Kingdom and France that they could not keep up with the pace of U.S. technology and that this could have significant interoperability and operational implications for future coalition operations. A clear lesson from *Operation Joint Endeavor* was that advanced technologies are of military value and are suitable for deployment only when they are accompanied by coherent doctrine, organizational support, equipment, people, and the ability to effectively integrate them into the operational environment. It is also important to note that not all coalition partners can afford the latest

C3I technologies. Furthermore, some high-tech nations such as the United States may not be willing to share their latest capabilities with all members of a coalition of the willing, and not all coalition members use the technologies of these nations either. These are the realities of coalition operations and the way of the future. The push for the use of advanced technology will and should always be there and therefore needs to be more effectively accommodated.

Finally, as long as systems development and procurement lead times for military systems remain significantly longer than the rate of technological change in communications and automation, commercial products will be the only practical means of delivering state-of-the-art capabilities. So the challenges of augmenting military systems with commercial systems must be met and overcome.

Some Common Threads for Lessons Learned

A lot has been learned from *Operation Joint Endeavor* that can be applied to future peace operations. Some have particular significance for future NATO operations and the realization of the NATO CJTF and NCCAP concepts. Others can be applied to coalition peace operations in general. Some experiences are simply the realities of complex coalition operations. Others are experiences re-visited, and still others are lessons yet to be learned or in the process of being learned as a result of the IFOR experience. In the latter case, lessons learned are used in the context of the Center for Army Lessons Learned definition, “a lesson is learned when behavior changes.” The following is an attempt to characterize some of the *Joint Endeavor* C4ISR experiences in these three categories. There is no priority of importance implied by the sequence in which they are presented.

Realities of Coalition Operations

- Participants must integrate what they get, not necessarily what they need.
- Forces should expect stove-piped system implementation with associated interoperability and security disconnects.
- The planning environment will be dynamic and confusing.
- The theater-level PTT infrastructure will be inadequate to support operational needs.
- Coalition partners will have uneven capabilities and experience.
- Command arrangements and force structures will be politically driven and implementation will be behind the power curve.
- Participants should expect to learn “on the job.”
- Participants must keep it simple.
- Agility, adaptability, and innovation will be the norm.

Experiences Revisited

- U.S. military strategic and tactical C4ISR systems and services once again provided critical communications and information systems and services in support of a major coalition operation.
- The division of strategic, theater, and tactical C4ISR systems has become less distinct and planning and operational staffs and commanders will have to learn how to deal effectively with a pervasive communications and information system environment.

- Centralized network control was essential for the success of the communications and information system operations. Lack of this for IFOR early on in the operation resulted from SHAPE and AFSOUTH C2 differences.
- Standing contract arrangements for acquiring products and services in support of contingency operations were needed.
- All requests for communications and information services were urgent during the initial build-up phase. An adjudicating authority was needed to sort out priorities and validate coalition requirements.
- The size of the communications pipes was not sufficient to meet the demands of the operations (experienced at all levels—strategic, theater, and tactical).
- Independent and separately managed communications systems supported the C4 and ISR systems. There was a need to be able to more effectively share these capabilities in the operational environment.
- The operation could not have been successful without the extensive use of military satellite capability that only the United States, United Kingdom, and France forces could provide.
- Interoperability continues to be a challenge. Even though progress is being made, there is still a long way to go to achieve seamless operation of the coalition communications and information systems.
- Reliance on commercial products and services needs to be more effectively incorporated into the CIS architectures, planning, procurement, contracting, O&M, logistics support, and training.

- Training for commercial products and services has two aspects to be considered: training the military on commercial systems and training the contractor to work in a military environment.
- Contractor support and related O&M and logistic support arrangements for military use of commercial equipment and services still need to be understood in terms of operational implications and the ability to ensure continuity of service in a hostile environment.
- Commercialization of military systems supports an exit strategy aimed at the early withdrawal of military tactical systems. However, the commercialization strategy must take into account the disposition of the entity you plan to lease from, i.e., vendors must be positioned to provide the support, and there is a FWF PTT assured service risk that needs to be accommodated. A military overlay needs to be maintained to provide assured C2 connectivity.
- Dust, dirt, and commercial power failures continue to affect operations.

Lessons Yet to Be Learned or Being Learned

- The U.S. military played a key leadership role in the provision of IFOR CIS services and the integration of disparate NATO and national systems to realize and operate the largest military-civil communications and information system ever built to support a major peace operation.
- The prominent role of U.S. Signal officers in key positions in NATO, SHAPE, AFSOUTH, DISA, USAREUR/5th Signal Command, USAFE, and other organizations was an important unifying factor. Many IFOR problems associated with ambigu-

ous roles, incomplete doctrine, and technical interoperability were successfully resolved through close coordination among these U.S. officers.

- NATO organizations such as AFSOUTH CISD, SHAPE CISD, NACOSA, ARRC G6, and NC3A, the Hague, rose to the occasion and provided untiring support to IFOR CIS installation, operation, and problem-solving activities.
- The United Kingdom was a key contributor to IFOR CIS systems, services, and problem resolution with important players in NATO, SHAPE, NACOSA, AFSOUTH, the ARRC, and UK Signal units.
- E-mail is largely replacing the formal messaging handling systems such as the U.S. AUTODIN and NATO TARE.
- VTC is becoming the C2 system of choice, especially for the U.S. Army.
- Information management and management of the use of information require careful consideration as NATO and the nations move into the global Information Age.
- Given the heavy reliance on the use of data networks and VTC to support operational C2 and intelligence requirements, consideration needs to be given to designing and implementing more robust operational networks in support of real-world operations; improving network and system management systems and structure so that continuity of service to essential C2 users can be ensured under stress conditions; providing low-bandwidth backup capabilities for essential C2 users for contingency use; and improving the management of access to and use of information network resources by non-essential C2 users under stress conditions.

- Despite the myriad of voice systems present, telephone service supporting the IFOR Joint Operations Center was still inadequate. Multilevel precedence and preemption down to the soldier in the field may be the only way to ensure that a common user system can be used for C2, especially in a damaged network.
- Network and system administrators are in high demand and there is a lack of trained military personnel to meet this demand. System-level troubleshooters for complex information systems are also lacking.
- Access to commercial Internet service and its use are required to support C2, mission support, and intelligence operations.
- Coalition operations dictate the use of collateral vice SCI classified material and facilities for the promulgation and reporting of intelligence information. At the tactical level, personnel are generally not cleared for SCI, nor is the security infrastructure available to support it.
- Proliferation of different information systems to support C2, mission support, and intelligence introduces unnecessary duplication and inefficient use of scarce bandwidth. Furthermore, no one individual in a command center was cross-trained (nor should they necessarily be expected to be) on all systems to either use them or maintain them.
- The CIS requirements of the PIO, CIMIC, PSYOP, CI/HUMINT, and other special activities such as NGO, PVO, and IO organization interfaces and support need to be made known up front so that adequate CIS services can be planned for and provided.
- There was no agreed baseline of NATO CIS services and information requirements for out-of-area operations.

- Inability to conduct proper reconnaissance for political reasons and last-minute changes resulted in deployment with incomplete planning and understanding of requirements.
- There needs to be an interoperable digital interface between national military tactical systems and between strategic civil and military systems and military tactical systems.
- Reach-back is an effective means for connecting deployed forces to the broader services of the strategic CIS infrastructure. NATO did not have such a capability per se (it only had a simple reach back to SHAPE for extension of headquarters services). The installed strategic-tactical digital network (STDN) gateway for the U.S. DII was not sufficiently capable to support *Joint Endeavor* needs. As a result, U.S. tactical switching and transmission equipment had to be employed at the strategic level (in Germany) to accommodate reach-back services and interfaces with the DII.
- Intelligence activities in support of peace operations require much more flexibility in databasing. More flexible and efficient information discovery and retrieval tools are needed.
- The technology insertion process is incomplete and imperfect and requires a more coherent and disciplined process to ensure that military value is achieved. Advanced technologies are of military value and suitable for deployment only when they are accompanied by coherent doctrine, organizational support, equipment, people, and the ability to effectively integrate them into the operational environment.
- Not all coalition partners can afford the latest and planned U.S. C4ISR systems. The United States may not be willing to share its latest C4ISR systems with all elements of “coalitions of the willing.” Furthermore, not all coalition partners use U.S. systems.

- The Information Age has arrived for NATO but largely stops at the division level. The Information Revolution needs to be extended to lower levels of the command structure to effectively support the troops who are actually executing the mission. The troops also need to be trained in how to prevent “information overload.”
- Advanced information discovery tools need to be developed and provided in order to improve the ability of the commander and his staff to find the useful details among the wealth of information available.
- NATO needs the ability to more effectively deploy forward communications and information systems in support of peace operations. The roles and relationships of the network and systems management organization elements need to be clearly defined and made a part of the operations order.
- The artificial separation of communications and data processing responsibilities needs to be removed in the Information Age.
- More extensive sharing of information and collaboration has become the norm for doing business in a coalition operation.
- NATO needs to establish COMSEC accounts to support multinational operations down to the unit level. COMSEC/INFOSEC for non-NATO partners also needs to be addressed.
- NATO’s peacetime procurement process is too complex and slow to meet the demands of a live peace operation. Nations must be able to have their say but care must also be given to national preferences that can complicate operational priorities. The situation did improve dramatically over the course of the IFOR operation.

- Tight CIS configuration management and control and a workable integrated logistics support plan are essential to support contingency operations.
- Major operational decisions (e.g., SFOR replacement of IFOR) should include active NATO CIS community involvement before the timelines on the move are finalized. IFOR/SFOR experience highlighted problems in this area.
- Software viruses caused problems for IFOR operations and appropriate detection and protection mechanisms need to be factored into the planning for information system enhancements. Also, there needs to be NATO policy guidance and enforcement.
- NATO and the nations need to carefully examine the defensive information warfare needs of future information systems and incorporate the necessary defensive capabilities (e.g., intrusion detection and protection) to reduce their vulnerabilities to potential hostile actions.
- Exercises and training demonstrated the value of setting up the expected C4I configurations in advance of the deployment to sort out integration and interoperability problems. The exercises also served to train and do some team building for those personnel who would deploy.
- NATO needs a proper organization for planning, implementing, and managing the communications and information networks required for out-of-area peace operations. The NATO CJTF concept and the IFOR CJCCC are building blocks for developing an appropriate capability. NACOSA is an established NATO organization responsible for planning, implementing, and managing the strategic CIS networks.

- Liaisons proved to be an effective means for facilitating coordination, collaboration, and cooperation among the many different NATO and national organizations participating in the management of the IFOR CIS network.
- A Frequency Management capability needs to be provided as part of the network management operation.
- Enhanced system and network management tools need to be made a part of an improved capability for NATO CIS network management.

In summary, the experiences from Bosnia reinforced the importance of information dominance. Getting the right information to the right person at the right time has significantly improved but has not yet reached or impacted the soldier on the ground to the same extent that it has changed the way business is done at higher headquarters. C4ISR interoperability continues to be a challenge, not only among the military coalition systems but also with commercial products and leased services and the systems used by the IOs, NGOs, and PVOs. Operational use of advanced information technologies and commercial products and services has become a reality and needs to be factored into the planning and training for peace operations. Innovative training and exercises and adherence to international standards are means to improving this situation as the world moves into the global Information Age.

One should not forget, however, that potential adversaries of the NATO alliance and the United States, in particular, will not be so foolish as to neglect glaring weaknesses in the C4I networks implemented in support of the IFOR operation. Active countermeasures against these networks may be the case in future operations. Doctrine and tactics based upon an assumed information dominance and freedom to communicate may not be sufficient the next time around, even for peacekeeping operations.

In conclusion, agility and accommodation continue to be keys to success, as well as some plain old good luck. Let us not forget, however, that the success of the IFOR C4I and national C4ISR network implementation and operation was in the final analysis because of the professionalism, dedication, and ingenuity of the men and women who were there and those who supported them. Good people make it happen.

XII. NDU/CCRP Bosnia Study

Larry K. Wentz

Background

Recognizing that the deployment and operation of C4ISR capabilities in support of the complex coalition peace operation in Bosnia provided a unique opportunity for learning, Mr. Emmett Paige, Jr., ASD/C3I, tasked the CCRP at NDU on February 15, 1996 to simultaneously collect experiences and lessons learned and to perform an analysis of the effectiveness of command arrangements and supporting C4ISR.

CCRP's charge was broad, covering both the effectiveness of command arrangements and the effectiveness of supporting C4ISR. Hence, the study addressed all of the classic issues of C4ISR, including structures, functions, capacities, doctrine, and training. Furthermore, CCRP was tasked to pull together the related ongoing C4ISR community activities and build a coherent C4ISR story, including lessons learned. The study charter was introduced to the Joint Staff through the J-6 (Director, Command, Control, Communications and Computer Systems), and was subsequently coordinated with the J-3 (through the Vice Director for Operations). Both endorsed the effort, and the decision was made that the J-3 would be the official Joint Staff point of contact for the effort.

The CCRP Bosnia study charter listed three major tasking areas: (1) document the build up and evolution of C4I systems and capabilities provided to all echelons; (2) document command arrangements (both formal and informal) as they evolve and the rationales for changes; and (3) assess the effectiveness of command arrangements and C4I systems and the adjustments made to them over time. Command arrangements of interest specifically included those (a) associated with joint operations, (b) within and among U.S. Government (USG) organizations, (c) among military organizations (NATO, Russians, and others), (d) between the United States and NGOs and PVOs, and (e) with local governments and organizations. In addition, CCRP was tasked to unify the C4ISR community activities and put together a coherent lessons learned story.

CCRP was sensitized to the need to be unobtrusive and to minimize demands on military organizations in the theater of operations. In-theater travel and visits, while necessary for some aspects of the study, were limited to those required to support a quality product. Research activities were initiated in February 1996, and it was expected that they would continue for at least 6 months after the exit of major U.S. forces from Bosnia. With the transition of IFOR to SFOR on 20 December 1996, the NDU effort was adjusted to focus on putting the IFOR story together as a first priority. The collection of SFOR experiences and lessons learned was to continue but at a much lower level of effort.

The NDU study was designed to produce a variety of products, and a final report will summarize all of the findings on C4ISR Lessons Learned. Study results have been briefed at C4ISR community symposia and workshops such as AFCEA, MILCOM, the NDU INSS-sponsored NATO symposium, and the Pearson Canadian International Peacekeeping Centre workshop on peacekeeping and conflict resolution. Findings were also presented at the Swedish Naval Warfare Centre-sponsored Partnership-for-Peace lessons

learned workshop, the NATO Panel 7 workshop on IFOR data collection and analysis, and the CCRP-sponsored International C2 Research symposium.

Using CCRP's approach of crafting balanced Mission Capability Packages (figure 12-1) to deal with emerging issues and opportunities, key findings will be provided to doctrine developers in the joint community and the services. In addition, the results will be used to develop professional military education (PME) materials for use at all levels of professional schooling. Finally, NDU/CCRP will select the most important topics and findings for publication as articles in *Joint Forces Quarterly* and other visible periodicals as well as books through the NDU Press.

Study Team

CCRP brought together a multidisciplined, diverse group of analysts and researchers to carry out the major tasking areas of the Bosnia study charter (figure 12-2). A core team was established under the leadership of the Director of the CCRP and consisted of participants from NDU/CCRP, Evidence Based Research Inc (EBR), C4I Integration Support Activity (CISA), MITRE, and Decision-Science Applications Inc. The core team was augmented, as required, with subject area experts from organizations such as DISA, JITC, SOCOM, J2/DIA, and J6Z. Staff from the Center for Naval Analysis (CNA) and Institute for Defense Analysis (IDA) also provided advice and inputs to the effort.

Approach

Operation Joint Endeavor was well underway before the NDU study effort was initiated and it was quickly determined that a number of other organizations had initiated efforts that would provide important information that the NDU effort did not need to duplicate. Therefore, CCRP made identifying all related efforts its

Figure 12-1. Mission Capability Package

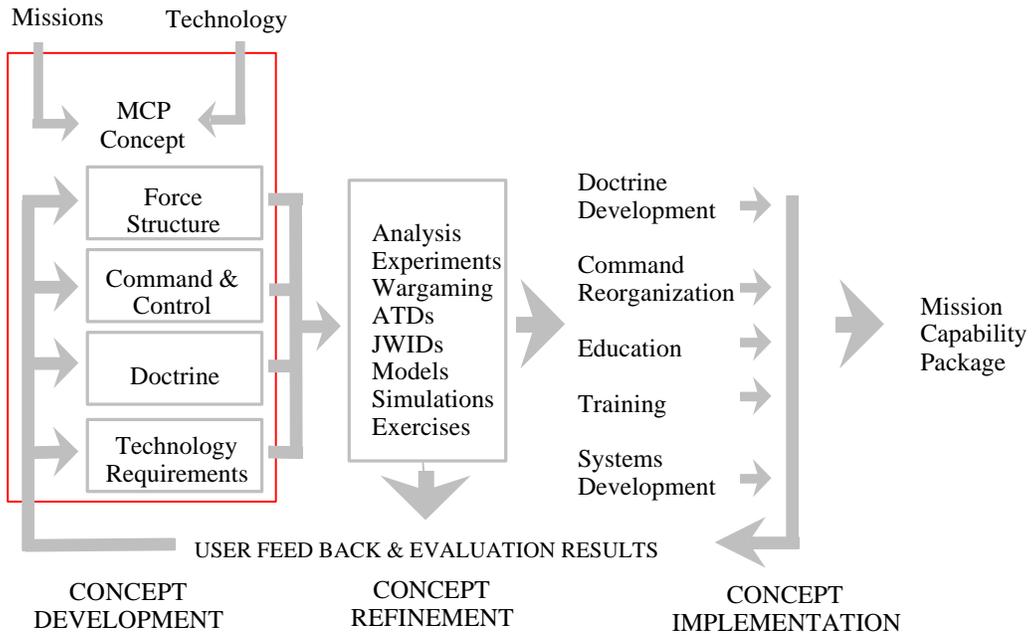
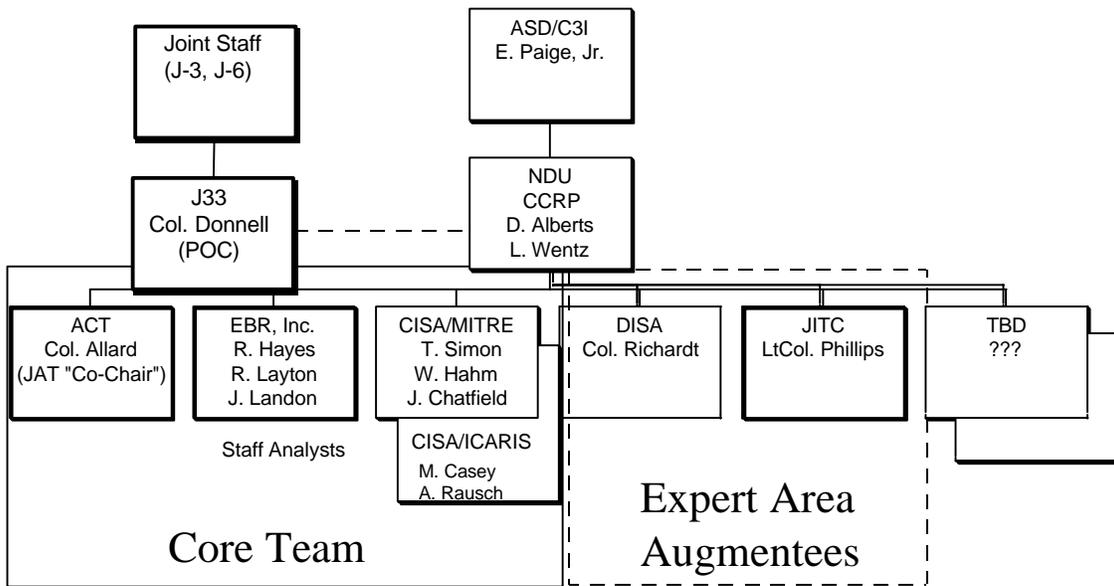


Figure 12-2. NDU/CCRP Bosnia C4ISR Team



first priority. These included lessons learned activities, research efforts, and assessments of C4ISR performance in Bosnia. The roundup of all relevant efforts was a key element of CCRP's four part, highly leveraged plan for accomplishing the mission of assessing C4ISR effectiveness and collecting lessons learned.

CCRP achieved its goal of a highly leveraged effort based upon attention to four principles: coordination, collaboration, integration, and focused research. **Coordination** allowed CCRP to avoid duplication, minimize demands on the commands in the field, and maximize the return on its own focused data collection efforts. **Collaboration** permitted the effective use of access and expertise in other organizations while also allowing CCRP's expertise to be used efficiently and effectively. **Integration** of all the work performed, whether by CCRP personnel, those working on their behalf, or those operating under very different charters, allowed CCRP to add value to the work of others and to provide a unique and important contribution. This included collecting products from all sources; comparing and contrasting them to test for consistency of findings across time, space, levels of command, and analyst perspective; and looking across the range of available evidence in order to detect larger patterns. Integrating the mass of material generated and being able to examine it from a relatively neutral perspective, the CCRP team was in an excellent position to detect the trends dominating the Bosnia experiences and the structures and processes that drive them. **Focused research** by the CCRP team was reserved for key issues that (a) were central to the charter from ASD/C3I and CCRP priorities, (b) focused on topics where CCRP had or could get expertise and relevant evidence, and (c) were not being adequately covered by other agencies or organizations.

Coordination

CCRP looked beyond conducting its specific technical analyses and developing specific products to helping the community at large do a better job of learning the lessons of the Bosnia experience. Therefore, CCRP devoted some of its efforts to create

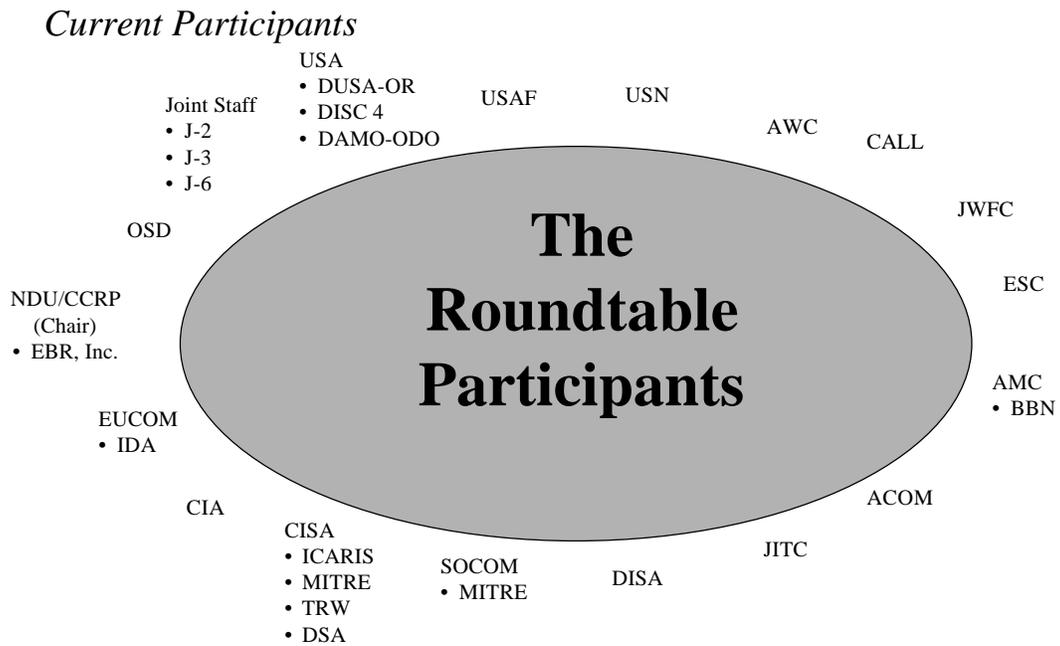
forums and mechanisms to encourage and facilitate studying the exchange of data, information, and ideas among the many organizations involved in studying the Bosnia experience. Formal and informal exchanges of drafts, professional discussions, workshops, publication of results, and the CCRP C2 symposia and community development programs were and will continue to be used to enrich the study and leverage its impact.

The most successful CCRP coordination initiative was the creation of a “Bosnia C4ISR Roundtable” (figure 12-3), where a range of U.S. activities involved in lessons learned and assessment of performance in Bosnia were brought together in a constructive atmosphere to encourage sharing and cooperation. The first meeting took place on April 10, 1996, with 21 activities involved. This session was an immediate and significant success. Virtually everyone present learned for the first time about one or more activities directly related to their own. Some initial findings were reported orally and consensus existed that the Roundtable should meet regularly. Participants readily agreed that the Roundtable should serve as a mechanism for reviewing draft materials and disseminating products on lessons learned and C4ISR performance.

Immediately after the first Roundtable meeting, CCRP published a directory of the organizations who had attended. This directory included the addresses (including telephone, fax, and e-mail) of the points of contact and a brief description of the relevant activities and interests of each of the organizations. An e-mail network was established to facilitate collaboration, coordination, and sharing of information. This network proved to be very beneficial to all of the participants. Follow-up meetings with a variety of Roundtable participants indicated that they had subsequently made a number of direct contacts with other members of the group and had been able to coordinate and focus their activities much better because of these new linkages.

The second meeting of the Bosnia C4ISR Roundtable took place on 30 May 1996. More than 30 activities or organizations asked to be represented, an increase of more than 50 percent from the first meeting. The agenda included presentations on several

Figure 12-3. The Bosnia C4ISR Roundtable



efforts that had reached preliminary findings. CCRP briefed the progress of efforts, IDA briefed their charter and first-order conclusions (largely on the planning and deployment phases) from their lessons learned effort for European Command (EUCOM), the Central Intelligence Agency (CIA) covered findings from their analysis of policies and procedures for intelligence sharing in the context of the Bosnia operation, and the CISA team briefed the progress of its C4ISR laydown. The first results of a study by the Center for Army Lessons Learned (CALL) were reviewed. Substantive discussion among different agencies was encouraged and proved highly productive.

As implied by its name, the Bosnia C4ISR Roundtable was a meeting among equals. All those U.S. organizations with a charter to collect data or lessons learned related to C4ISR, either in terms of command arrangements or supporting systems, were welcomed, as were those agencies or organizations who were potential consumers of the results of those analyses. CCRP served as the chair of the Roundtable. The organizations listed in figure 12-3 were all self-nominated by declaring that they had a role in Bosnian C4ISR and an interest in its assessment.

Taken together, the Roundtable was a major asset to the broad task of developing valid and meaningful lessons learned on the Bosnia C4ISR experience. While participation was voluntary, the value of the information exchange created a very real incentive for joining and attending. CCRP continued to use the Roundtable for the duration of the IFOR phase of the Bosnia operation. It was a useful mechanism to coordinate efforts and to ensure cross-checking of facts and findings within the community.

Collaboration

The rich set of lessons learned and effectiveness assessment activities already underway (figure 12-4) when the CCRP study started represented both major opportunities and potential problems. On the one hand, the opportunities for synergistic work were obvious. Moreover, as CCRP made contacts in the theater and the U.S.

community, virtually everyone indicated a willingness to cooperate and a positive attitude toward working together. Every organization involved in lessons learned or performance assessment also recognized that many different activities were underway. Almost all of them also expressed a strong desire for efficient and effective information exchange in this arena.

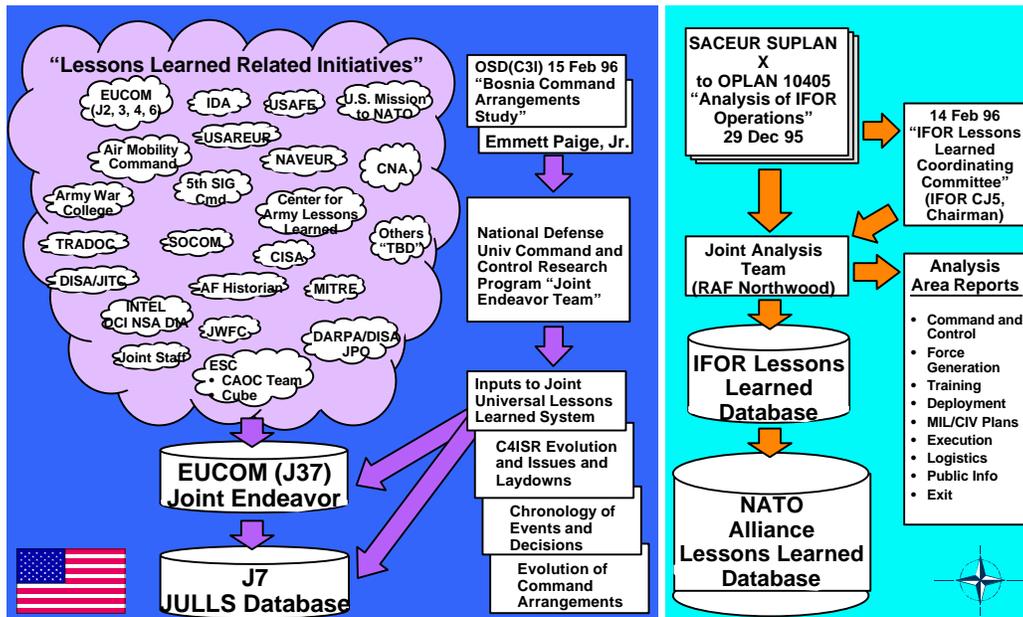
At the same time, there was a potential for problems to arise from the number and variety of activities underway. Overlapping missions and redundancy of data collection efforts were the most obvious. The demands on the time of key officers and staff in the field commands and operational headquarters were already high and a multitude of visitors became a significant burden. From the IFOR Joint Analysis Team (JAT) headquarters to the field commands, CCRP's analysts heard complaints about "IFOR Tourism" almost from the first contacts in theater. Some of these comments were pointedly directed at the United States, which reportedly had the largest number of visitors in the theater. Moreover, NATO sensitivity about national access to materials within NATO commands remained high and, reportedly, had not been well handled by U.S. and other national activities.

CCRP's approach was heavily influenced by attempts to take advantage of ongoing efforts where it could focus its limited resources on collecting data and conducting analyses of key issues. Considerable progress was made. By stressing collaboration, working closely with the JAT and selected U.S. activities, establishing mechanisms for cooperation and information exchange, and positioning itself to address key issues in command arrangements and C4ISR, CCRP was able to put an efficient and productive process in place and bring a coherent picture into focus. Having set up the necessary data collection and sharing mechanisms, CCRP became fully engaged in documenting the Bosnia C4ISR experience and identifying and researching key issues.

Three major thrusts existed (figure 12-4) in the IFOR lessons learned arena: NATO's formal effort, the NDU effort directed by ASD/C3I, and the relatively uncoordinated set of initiatives underway within the overall U.S. community. There were also na-

Figure 12-4. Collaborative Opportunities

Joint Endeavor / IFOR Lessons Learned Activities



tional efforts undertaken by the French and British, but these were not discovered until well into the CCRP study. The NATO process had a formal and relatively integrated structure. The charter of the JAT was explicitly derived from SACEURs Operations Plan (OPLAN), SUPLAN X. The JAT's charter focused on nine issue areas, including several related to C4ISR, particularly C2, force generation, military-civilian plans, execution, public information, and exit. The JAT also had the formal right to locate observers in NATO and IFOR headquarters and command centers in theater and had already done so. While the JAT viewed its charter as limited (primarily at the operational level and above, focused on its nine issue areas), they had the lead in NATO for IFOR operational lessons learned. This enabled them to collect information and conduct interviews on-site and in locations where unobtrusive presence was difficult. The JAT also maintained an extensive automated database on IFOR operations. They produced three interim reports (March 1996, June 1996, December 1996) which were forwarded to SHAPE and COMIFOR for distribution. A final report on IFOR lessons learned was sent to SHAPE in April 1997. In accordance with SUPLAN X, an IFOR/SFOR Lessons Learned Database was established and implemented on CRONOS. This database was the first of its kind in NATO to support an ongoing operation and it continued to be available for SFOR. In regard to the latter, the JAT charter was extended to June 1997 to accommodate the collection of lessons learned associated with the transition of IFOR to SFOR.

Clearly, a constructive interface with the JAT and the formal NATO process represented an important opportunity for collaboration, and this was an immediate priority for the CCRP team. An agreement was arranged between the director of JAT and the director of the NDU/CCRP study team. Under this agreement, CCRP provided both observers and analyst support to the JAT in return for access to data, information, and the Bosnia theater of operation for firsthand collection of experiences and insights. The CCRP and JAT collaborative effort proved to be extremely beneficial for both organizations.

In addition to the JAT, CCRP collaborative efforts were pursued with U.S. organizational elements such as EUCOM, USAREUR, U.S. Air Force Europe (USAFE), JAC at Molesworth, Electronic Systems Center (ESC), Air Mobility Command (AMC), AMC/BTIC, CISA (which became an active member of the CCRP core team), DISA/JITC, SOCOM, J2/DIA, CIA, NSA, CNA, IDA, the Air Force Historian, CALL, and the Army War College Peacekeeping Institute (AWC/PKI). The CCRP team had varying degrees of success in this regard, but in all cases, received numerous lessons learned reports and briefings from these organizations. Briefings and reports were also obtained from NATO organizational elements such as the JAT, the IFOR CJ6/CJCCC, the ARRC, the MND HQs, the IFOR Commander for Support (C-SPT), and several other sources.

CISA also undertook two major studies as part of its support to the CCRP effort. An IFOR C4ISR laydown was developed and is now available from them on a CD-ROM. A communications lessons learned assessment was done and is documented in their report, "Compendium of Operation Joint Endeavor Lessons Learned Activities," May 1997. An assessment of BC2A/JBS implementation lessons learned was also done for the CCRP effort by BAH in support of a DARO offer of help to CCRP.

CCRP contacts have also been made with the British and French lessons learned activities. Overall, the number of opportunities for collaboration was very large and potentially overwhelming for the modest size of the CCRP team. However, every effort was made to find and develop efficient mechanisms for collaboration. No significant effort was ignored and all relevant products were captured to ensure that CCRP's analyses and lessons learned were based on the best available insights and evidence.

Integration

CCRP assembled, reviewed, and integrated a large quantity of CCRP and non-CCRP briefings, reports, and other material. Products from a wide variety of sources were assembled first, so they would be available to support CCRP's analyses and reduce the

effort that was required to create a comprehensive picture. Assembling the variety of views contained in these products put CCRP in a position to see what they had in common, to identify differences, and to assess their relative reliability and validity, as well as the comprehensiveness, reliability, and validity of the overall body of work. Moreover, CCRP was able to both use these products as sources of information in its own analyses and also develop the larger picture of C4ISR experience and performance.

The products covered the entire field of C4ISR. For example, the intelligence community undertook a number of assessments and lessons learned efforts. The CCRP team received inputs from the Task Force Eagle G2 on intelligence operations and ISR system performance in MND(N). Inputs were also received on the U.S. NIC operations in Bosnia and JAC support activities. Very early in the deployment SOCOM sent a team to inventory intelligence systems in the field and assess their contribution to SOF missions. The DCI organized a lessons learned activity that generated several significant reports on information releasability and dissemination. DIA and NSA also conducted their own review of the Bosnia experience. Virtually every intelligence organization with presence in the theater was seeking to place its own experience in context. These efforts were very valuable inputs to CCRP's understanding of the overall C4ISR issues. In addition, the Defense Science Board Bosnia Task Force report on the Application of Intelligence to the Battlefield was also made available to the CCRP team.

More focused efforts were underway from a number of other perspectives. The U.S. research and development community, particularly those elements led by DARPA and the DARPA/DISA JPO through various technology demonstration programs, was assessing the performance of leading-edge services and the process by which they were introduced into the *Operation Joint Endeavor* command structure. These were valuable sources for lessons learned in the technology insertion process. The Air Force established a Bosnia-oriented integration activity (referred to as the CUBE) at ESC to simulate the network of C2 systems controlling air operations in the theater with a particular emphasis on the CAOC. This allowed

them to examine proposals for changes and assess the integration and introduction of new C2 capabilities before deployment into the Bosnian theater of operation. The ESC and Air Combat Command (ACC) also coordinated with the CAOC to assist with decision support system integration and air operation processes enhancements. The ESC lab also provided a Help Desk for dealing with real-time integration issues. The Army's AMC/BTIC served as a clearing-house for critical technologies and the "nerve center" for tracking and integrating the technology communities' efforts to support U.S. soldiers in Bosnia. The SHAPE Technical Center (now the NATO C3 Agency, the Hague), who was responsible for technical support to NATO's C2, logistics, and transportation decision support systems as well as the new information systems used to support NATO's C2 operations (e.g., CRONOS) in-theater, was also collecting lessons learned and provided valuable insights to the CCRP team. Some of the contractors involved in bringing new technology into the theater and supporting it there were also learning important lessons and they too were documenting their experiences. N.E.T. provided CCRP lessons on the IDNX deployments and EDS provided lessons on the deployment of the IARRCIS.

SHAPE NACOSA and Communications and Information Systems Division (CISD), IFOR CJ6, the CJCCC, the ARRC G6, the MND G6s, and the C-SPT G6 provided insights on the deployment and management of the NATO communication and information networks, including lessons learned. IFOR CIMIC, Public Information, and PSYOP organizational elements provided insights to the CCRP team in the areas of civil-military operations and the IFOR information campaign. IOs, NGOs, and PVOs were also interviewed as a means to better understand the civil-military aspects of the operation.

The doctrine community was also watching operations in Bosnia closely, particularly for lessons learned in coalition C2 as well as civil-military relations. CALL deployed dozens of personnel with the U.S. troops supporting Task Force Eagle and issued four (a fifth in final review) volumes on findings and lessons learned. While largely at the tactical level, this work was very important to

capture the U.S. experience. The U.S. Air Force had considerable interest in the Bosnia operation and began a vigorous effort to examine the problems associated with generating an integrated air picture in the theater, but then recognized that this was only a subset of the larger and more crucial issue of generating an integrated battlespace (air, ground, and maritime) picture and was deeply involved in that effort. IDA worked with the Air Force on issues related to air management, largely in the context of the CAOC. The Army War College Peacekeeping Institute held two After Action Reviews (AARs) to examine Title 10 issues that impact on the Army in the Bosnia context. These AARs have been made available to the CCRP study as well.

The AMC completed an analysis of its experiences in supporting the Bosnia deployment. The C2 elements of that report were valuable in the context of NATO lessons learned on this same topic and assisted CCRP in ensuring a balanced appraisal. EUCOM ECJ37 was designated by the Joint Staff J7 to be the theater manager for Joint Universal Lessons Learned System (JULLS). IDA was contracted to support EUCOM in this regard and to do an in-depth analysis of the planning, deployment, sustainment, and redeployment phases of the operation. These efforts provided the CCRP team with insights and a channel for monitoring a broader set of inputs relevant to C4ISR. The in-theater commands themselves held lessons learned conferences and meetings covering the deployment, sustainment, and transition of IFOR to SFOR phases of the operation. The results of some of these activities have been provided to the CCRP team in the form of briefing material.

The historians in NATO and U.S. commands were generally well informed and only a few days or weeks behind real-time capturing of important events. The NATO and IFOR historian's material and chronology were accessible through the JAT. The IFOR historian had recorded thousands of hours of interviews with all levels of the command structure. Activities of the other historians were generally releasable by the commands themselves. CCRP has initiated contact with the USAREUR, EUCOM, and Air Force historians to get access to their findings and databases.

Assembling the documentation in itself has created a valuable resource for future research and analyses. By actively reviewing and integrating these materials, CCRP has been able to make a meaningful contribution to the overall national and NATO lessons learned activities. By acting as a clearinghouse for the exchange of such materials, the Bosnia study has also contributed to the coherence and quality of the overall U.S. lessons learned activities.

Focused Research

CCRP's priorities were based on the needs and missions of the C4ISR community. They took two different perspectives: organizational and international. Organizational priority was given to OSD and the Joint Staff, with a recognition that the needs of the CINCs and services were also important priorities. At the same time, however, NATO's needs as a coalition and issues important to the non-NATO coalition partners were not ignored. Rather, they were picked up in the context of U.S. national needs. At the international level, U.S. issues were examined as well as issues that related to U.S. operations in the NATO context, NATO operations, and IFOR or NATO operations involving non-NATO partners. C4ISR was seen first as a military issue, but was also examined in terms of civil-military relations at all levels. CCRP's focused research addressed areas such as support to the warfighter, coalition command arrangements, C4ISR system performance and vulnerabilities, information operations, technology insertion, civil-military cooperation, and the lessons learned process.

Theater Visits

The ASD/C3I tasking for the Bosnia Command Arrangements Study was signed out on 15 February 1996 and study data collection began in the March/April 1996 time frame. The early phase of the CCRP study focused on data collection. Monthly visits were made to the JAT to gain insights and to review the database

they were putting together on the IFOR operation. In addition to the data collection activity, CCRP also provided analyst support to the JAT during these visits. This too provided useful insights from a NATO perspective. Extensive visits were also made to supporting commands and to the theater of operation. These visits included EUCOM, DISA-EUR, the JAC, the 66th MI, USAREUR, USAFE, NATO, SHAPE, and the SHAPE Technical Center (now the NC3A the Hague). Two extended visits were made under the umbrella of the JAT observer corps to Bosnia and Croatia. In regard to the latter, visits were made to IFOR and the ARRC in Sarajevo, MND(SW) in Banja Luka, MND(SE) in Mostar, C-Support in Zagreb, and COMMZ (FWD) in Split. Visits were also made to the IFOR CJ6 and the CJCCC in Naples. NDU/CCRP also provided two observers to the JAT for duties at MND(N) in Tuzla and at IFOR (FWD) in Sarajevo. In addition, an NDU/CCRP observer and analyst was also provided to the JAT to focus on the area of IFOR information operations. This support included two extended visits to Bosnia and Croatia as well as visits to NATO, SHAPE, and the UN HQs in New York. The NATO and national insights gained through CCRP participation in the JAT observer and analyst activities have been invaluable.

The Future

The CCRP team continues to collect experiences and lessons learned from the IFOR portion of the operation, including those emerging from similar activities of the other two framework nations—France and the United Kingdom. Collection activities have also included the SFOR portion of the operation but at a significantly lower level of effort. It is planned to extend the IFOR database and library of lessons learned reports to include those of SFOR and any follow-on NATO activities. As new insights and findings emerge from the ongoing CCRP study activities, these will be documented in professional publications and shared through symposia and other professional forums.

XIII. Lessons Learned About Lessons Learned

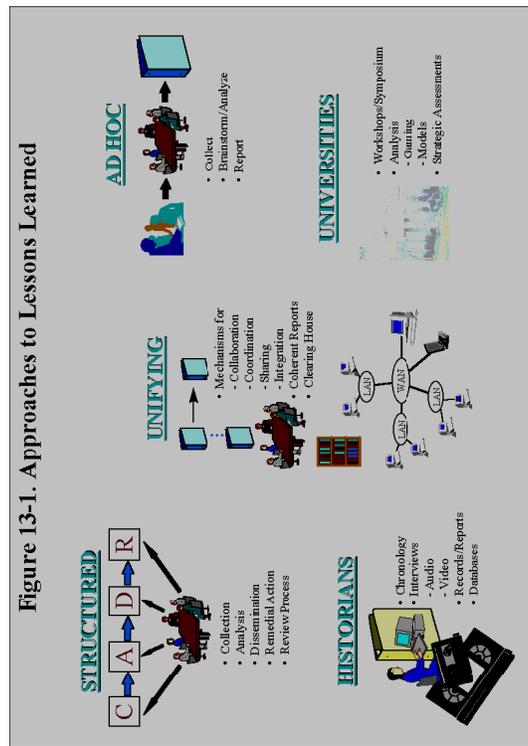
Larry K. Wentz

Many NATO and national initiatives have attempted to collect Bosnia insights, assess the effectiveness of the IFOR, and assemble lessons learned from the Bosnia experience. Most of these activities were not well coordinated and no overarching set of issues or functions drove the independent activities. Furthermore, no one person or organization was given the responsibility for setting the agendas and priorities of these efforts. Hence, there were redundancies and overlaps in the related activities. The initiatives also varied in complexity and depth, duration of the efforts, and focus of the areas of interest. NDU was tasked by the ASD (C3I) to attempt to pull together an appropriate collection of ongoing activities and put a coherent C2 and supporting C4ISR picture together, including lesson learned. A by-product of this effort was firsthand experience with the numerous ongoing lessons learned activities and their strengths and weaknesses. This chapter discusses findings and experiences from both a U.S. and NATO perspective, including some national perspectives. This chapter discusses NDU's efforts to act as a clearinghouse for Bosnia study activities, to facilitate collaboration and cooperation among the related community initiatives, and to integrate the C4ISR community experiences and lessons learned into a coherent picture.

Approaches To Lessons Learned

As soon as CCRP began organizing its effort and seeking to assemble a list of ongoing activities, it became clear that a multitude of organizations and agencies were either already engaged in lessons learned activities in Bosnia or planning for them. CCRP alone had more than 40 U.S. Organizations participating in its Bosnia C4ISR Lessons Learned Roundtables. There was also a variety of approaches being employed to collect insights, assess operations, and assemble lessons learned (figure 13-1). These approaches ranged from more formal and structured arrangements such as the IFOR JAT, CALL, and the JULLS process employed by USEUCOM, USAREUR, and USAFE, to ad hoc arrangements such as the Air Mobility Command and DCI quick-look assessment activities. There were also other structured approaches such as the NDU/CCRP study, the Army War College Peacekeeping Institute After Action Reviews, the IFOR CJ6/CJCCC, C-SPT and ARRC lessons learned activities, and the activities of the historians (USEUCOM, USAREUR, USAF, SHAPE, IFOR, and others). The French employed a more ad hoc (individual collection and hot debriefing of returning commanders) approach to collecting their lessons and the British used a more structured (team) and unifying approach for their national effort. There were longer term strategic thinking-oriented assessment activities such as those being conducted at the George Mason University (GMU) Institute of Public Policy, the Army War College Peacekeeping Institute, the National Defense University Institute for National Strategic Studies, the Naval War College, and the Pearson Canadian International Peacekeeping Centre. These activities employed workshops and modeling and gaming techniques to examine policy, strategies, and options for the future.

The formal approaches tend to be long-term efforts that employ highly structured processes with collection, analysis, dissemination, and action resolution phases. They use subject area experts to collect information and insights through interviews, after action reviews, unsolicited inputs, and formal reporting such as JULLS. They also use a collection plan to focus and guide their



activities. Professional analysts are used to assess the insights and experiences and to derive the lessons learned and recommend actions to resolve outstanding issues. Extensive databases are maintained on findings and recommendations. A review process is employed to ensure consistency and quality and to provide direction and guidance to the overall effort as appropriate. Results are disseminated in the form of formal reports, pamphlets, memorandums, bulletins, newsletters, customized reports, and Web home pages (both Internet and military networks). Finally, in some cases, a remedial action program is used to task organizations to fix problems and to track the resolution of outstanding actions.

The ad hoc activities tend to be less structured and of shorter duration. Subject area expert teams are formed and quick-look assessments using detailed theater interviews and brainstorming sessions are employed to drive out the key findings and recommendations. As an example, this was the approach used by the Air Mobility Command. The actions from ad hoc efforts tend to be focused on fixing near-term problems.

The other efforts are somewhere in between in terms of complexity and duration. For example, the JITC put a team of subject area experts in Bosnia for 3 months to collect insights and develop the communications baseline and associated interfaces and interoperability issues. Two months were then spent documenting and briefing their findings and recommendations, and a final report was published for broader distribution. The Army War College Peacekeeping Institute convened subject area experts, specifically those with Bosnia operational experience, for two different 1-week intensive after action reviews. The AAR outputs were briefings and reports with actionable items that were strategically oriented, i.e., things the Chief of Staff of the Army needed to be aware of and could take an action on. This effort was mainly focused on Title 10 issues but some other C2 issue areas were also addressed. The NDU/CCRP effort employed a small team of professionals oriented toward leveraging community activities to put a coherent story together that addressed strategic, operational, and tactical issues. The products were and will be briefings, reports, symposia and work-

shop participation and papers, and books and other material for the professional military education program. The IDA study done for EUCOM employed a small team of professionals to review, document, and analyze the U.S. participation in the Bosnia operation. Their reports addressed strategic- and operational-level issues related to the planning, deployment, sustainment, and redeployment phases of the IFOR operation.

Many of the commands involved in Bosnia had staff historians who were also seeking to document their commands' participation in the operation. The SHAPE and IFOR historians, in particular, had rich access and developed valuable material on the command history. The EUCOM, USAREUR, USAF, SHAPE, and IFOR historians were valuable sources for the NDU study. The historians used both audio and video taping extensively as the principal means for recording insights and experiences.

The commands, including the combat support organizations, also tasked their own headquarters to assemble lessons learned and to perform assessments. There were a few organization elements who, because of resource limitations and pressures of the operation, were unable to devote the level of effort necessary to do as complete a job as they would have liked to do. These units were, however, willing to work with unifying activities such as the NDU/CCRP effort to help them, but their lessons learned story together. IFOR held meetings of senior officers to review phases of the operation and to look ahead at future challenges. Indeed, virtually every level of command established similar tasking to ensure that lessons were both recorded and acted upon in the near term. Some of these reviews included specific review of performance issues, but their major focus tended to be on process improvement.

Finally, the universities and the military education community also monitored Bosnia. GMU's Institute of Public Policy (Program on Peacekeeping Policy) used their Conceptual Model of Peace Operations to examine issues related to Brcko. As noted earlier, the Army War College Peacekeeping Institute held two After Action Reviews focused on Title 10 issues. NDU's Institute for National Security Studies has been engaged in political-military analyses based

on its expertise in prior peacekeeping efforts such as Somalia and Haiti. They have held workshops and used the NDU gaming facility to examine Bosnia issues related to civil-military operations, Brcko, IPTF, and conditions for exiting Bosnia. The Naval War College has also used its Situational Influence Assessment Module (produced by SAIC) to examine exit strategies. The Pearson Canadian International Peacekeeping Centre has sponsored a number of workshops and symposia on conflict resolution.

IFOR Lessons Learned Experiences

Despite the number of organizations involved in the lessons learned effort, no one, has yet been able to pull all of these activities together into a coherent “big picture” story for the military aspects. Furthermore, since little to no collection of lessons learned has occurred in regard to the political, civil reconstruction, nation building, and economic recovery aspects, an integrated picture of the “Dayton Perspective” has not even been attempted and it is not clear who would put such a perspective together in any case.

The IFOR JAT observers noted that many nations had fielded teams of analysts in various HQs, so there was the potential for much duplication of effort. Additionally, there was the burden placed on the staff in these HQs by a multiplicity of queries for essentially similar information. If a more coordinated approach had been possible from the outset, perhaps greater value might have been achieved to the benefit of all parties.

Lessons learned are multidimensional. In addition to the doctrine, policy, processes, procedural, and training aspects, there are also technical, system, operational, and command structure perspectives. One can look at them from NATO and national points of view or from the civilian, military, and humanitarian aspects. There are mission and function cuts that can be looked at as well as the planning, deployment, sustainment, and redeployment phases of the operation. The point is that no one organization covers all aspects of an operation in a way that puts a coherent big picture story to-

gether. For example, the IFOR JAT did not address the intelligence aspects of the operation. The IFOR CJ6 and CJCCC focused mainly on communications. The IFOR Commander for Support focused on functions such as movement control, legal, medical, and contracting but also covered some C2 structure and communications and information support aspects. The Air Mobility Command focused mainly on the airlift support for deployment. CALL, USAREUR, and the Army War College focused on the Army role in support of the operation. EUCOM and its IDA study looked at the U.S support to IFOR. The French and British focused on their national roles. The NDU/CCRP effort tried to pull a bigger picture story together, but again its guidance was C2 structure and the supporting C4ISR. There are lessons to be learned from the political, economic, and humanitarian activities in support of the Dayton Accord but it is not clear if anyone will be collecting insights and lessons learned for these aspects of the operation.

Clearly, broad participation has considerable benefits. The recognition of the importance of learning from the Bosnian experience, the active participation of both C4ISR producers and consumers, and the involvement of many agencies and organizations in both issue identification and problem solving are signs of learning and adaptive organizations. Hence, this bodes well for the future.

The current “catch as catch can” broad participation lessons learned system also has some very positive attributes. Lessons learned were sought throughout the operation and its supporting activities. The variety of actors involved meant that a broad range of perspectives were being considered. Moreover, because the operators were deeply involved, lessons were not generally collected and forgotten, but rather became the subject of specific actions to correct them. Obvious examples included the vigorous follow-up after LIWA reported vulnerabilities in unclassified LANs to USAREUR and the intelligence community’s review of dissemination policy and follow-on aggressive action to change the field practices to improve the service to the coalition operation.

However, the lessons learned process had its problems. First, overlap and redundancy existed, which led to excessive demands on operator time. One senior NATO officer identified nine separate occasions when he had been interviewed by U.S. lessons learned efforts. Second, to the extent that lessons learned activities were performed within operating organizations, they tended to have parochial agendas and results. Third, no overall set of integrating issues or functions was created, so the lessons learned suffered from gaps on key issues and lacked systematic data collection efforts and sharing of lessons and insights. Finally, while lip service to information exchange was plentiful, many products were still held closely by their originators. The players in Bosnia lessons learned represented almost every organization or agency involved in or supporting *Operation Joint Endeavor*. The most important lessons learned activities were those of the commands and headquarters themselves, both U.S. and coalition partners, because they typically involved vigorous action programs to resolve the issues identified and because they represented the difference between the anticipated operating environment and the one actually encountered.

NDU's efforts to assemble a coherent lessons learned picture highlighted several difficulties as well. The most important problem encountered was the uncoordinated collection of information. In an effort to reduce demands on operators and simplify the situation, some commands granted "official" status to some collectors. For example, the IFOR JAT was given official monopoly on collecting lessons learned for NATO. Unfortunately, the focus of the formal IFOR effort was limited to the nine items in the JAT charter (see chapter 12). Furthermore, the quality of collection and analysis was dependent upon the specific officers the member nations were willing and able to provide the JAT for this tasking (it was necessary to augment the JAT with observers and analysts provided by NATO member nations). Only a fraction of the JAT team were trained analysts, and data collection tended to be more idiosyncratic than systematic. EUCOM granted similar "official" status to its IDA team. CALL functioned as the primary activity for

U.S. Army collection. Allied efforts were seldom as systematic as those used by U.S. commands. All in all, the high level of activity did not translate into systematic coverage of key issues.

Many of the lessons learned efforts have also proven parochial. They tended to focus on the relatively minor and technical issues that made day-to-day operations inconvenient or difficult rather than on more fundamental questions. There was a natural tendency to avoid putting one's own command on report so this resulted in a careful documentation of external factors without a balanced recognition of internal problems. Moreover, internally identified lessons learned had a tendency to focus on symptoms rather than causes. As a simple example, analyses of problems with computer systems viruses focused more on installing better virus protection devices rather than changing the behaviors that caused them to proliferate.

The most serious problem in lessons learned has been the inability to create an overarching set of issues or functions. While most lessons learned charters were very broad, no single person or organization had been given responsibility for setting the agenda. This resulted in gaps in coverage, particularly where the issues were potentially embarrassing or resided near organizational boundaries.

The lack of an overall structure for lessons learned collection and sharing was reinforced by the multiplicity of nations, organizations, and agencies involved and the inability to freely share findings and experiences. As noted earlier, the NATO JAT charter was limited to nine specific functional areas. C4ISR issues that cut across levels or national boundaries were particularly difficult to analyze because the charter seldom existed to examine the causal factors at work. Finally, broad community information exchange was more difficult than anticipated. The players were willing to orally discuss issues, insights, and lessons learned but few were willing to pass on formal or draft documentation until it was appropriately staffed and/or approved by their respective organizations for more general release. This reflected parochial agendas, NATO

sensitivity to national access, and the lack of a central, authoritative lessons learned organization to facilitate information exchange and provide issue-focused guidance to the various efforts.

The Way Ahead

The need to capture lessons learned from real-world operations and use them for subsequent remedial actions is widely acknowledged throughout the international community. The need to build a more coherent story and more effectively collaborate and coordinate the collection and sharing of experiences and lessons learned may not be as widely accepted. Certainly, the international community needs to consider putting some mechanism in place to better focus, facilitate, and encourage the coordination, collaboration, and sharing of lessons learned activities and findings. The ability to enforce remedial actions also needs to be a part of this consideration. In order to accomplish this, an international organizational element needs to be granted some degree of official status and authority to perform the role. It also needs a staff of appropriate subject area experts and professional analysts, adequate funding, and an agreed process to guide the participation of the international community. NATO would be a logical organization to establish such a capability. If NATO were to provide such a capability, it would need to go beyond the level of effort and capability the JAT established to support IFOR and the NATO Permanent Maritime Analysis Team that supports maritime exercises and operations. Furthermore, it would need to not only be a BI-Major NATO Command (MNC) initiative that addresses the military aspects but also include the political aspects of NATO as well.

The NDU/CCRP approach to facilitate coordination, collaboration, and sharing through the use of the Bosnia C4ISR Roundtable was quite successful. This coupled with the special relationships formed with the IFOR JAT and U.S. command elements significantly helped CCRP's attempts to build a coherent story out of the various independent lessons learned activities. CCRP

has been able to perform the role of clearinghouse with a reasonable degree of success. A lot of perseverance and community willingness to cooperate was necessary to pull off the successes to date. The effort is now bearing fruit.

The use of a unifying organization is certainly one way of pulling the community and their activities together. In the end, this may be the best way to approach improved collaboration, coordination, and sharing in order to ensure that a more coherent story emerges from the large number of activities triggered by a major international operation. It is certainly not a technology issue; the information networks of today provide the means to the end. It is an issue of political will. There is certainly a need to do this but the issues of who, where, level of effort, staffing, ability to enforce remedial actions, and funding of such an activity are yet to be fully addressed for either national or international initiatives. The system is broken and needs to be fixed.

There is an encouraging sign on the horizon. The lack of a standing NATO Joint Analysis capability, which led to the creation of the ad hoc JAT, also prompted discussion on the requirement for a permanent JAT. As a result of SHAPE's experience with IFOR, there is a BI-MNC proposal in front of the NATO Military Committee to consider the establishment of a BI-MNC Joint Analysis and Lessons Learned Centre. The stated purpose of this center is to be NATO's central agency for the operational analysis of exercises and real-world operations, and for the coordination of the related lessons learned and the associated remedial action process. It is the view of the two MNCs (SACEUR and SACLANT) that these three activities—analysis, lessons learned, and remedial action process—are closely connected and mutually supportive. This is certainly a step in the right direction to fixing the system for NATO and possibly for multinational operations as well.

XIV. Summary

Larry K. Wentz

NATO Comes of Age

The NATO Alliance proved that it can be flexible and adaptable and showed that with clear political guidance, the operational military arm can accomplish tasks given to it by its political authorities. The successful deployment of the NATO-led IFOR in support of *Operation Joint Endeavor* can be attributed to a number of factors. First, there was the pressure of world opinion to take action given the massacres in the country, the previous failures of the UN, and the opportunity for achieving a more permanent settlement provided by the Dayton Peace Accord (DPA). Second, relative to other international organizations (UN, WEU), NATO had an effective military and political structure. NATO had exercised its capabilities both politically (in the Partnership for Peace program) and militarily (in *Operations Deny Flight* and *Deliberate Force*) to bring stability to this part of the world. Finally, NATO had an intact command and control system, one based on 45 years of cooperation and refined during NATO operations in support of the UN in Bosnia.

Influencing Factors

The first ever out-of-area operation for NATO was a military success, but there were a number of key issues that IFOR had to address early on to ensure that it would happen. First, the Dayton Accord did not designate a single authority to synchronize the military, political, economic, and humanitarian aspects of the mission. Ad hoc arrangements were initially employed to facilitate collaboration and cooperation and more formal arrangements were employed later through participation in the Office of the High Representative (OHR)-established Joint Civil Commission (JCC).

Second, the civil-military activities in support of peace operations were new for NATO. There was no common understanding by commanders and staff at all levels of IFOR of the capabilities, roles, and mission of Civil Affairs units and personnel, referred to as Civil-Military Cooperation (CIMIC). Furthermore, the civil-military aspects did not receive sufficient attention during the planning and initial execution phase of the operation due to the heavy emphasis on the military enforcement aspects of the Dayton Accord and force protection.

Third, information operations for peacekeeping were also new for NATO. The NATO and SHAPE doctrines on public information and PSYOP had just been revised. National PSYOP doctrine differed and the command and control of PSYOP contingents remained with the participating nations (mainly the United States with participation from the United Kingdom, Germany, and to a lesser extent France) and was not placed under NATO C2 during the IFOR operation. The public information, civil affairs, and PSYOP aspects of the IFOR information operations required special attention to ensure coordination and synchronization of related activities. Ad hoc committees were established at the IFOR and ARRC levels to facilitate coordination.

Fourth, NATO had no in-place ability to deploy forward its strategic C4I capabilities. There was little to no Bosnia telecommunications infrastructure because it had been destroyed by the war and NATO air strikes. NATO, therefore, had to rely heavily on the

national tactical assets of the framework nations—particularly the United States (the major contributor), the United Kingdom, and to a lesser extent France. The UN VSAT network, which was already in place, was used extensively and commercial products and deployable commercial SATCOM services were employed to extend NATO's strategic network connectivity into Bosnia and to provide information services to the deployed headquarters and forces.

There were other factors that influenced NATO and national activities in preparation for and execution of the IFOR deployment. The operation was occurring at a time when NATO and the nations were reducing force structures. Non-NATO and PfP nations would be involved with NATO in a real-world operation for the first time as well as the Russian Federation and there was little NATO guidance on how to proceed with these first-time events. In addition to being the first out-of-area operation, it was also the first major ground operation ever. There were multiple OPLANs that added some confusion. NATO would be taking over from the UN and other peacekeeping agencies and this had some built-in uncertainties. Deployment would take place in the depth of winter in difficult terrain. The likelihood of hostilities was a major concern because of the fragility of the peace arrangements in Bosnia. There were morale problems associated with deploying troops over the Christmas period. Therefore, one should not underestimate the degree of difficulty NATO and the nations faced as they prepared for and deployed to Bosnia in support of *Operation Joint Endeavor*.

Threat Environment

The threats in Bosnia were real. Three former warring factions, not only with significant combat power but also with robust intelligence collection capabilities, were waiting for the arrival of NATO forces and it was not clear how they might react to the IFOR deployment. The FWF also had a propaganda and disinformation campaign in operation and targeted against IFOR. Terrorists, organized crime, and petty criminals were also part of the threat. Finally, minefields were numerous and added risk to deployed personnel.

The local, national, and ethnic media were well established and generally trusted. The population of Bosnia was to a large extent literate and relatively well educated and used to all forms of media that characterize an “information society.”

Making a Difference

Upon arrival in country, IFOR made it very clear to the FWF at the outset that they were there to enforce compliance with the Dayton Accord and would use force if necessary. Checkpoints were bulldozed, road blocks shut down, the FWF separated, and their forces and equipment placed in cantonment areas and barracks. Violations were experienced from time to time: weapons were discovered in unauthorized locations, soldiers and tanks in the ZOS, and unauthorized police checkpoints. Such violations were not tolerated and swift actions were taken when the FWF tested IFOR’s resolve. The IFOR information campaign was also a powerful tool in getting the message to the FWF and the local population.

In the end, the Bosnia theater was more peaceful than expected. Except for a few overt physical attacks on facilities and personnel, the FWF were generally in compliance with the GFAP. One must be reminded, however, that the situation could have changed for the worse at a moment’s notice.

Certainly, IFOR’s tremendous military firepower was a deterrent but the military also put a lot of faith in the deterrent power of information dominance. IFOR was able to make it clear to the FWF that they could monitor them any time of the day or night and under any weather conditions. The ability to see, understand the situation, and strike with precision no doubt had its effect in deterring aggressive actions on the part of the FWF. In the words of MGEN William Nash, Commander MND(N), “We don’t have arguments. We hand them pictures and they move their tanks.”

The Fog of Peace Operations—Bosnia Experiences

Operation Joint Endeavor was, of course, an Operations Other Than War (OOTW) with all of the associated ambiguities, complexities, and challenges. As experienced in other OOTWs, these operations tend to be frustrating because the structure that militaries take for granted, such as a unified chain of command and clear, simple rules of engagement, are lacking.

For many reasons, OOTWs are usually messy and almost always involve ad hoc coalitions of the willing with politically driven command arrangements. More often than not they involve, at least in practice, a consultative environment in which key parties need to develop and maintain a common understanding of the mission, issues, and progress toward meeting the end state. Planning and executing such operations are complicated by factors such as short time lines, a highly dynamic environment, and uneven capabilities and experience among coalition members.

In almost all instances, OOTW operations are not able to rely on the in-country infrastructure to support their C2 needs and require augmentation of the limited indigenous capabilities with national tactical military systems. Given that a number of different players are usually involved and given their desire to use systems they are comfortable with, these operations typically begin with a “Federation of Systems” with the inevitable interoperability challenges and security disconnects. These are simply the realities of such operations and were true for *Operation Joint Endeavor* as well.

Force Protection

Bosnia was a somewhat schizophrenic operational environment. In MND(N), force protection measures were strictly enforced and troops were required to wear full battle gear and travel in four-vehicle convoys. For other parts of the area of operation, the force protection measures were less severe. The headquarters facilities

were located in urban and/or open areas and many employed limited traditional lethal and physical protection such as heavily armed guards, tanks, barriers, sandbagged bunkers, and obstacle courses in access areas.

Protection for U.S. forces will always be a significant issue. In Bosnia, U.S. force protection took on a higher degree of importance than had been seen in other U.S. military peace support operations. It was a formal part of the OPLAN mission statement and permeated all aspects of mission execution. Many non-U.S. IFOR participants believed that U.S. force protection measures were politically motivated and not based on a realistic threat assessment. MGEN Nash, Commander MND(N), defended the tough self-protection standard as important for both safety and discipline reasons. Furthermore, in his view, “the American soldier today is...more of a target than soldiers of other countries and they deserve all the protection I can give them.”

Enforcement of force protection was inconsistent between U.S. service members serving under a U.S. command and those under NATO control. Civil agencies were concerned that this inconsistency was sending mixed signals to the warring factions. The stringent U.S. force protection measures hampered civil-military cooperation activities and the ability of U.S. soldiers to move away from the peace-enforcement-only mindset. It appeared to many that the second- and third-order effects of the stringent force protection measures were neither fully understood nor properly anticipated. Some easing of the rules occurred over time as the operation evolved and more civil affairs work was performed off post.

Security Challenges

OPSEC was particularly challenging for the IFOR operation. The operational environment was reasonably stable for Bosnia and the lack of an obvious threat created the possibility of a relaxed security posture and increased complacency. Other types of OPSEC risks had to be managed as well. There were numerous television and print journalists questioning soldiers. On a daily basis, hun-

dreds of local national workers entered IFOR areas of operation. It was a challenge for the CI and HUMINT operators to keep a close eye on these daily visitors.

There were COMSEC and INFOSEC issues that had to be dealt with as well. Although the military communications and information systems operated SECRET system-high, there were other systems that were not secure. The UN VSAT network, INMARSAT, cellular, and the commercial PTT telephone systems were not protected and they were used frequently for command and control purposes. The commercial Internet was also used frequently. Configuration management and information protection measures were slow in implementation. An enormous amount of classified and unclassified material was produced; extra care had to be taken when dealing with mixed classifications of information. There were releasability issues related to sharing information and capabilities among 30 plus nations. Diskettes were shared between classified and unclassified systems and there was a lack of discipline and standard operating procedures to effectively control the situation.

Security was an ongoing responsibility for which improvements were continuously made over the duration of the operation.

Information Activities

In today's high-technology environment, information can determine the success or failure of the military operation. The "CNN effect" (i.e., unsubstantiated media reports), coupled with the "information revolution," created formidable challenges for the military. In Bosnia, there was media presence throughout the country when IFOR arrived. The information networks serving the media, IFOR, and its coalition member nations provided the ability to share information at a speed and efficiency never before experienced. Frequently, media reports of incidents would reach the home country and/or higher headquarters before the commander on the ground was aware of the situation and able to react.

There were e-mails to home from the troops in the field and Internet home pages were used by the NATO and national public affairs organizations to inform and update the general public on IFOR operations. The ease with which information could be shared fostered active, and sometimes lengthy, reporting (such as daily situation reports). Higher headquarters were constantly apprised of matters both large and small. Occasionally, headquarters and other command elements would use the networks to bypass intervening organizations in order to get information firsthand, sometimes leaving the broader community in the dark. The problem soon became one of finding the useful details among the wealth of information available rather than a lack of information. Because of the improved ability to inform and influence, the Public Information Office and the IFOR Information Campaign (IIC) became important tools of the Bosnia operation.

As noted earlier, in some areas of Bosnia, such as those occupied by the Serbs, an information campaign targeted against NATO was already in full operation when the IFOR troops arrived. Hence, the IIC was at a disadvantage at the outset because it had to compete with an already established and effective campaign that could get inside of the IFOR decision loop and outmaneuver some of the initial IFOR efforts. A contributing factor was NATO rules of engagement for the IIC. The campaign was forbidden to use disinformation and deception and could not take actions that undermined the factions, take sides, or directly refute FWF disinformation activities.

IFOR also had some problems adapting to the local population's media consumption habits. While IFOR relied primarily on printed material (*The Herald of Peace* and *Mircko*, posters, and handbills) and radio to start with, the Bosnian's preferred medium was television. Also, IFOR radio transmitted on AM and the Bosnians listened mostly to FM radios. Adjustments were made to accommodate other media forms such as FM radio and television, including the use of local radio and television facilities as well. The

U.S. PSYOP platform, Commando Solo, was not deployed until the SFOR phase of the operation to support the September 1997 election activities.

The IIC proved to be a difficult task for IFOR and the jury is still out on its overall success. It was certainly a success in the first 9 months of the operation in support of force protection and Dayton Accord compliance activities and for the September 1996 national elections. There were also some other successes such as the raid on Fortica (terrorist training camps) and *Operation Volcano*, the destruction of 250 tons of Bosnia Serb munitions. The success on the civil, economic, and humanitarian side of the operation was not as obvious. A top-down driven campaign plan with top-down driven products was viewed as an important contributor to the military successes.

Intelligence Considerations

The intelligence community also faced challenges unique to supporting a coalition peace operation. Traditionally, intelligence tends to focus on the enemy. However, it is not always clear who the enemy is in a peace operation.

The bulk of the national intelligence systems supporting IFOR were designed for go-to-war, not peace, operations. The NATO intelligence doctrine, principles, and practices were being revised at the outset of the operation. In the case of the United States, “force protection” and the Army maneuver warfare doctrine drove the U.S. intelligence architecture put in place for *Joint Endeavor*. In reality, though, the IFOR operational environment was relatively benign and the peace support operation was not maneuver warfare.

The Bosnia intelligence operating environment was marked by large areas of operation and interest, difficult terrain, and poor weather conditions. There were multiple belligerent factions and a “front line” that was 360 degrees. The operation had to adapt to differences in NATO and national methodologies and procedures. The operation had to monitor a wide spectrum of threats, including

the FWF, criminal activities, extremists, civil disturbances, and terrorism. FWF equipment storage sites and barracks, the ZOS, mass gravesites, and potential “hot spots” caused by freedom of movement, resettlement, and inter-ethnic conflicts had to be monitored as well. The nature of the operation muddled any clear division among strategic, theater, and tactical levels. Finally, equipped to function in a tactical fight, NATO and the national tactical intelligence capabilities were less prepared to function in a peace support role. Doctrine, CONOPS, procedures, intelligence preparation of the battlefield, and intelligence, surveillance and reconnaissance (ISR) capabilities had to be adjusted and augmented to accommodate peace operation requirements.

Experience with other OOTWs also clearly demonstrated that although non-intrusive means of collecting information were especially useful, HUMINT was usually key. In Bosnia, the man and woman on the ground collecting firsthand information about political leaders, business people, the condition of roads and bridges, withdrawal of forces from the ZOS, weapons and ammunition in cantonment areas, freedom of movement violations, and demonstrations and ethnic incidents proved invaluable. Over time, HUMINT became the dominant player in the IFOR intelligence operation.

The other intelligence disciplines proved important as well. SIGINT provided warning and a hedge against conventional threats. IMINT used the full spectrum of traditional assets from handheld to U.S. national to monitor verification sites and for the surveillance of “hot spots” and FWF compliance activities. There were also some non-traditional IMINT sources such as the Combat Camera Crew products, the AH-64 gun camera tapes, and the OH-58 cockpit tapes that proved invaluable. In addition, downlinked UAV imagery provided near real-time surveillance support. Many areas had land mines or were difficult to access from the ground; hence, the use of the advanced surveillance and reconnaissance capabilities avoided the need to put soldiers in harm’s way. OSINT provided indications and warning of increased tensions in local areas, supported predictive analysis efforts, and helped focus other collection efforts. The “Night Owl,” which was produced by the United

States at Camp Lukavac in MND(N), provided a daily summary of news and media commentary—a Bosnia version of the Pentagon’s “Early Bird.” Through its publication and use, commanders and staff were able to gain a better appreciation for the political, economic, and cultural environment. MASINT was used to support treaty compliance, early warning, and force protection.

The cumulative effect of the intelligence operation sent a clear signal to the FWF that IFOR was capable of knowing all and seeing all—Information Dominance. The U.S. military’s phenomenal array of technology on the ground, in the air, and in space helped keep a risky operation relatively casualty-free. The counter-intelligence and HUMINT activities in Bosnia were also essential to accomplishing the force protection mission by providing the information and intelligence the commander needed to manage and avoid risk and still accomplish the mission.

Civil-Military Aspects

The real “peacekeepers” in a peace operation are the humanitarian relief organizations that provide aid for the present and hope for the future. They are there before the military arrive, remain during the military presence, and stay after the military leave. Although Bosnia was a mature theater of operation for them, the military planners gave little (minimum) consideration to their experience, expertise, and activities in preparing for the IFOR operation. As a result, the military support to the humanitarian aspects of the operation was more reactive than proactive, especially during the early stages of the operation.

Military interaction with civilian organizations was more than civil-military cooperation. Civilian agencies (NGOs, PVOs, and IOs) had developed a network of influential contacts, compiled historical and specialty archives, and established relationships with local leaders and business people. They understood the infrastructure of the region, as well as the political and economic influences. These civilian agencies and centers of operation were both sources and consumers of intelligence information.

The humanitarian relief organizations tend to have limited communications and information system capabilities, especially in the theater of operation. Typically, they will use the in-country telecommunications infrastructure to the extent possible but many also have their own HF and/or VHF radios. These radios, however, may or may not be interoperable with the military systems they come in contact with during peace operations. In Bosnia, the NGOs/PVOs/IOs had reasonably good communications capabilities since many had already been in country for at least 4 years. They had access to the UN system and some of the regional PTT services in the country could be used as well.

Communicating and sharing information with the NGOs/PVOs/IOs was a new experience for NATO. The humanitarian relief organizations bring with them cultural and language differences that need to be understood and dealt with by the military in order to avoid misunderstandings, unnecessary competition, and mistrust. The need for the military and civil organizations to work together toward a common goal in Bosnia was not fully appreciated by the military at the outset. The emphasis by IFOR and the U.S. forces, in particular, on the military aspects of the Dayton Accord inhibited early progress in developing the civil dimension. Many of the new civilian agencies such as the OHR were consumed with problems in setting up their own organizations and cooperation with IFOR was not their main concern.

Civil-military activities prior to IFOR were very narrowly conceived by NATO and were generally regarded as “rear area” activities associated with host-nation logistic support and alleviating refugee interference with military operations. This combat-oriented doctrine had little relevance in the Bosnia context. The essence of the IFOR mission was to maintain a safe and secure environment so that reconciliation and reconstruction could take place. Since mission accomplishment depended upon effective civil-military cooperation (CIMIC), such cooperation and the CIMIC organizational element, in particular, became a vital “front line” asset. Widespread civil-military coordination and cooperation did not really occur un-

til the May 1996 time frame. To quote Admiral Leighton Smith, COMIFOR, “In November we never heard of CIMIC. We had no idea what you did. Now we can’t live without you.”

Accommodating Differences

Coalition peace operations are accompanied by other doctrine, cultural, and language differences that challenged the overall coordination of the mission and ability to achieve unity of effort. Although a common language (such as English or French) was needed to participate, many of the players were not able to speak or understand the language used, placing an added burden on the coordination activities.

In Bosnia, PSYOP and CIMIC doctrines differed. The U.S. approach to PSYOP was to centrally manage and control at the highest level of command, whereas other nations such as the United Kingdom favored delegation to lower levels of the command structure, e.g., division headquarters. For CIMIC, there was no common understanding or approach at the outset of the IFOR operation. The ground commanders lacked a basic understanding of the role and value of CIMIC. This lack of understanding led to misperceptions that the CIMIC activities were contributing to mission creep and resulted in some unanticipated constraints being placed on their operation until their value became more apparent to the commanders. Unofficial doctrine and practices were essentially developed as the operation progressed. In the end, both the PSYOP and CIMIC operations were run out of their respective headquarters in Sarajevo.

Finally, with more than 30 different nations participating, it was a significant challenge to merge the cultural perspectives to achieve unity of effort and avoid cultural clashes. Liaison activities became very important and were used effectively to facilitate coordination and to bridge the language gap.

Putting the IFOR C2 Structure Together

NATO's ability to influence events during the early preparation for IFOR deployment helped avoid problems encountered by UNPROFOR and ensured a clearer definition of military tasks under a unified chain of command. Consequently, the language hammered into the General Framework Agreement made it clear that IFOR would "operate under the authority of and subject to the direction and political control of the North Atlantic Council through the NATO chain of command." UNSC Resolution 1031 provided NATO with the mandate and the necessary political authority to direct NATO and non-NATO forces under IFOR. However, NATO's robust military terms of reference highlight the paucity of authority for the civil activities of the High Representative—the weak link in the implementation of the Dayton Accord. In any future operation that depends on the success of both military and civil tasks, NATO will want to ensure that its civil counterpart also enjoys a commensurate amount of authority to fulfill its responsibilities.

The lack of unified political direction for the overall peace implementation process was a risk to the success of IFOR. The General Framework Agreement established three structures for implementation: an Implementation Force for the military aspects, a High Representative to coordinate civil tasks, and Donors Conferences to stimulate reconstruction. Given the UN's reluctance to take the lead, there was no internationally recognized political organization providing overall political direction. Consequently, the three structures remained virtually autonomous, operating within a loose framework of cooperation and without a formal structure for developing unified policy. The absence of a standing political organization with which the North Atlantic Council could coordinate policy exacerbated the inherent difficulties of synchronizing the civil-military implementation of the peace process at the strategic level and NATO's role in implementing the Peace Agreement.

There were some NATO and U.S.-related command arrangement shortfalls. Command and control differences existed between SHAPE and AFSOUTH/IFOR and between IFOR, the ARRC, and

the Multinational Divisions, the most significant being with the U.S. MND(N). There was the need for a better definition of the command relationships between NATO, USCINCEUR, and USAREUR. Forces in a multinational environment operate with two chains of command: one for operations and the other for command, administrative, and logistical matters. The absence of a clear definition led to some inefficiencies and confusion during the operation. At the center of this issue was how the Army (Component) fulfilled its Title 10 responsibilities. The root cause of the problem was the absence of a U.S. Joint Task Force command equivalent that had the authority, expertise, and staffing to sufficiently provide U.S. C2 and coordinated logistics for out-of-sector U.S. service members. In addition, in accordance with National Security Decision Directive 130, the U.S. PSYOP forces were not placed under IFOR C2. These forces remained under USEUCOM control. This caused some problems in the product coordination and approval process and limited the flexible use of PSYOP elements at the tactical level. The U.S. Civil Affairs and IFOR/ARRC CIMIC elements experienced command and control problems as well. Furthermore, having two headquarters (IFOR and ARRC) in the same local area of operation created problems not only for CA/CIMIC activities but also for the Public Information Offices too. Another important C2 shortfall was inadequate early coordination with humanitarian organizations, particularly the NGOs and PVOs already in country.

IFOR Command Arrangements

The AFSOUTH was made the operational-level headquarters for *Operation Joint Endeavor*. However, AFSOUTH was neither staffed nor equipped to lead an expeditionary land force into combat. The ARRC, NATO's rapid reaction force, was established as IFOR's corps-level land component command. The three framework nations (the United States, United Kingdom, and France) formed the basis for the multinational divisions (North, South West, and South East, respectively). OPCON and OPCOM of the divisions were also assigned to the ARRC. IFOR headquarters was

split between Naples and Sarajevo and the ARRC's headquarters was located at Ilidza near Sarajevo, placing two major command headquarters within a few miles of each other. The U.S.-led MND(N) was the largest division and included brigades from Turkey, Russia, and a third non-U.S. brigade referred to as the NordPol brigade (made up of troops from Finland, Sweden, Norway, and Poland). The British-led MND(SW) was built around a British brigade along with troops from Canada, the Netherlands, and Denmark. Finally, the French-led MND(SE) was the smallest division and was comprised of troops from France, Italy, and Portugal. Both the British and French already had a large number troops in Bosnia in support of UNPROFOR and the Rapid Reaction Force. Hence, the bulk of the deployment activities for IFOR were the NATO command unit forces, the U.S. forces, and the forces of the non-NATO participating nations.

Maritime and air operations were run through COMNAVSOUTH, COMSTRIKFORSOUTH, and COMAIRSOUTH. The command of air operations was achieved by designating the IFOR Air Component Commander as the Joint Force Air Component Commander. A single-layer C2 structure was established at the CAOC in Vicenza, Italy, and was responsible for the entire air effort, simplifying the C2 for air operations. Collection management authority for aerial intelligence platforms (such as Predator) was a CAOC responsibility as well. The IFOR Regional Air Movement Control Center that was collocated with the CAOC exercised airlift movement control. This facilitated coordination with the other air operations. The air tasking process brought together all of the different tasking requirements and unified them in a single order, the Air Tasking Message.

The U.S. SOF established a Special Forces operating base in San Vito, Italy, and a forward operating base in Sarajevo under IFOR. Liaison control elements were assigned to coalition and NATO units to integrate intelligence, operations, communications, close air support, and medical evacuation. SOF also assisted in surveying and monitoring the zone of separation, supported civil-military activities, and provided liaisons with the FWF. Commander,

Special Operations Command Europe (also Commander, Special Operations Forces, IFOR) assumed OPCON of all SOF elements in support of *Operation Joint Endeavor* except for SOF afloat, PSYOP, and CA forces. U.S. PSYOP forces remained under USEUCOM C2 and CA forces under USAREUR command. As noted earlier, the command relationships of the U.S. PSYOP and CA forces were not clearly defined at the outset of the operation and this caused problems for the deployed forces. There was a Combined Joint Special Forces Operations Task Force located in Sarajevo which the U.S., UK, and France SOF elements supported. The United Kingdom and France also had their own national SOF units supporting MND(SW) and MND(SE) respectively.

An IFOR Commander for Support (C-SPT) was established in Zagreb, Croatia. His responsibilities included coordinating the sustainment, movements, medical, engineering, and contracting operations of the national logistic elements; and commanding selected IFOR units in support of the deployment, execution of peace implementation, and redeployment of IFOR. C-SPT was also designated as the single point of contact for all IFOR matters pertaining to relations with the Croatian government. The NATO Maintenance and Supply Agency (NAMSA) established a field office in Split, Croatia. They were responsible for all NATO common-funded contracting and contracting for all scarce resources in theater. They provided liaisons with C-SPT and the framework division headquarters. NAMSA headquarters in Luxembourg held all contracts for the theater. The ARRC COSCOM commander was designated the COMMZ Forward Commander and was located in Split, Croatia, as well. He was responsible for reporting movement into theater to C-SPT. Finally, three National Support Elements were established to support the framework nations' movement activities: the United States in Kaposvar, Hungary, the British in Split, Croatia, and the French in Ploce, Croatia.

Special Arrangements

Some of the IFOR C2 relationships were politically driven. For example, a special agreement was required between the U.S. Secretary of Defense, William Perry, and the Russian Minister of Defense, Pavel Grachev, for the employment of Russian forces in IFOR. This agreement provided SACEUR (General Joulwan) control of the Russian brigade through the Deputy Commander of IFOR for Russian Forces, Colonel General Shevtsov. COMARRC exercised tactical control (TACON) of the brigade through the Commander MND(N) in whose area the brigade operated. OPCON remained with the Russian chain of command. As with other politically dominated C2 structures, this arrangement would be problematic under stress, particularly if new missions were required. It did, however, initiate military cooperation between Russian and NATO forces.

IFOR established a Joint Military Commission (JMC) as the central body for commanders of military factions to coordinate and resolve problems. Two or more FWF military representatives (usually commanders) attended meetings under IFOR supervision to coordinate joint activities, disseminate intent and instructions, and resolve differences. COMIFOR delegated routine JMC chairmanship to COMARRC who issued instructions to ensure the parties' compliance with the military aspects of the GFAP. Below the COMARRC level, the MNDs, their subordinate brigades, and battalions established subordinate military commissions. At these lower levels, the JMC activities included disseminating policy, issuing instructions to factions on policies and procedures, coordinating GFAP-required actions, resolving military complaints or questions, coordinating civil-military actions where appropriate, and developing confidence-building measures between the parties.

The integration of the Partnership for Peace (PfP) nations and other non-NATO nations under NATO C2 was a success for several reasons. First, NATO already had experience dealing with the PfP nations through the NATO PfP Program and related exercise activities. Second, innovative command arrangements were

employed at several levels. For example, national officers were brought into the multinational HQs and senior national officers were “dual hatted” as deputy commanders.

The command arrangements for the Public Information Office (PIO), PSYOP, and CIMIC operations and some aspects of the intelligence operations (e.g., CI/HUMINT) also required innovative adjustments to effectively integrate them into the overall IFOR command structure and operation. OPLAN 40105 called for PIO and coalition press and information centers with each of the major IFOR headquarters. In Sarajevo, IFOR and the ARRC decided to share a single press center located in the Holiday Inn but this caused confusion in the chain of command because of the dual command relationship and sometimes conflicting guidance. At the multinational divisions, the commanders preferred to bring their own national PI assets to run the PI program and this too introduced some confusion into the IFOR PI operation due to conflicting IFOR and national doctrine, procedures, and guidance on the nature and amount of information to be released to the media.

Putting the IFOR C4I Puzzle Together

In spite of formidable obstacles and a somewhat chaotic beginning, NATO and its member nations installed and operated the largest military-civil Communications and Information Systems (CIS) network ever built to support a major peace operation.

NATO had never attempted peace enforcement. Consequently, there was no doctrine, experience, or accepted practices to guide CIS planning and implementation—the NATO CJTF was just a concept and not doctrine. Furthermore, there were multiple NATO and national CIS organizations involved in the planning, implementation, and management activities related to the IFOR deployment. AFSOUTH and SACEUR OPLANs reflected differing perspectives on CIS network management. The Dayton Agreement assigned frequency management responsibilities to IFOR even though NATO had no established capability. These factors contributed to CIS

organizational problems at the outset for the IFOR CJ6. As a result, it was necessary to create a Theater Frequency Management (TFM) capability to address the Dayton Agreement tasking and a Combined Joint Communications Control Center (CJCCC) to facilitate NATO and national coordination and focus the planning and management of the CIS aspects of the IFOR operation.

Dynamic Requirements Base

The communications and information needs of operations such as the Public Information Office, IFOR Information Campaign, Engineers, PSYOP, CIMIC, CI, and HUMINT were not completely formulated or necessarily fully understood at the outset of the operation. The need to be able to interface with and provide some limited support to the NGO/PVO/IO community was also underestimated. Therefore, the requirements were not adequately articulated to the CIS planners and providers so that the necessary services could be made available at the outset of the operation to support these activities. The CJCIMIC operation in the Burger building in downtown Sarajevo only had a few local telephone lines to conduct business in the early stages of operation. If they needed information services or a broader IFOR communications capability, they had to go to IFOR headquarters at the Tito Residency several blocks away. The CIMIC and some HUMINT operations vehicles lacked radios for communicating while operating in the countryside. The engineers also generated a requirement for force protection communications since they too were frequently scattered throughout the country.

Established NATO policy precluded the use of the Internet for operational purposes. However, the engineers and legal and medical personnel needed to use the Internet to access reference material. The PIO also needed Internet access for media interaction and more effective communications and information services to be able to quickly inform the chain of command of media-related, time-sensitive issues. The PIO could use the Internet to get English trans-

lations of Croatian and other international press releases and news articles. The NATO policy makers were slow to make a change regarding the use of the Internet.

The timely distribution of Combat Camera and CI/HUMINT digital camera and other video products was a problem faced early on in the operation. Adjustments had to be made to accommodate these needs. One of these adjustments was the integration of the U.S. CI/HUMINT commercial notebook computer-based data acquisition, management, and communications system into the SIPRNET—the capability is referred to as TRRIP. Linking the U.S. MSE network with the SIPRNET via Trojan Spirit provided broader bandwidth connectivity to the battalion level for TRRIP and other intelligence users and over time significantly enhanced the operational effectiveness of the CI/HUMINT teams in particular.

Extension of NATO CIS Capabilities

NATO's existing CIS infrastructure was not able to satisfy the requirements for this first out-of-area operation. The so-called NATO CIS Contingency Assets Pool (NCCAP) concept, which envisaged a core of deployable and earmarked national equipment, pre-authorized funding for contingency purchases, and use of national assets, was not sufficiently mature to support the operation. Significant enhancements were needed to extend NATO systems to the deployed forces and to improve the in-area CIS capabilities. Heavy reliance was placed on the framework nations' tactical CIS assets, particularly those provided by the United States, and the lease of PTT/IDNX connectivity by NATO to extend services into Croatia initially and later into Bosnia. Pragmatic and unconventional steps were taken to procure CIS capabilities. In addition, service was leased from the UN VSAT telecommunications network, which was already in operation in Bosnia and Croatia, and used by IFOR to support both the deployment and sustainment phases of the operation. Other systems and services were acquired through "emergency" acquisition procedures and leasing.

CIS support for air and naval operations remained in place following *Deny Flight*, *Decisive Force*, and *Sharp Guard* and did not require special efforts to integrate them into the IFOR operation. There was a similar arrangement for the Special Forces CIS support. Although a Reserve Force was never allocated to IFOR, the U.S. Marine Expeditionary Unit offshore remained an option and had to be considered in the development of the CIS architecture.

Due to the lack of Bosnia telecommunications infrastructure and cross-IEBL connectivity, mountainous terrain, and high cost of clearing land mines and providing force protection for mountain-top radio relay sites, an extensive tactical military satellite communications network was deployed to provide the required connectivity into the area of operation. The network used U.S. and UK national tactical satellite ground terminals that were placed in or near urban areas where the headquarters facilities were located and were provided force protection commensurate with these facilities. NATO only had one TSGT at the time of deployment and it was deployed to Sarajevo to support HQ IFOR. As the operation evolved, commercial VSAT services were extended into the Bosnia area of operation as well.

Unanticipated Training and Contracting Considerations

For any military operation, a certain amount of “learning on the job” is expected. However, the deployment into a generally urban environment, coupled with the extensive use of commercial products and services, created a need for more intensive on-the-job-training than had been anticipated. The CIS staff had to be prepared to operate in both a fixed (rewire buildings for telephone and LAN services) and tactical environment. In many cases, it was necessary to pull tactical equipment out of the vans and install it in a commercial office-like environment. Staff was required to operate across multiple disciplines (e.g., pull cables and install LANs). The use of commercial technologies such as VSATs, IDNXs, VTCs, ROUTERS, digital switches, and other data network products and

services added training requirements. In fact, it was necessary to establish a special training program at the NATO Latina training facility for the IDNXs.

Dealing with contractors and the Croatian and BiH PTTs also provided new challenges. Both the military and the contractors were on steep learning curves. Inadequate spares were purchased for equipment procured under emergency procedures and the repair time for assets under warranty was excessive. In the early phases of the IFOR operation, CIS was in a permanent state of flux. CIS personnel at all levels worked on improving the CIS infrastructure with remarkable enthusiasm and initiative. The success of the CIS implementation and operation was, to a large degree, due to their abilities and dedication.

The IFOR C4I Puzzle

In preparation for the execution of OPLAN 40104, the extraction of UN forces, a leased E1 (2mb/s) network was extended by SHAPE/NACOSA into Croatia and the United States into Hungary. By the end of May 1995, an IDNX-based strategic backbone information network was fully operational. The NATO TSGT was deployed to Camp Pleso (Zagreb) and used to extend SHAPE headquarters voice, message, and data services to the Zagreb area through the use of the REPLICA system, a SHAPE reach-back capability. With the signing of the Dayton Peace Agreement on 14 December 1995, the mission changed and Croatia and Hungary became the embarkation points for NATO and national troops deploying into the region. OPLANs 40105 and 10405 provided the guidance for the deployment of these forces and the supporting CIS infrastructure.

A complex mixture of NATO, national, UN, and civilian and commercial networks and components provided IFOR CIS services (i.e., voice, message, data, and VTC services). National tactical equipment was used to establish the core IFOR telecommunications infrastructure. The U.S. TRI-TAC system provided a large portion of the strategic- and theater-level telecommunications infrastructure supporting organizations such as SHAPE,

AFSOUTH, IFOR, C-SUPPORT, COMMZ, and the NSEs. NATO also provided some. The UK tactical system, PTARMIGAN, provided the telecommunications support for the ARRC and between the ARRC and the MND headquarters. The United States, United Kingdom, and France used their tactical systems to support division-level communications including service to those forces assigned to their divisions. TRI-TAC/MSE equipment was employed in support of MND(N) and the U.S. NSE in Hungary. PTARMIGAN was used to support MND(SW) and the UK NSE in Split. French tactical systems already in place were used to initially support MND(SE). The tactical system RITA was deployed in the March 1996 time frame to provide additional support to MND(SE) and its NSE in Ploce. The Italian system, SOTRIN, supported the Italian brigade in MND(SE) and the German tactical system, AUTOKO, supported the German contingent in MND(SW). The data and VTC networks were largely derived from commercial products and services. Commercial VSAT and IDNX products and services supplemented the tactical satellite backbone connectivity provided by the U.S. and British tactical satellite systems.

STANAG 5040 was employed to provide an analogue interface between the national tactical and strategic voice networks, between TRI-TAC and the NATO strategic voice network, IVSN, and between TRI-TAC and the commercial networks such as the UN VSAT and the Bosnia and Croatian PTTs. The Interim Digital Interface PTARMIGAN (IDIP), designed by the United Kingdom for this operation, provided a digital interface between PTARMIGAN and the TRI-TAC/MSE systems. STANAG 5040 was used for the TRI-TAC to RITA interface as well as by SOTRIN and AUTOKO interfaces with RITA and PTARMIGAN respectively.

The NATO CRONOS Wide Area Network and the Interim ARRC CIS network (both client-server architectures, employing Microsoft Office for office automation and providing M/S e-mail service) provided valuable crisis response and command and control capabilities for the IFOR operation. However, they lacked common standard operating procedures and needed more efficient network management. VTC was used extensively by IFOR and the

ARRC and as time went on, it became a key element in conducting business. VTC was also the C2 system of choice for the U.S. Army forces.

INMARSAT was used extensively and commercial cellular services were available in some areas of Croatia and towards the end of the IFOR phase of the operation in the Sarajevo area as well. Unclassified Internet was also used frequently and demands for service increased throughout the operation. Internet use by NATO, IFOR, and national elements was not planned; its use simply grew with user demand. An interesting side note, the Internet was used by the factions to tell their story (e.g., Serbs used it for their disinformation campaign). The UN and humanitarian relief organizations also made extensive use of the Internet to inform the international community of their actions.

The U.S. LOCE system was extended to division headquarters level and above to support IFOR intelligence needs. Nations also provided national intelligence support and services to IFOR through liaison officers and National Intelligence Cells (NICs). A mixture of prototype and operational systems were used in an attempt to fuse various land, sea, and air pictures into a tactical picture. The maritime and land pictures provided to the tactical commanders were of good quality. The air picture (referred to as RAP—Recognized Air Picture) in the CAOC, made up from a variety of sources, was of particularly high quality. However, there was no overall integrated maritime/air/land picture. The CRONOS network was used to distribute the RAP to the IFOR C2 nodes.

Network and system management of IFOR's communications and information networks proved to be a major challenge. An IFOR CIS organization structure had to be created, agreed upon, and staffed quickly. The U.S. Joint Pub 6-05 provided the basis for the establishment of the CJCCC to plan and manage IFOR's networks. System tools had to be acquired to monitor and manage the networks. There were multiple NATO and national players (e.g., SHAPE's NATO CIS Operating and Support Agency (NACOSA), the AFSOUTH ACOS CISD, the IFOR CJ6, the CJCCC, the ARRC

G6, the MND G6s, and national J6s) whose roles and relationships needed to be established and their activities in support of the operation coordinated.

C4I Integration and Interoperability Considerations

There were overlaps in network and system management organizational responsibilities that needed to be worked out since the distinction between strategic, theater, and tactical became blurred. NATO communications and ADP were managed separately and this needed to be accommodated by the CJCCC. There were stove-piped network implementations that had to be accommodated as well. The NATO and national C4 and I and national ISR systems were managed separately. Coordination and collaboration became key ingredients in the evolution of the IFOR network management structure and capabilities. Over time, these issues were resolved and the CIS system provided reasonable services. However, the CIS system for the most part was never heavily stressed during the IFOR operation. Therefore, the performance of the networks and the supporting management organization were never tested under more hostile or stressful conditions.

Historically, interoperability has been one of the most difficult areas to deal with and this operation was no exception. The analog-based STANAG 5040 was still the norm for interfacing strategic, theater, and tactical voice systems. No digital interface existed for interfacing strategic and tactical networks. The TTC-39D experienced interface problems with the Ericsson MD-110 switch used by the UN and IFOR. The STU-IIB is a NATO-approved secure voice equipment and was used extensively by IFOR. A large number of the U.S. forces that deployed to Bosnia brought with them STU-IIIs that were not interoperable. The Interim Digital Interface PTARMIGAN (IDIP), designed by the United Kingdom for this operation, was used to provide a digital interface between the UK PTARMIGAN and the U.S. TRI-TAC/MSE tactical systems. The IDNX deployment required the certification of some 50 interface arrangements.

There were no automated interfaces between the IFOR data networks (CRONOS, IARRCIS, and LOCE) and national networks. The CRONOS was not interfaced with LOCE or the ADAMS networks even though information was manually transferred between the systems. The main reason for this was security considerations. There were no approved secure guard gateways that could accommodate an automated interface. The ADAMS movement control system and JOPES required a manual interface for exchanging information. U.S. intelligence processing systems used at echelons above corps (EAC) did not “talk” to the echelons at corps and below (ECB) systems. To fix the problem, some EAC systems such as the U.S. Joint Deployable Intelligence Support System (JDISS) had to be deployed to ECB intelligence centers. Exercises such as *INTEROP 95* and *Mountain Shield* helped to work out many of the integration and interoperability issues in advance of the deployment and also provided excellent training for the organizations that deployed in support of the operation. However, while interoperability is improving, there is still a long way to go to achieve seamless integration of CIS systems and services.

IFOR Information Services

The pervasive use of COTS information products and services propelled NATO and IFOR into the Information Age and a new way of doing business. There was extensive use of e-mail and a reduced reliance on formal messaging. The formal message traffic (the NATO TARE message network) by volume (megabytes per day) was less than 10 percent of the total IFOR daily data network traffic. The VTC was used daily by IFOR and ARRC command elements for collaboration and coordination. For USAREUR and its deployed commanders, VTC became the C2 system of choice. The VTCs were also used by subordinate command elements to conduct day-to-day business. PowerPoint briefings were the medium of choice for presentations and were readily distributed over the data network. A cottage industry of “PowerPoint Rangers” emerged, as the presentations became very sophisticated. The brief-

ing packages frequently exceeded a megabit in size and placed heavy loads on the data networks as they were distributed around the theater. The data networks were also used for collaborative planning and distribution of wide-band information such as images.

The new capabilities provided the opportunity to share information efficiently and nearly simultaneously at all levels of the command structure. This was a vast improvement over the previous procedures, requiring the corroboration of data successively reported through each level in the chain of command. It was also possible to exchange information that bypassed (“skip echelon”) intervening levels of the command structure. The ability to electronically bypass levels of command to obtain information first-hand was occasionally used in the interest of expediency and providing information up the chain of command but sometimes at the expense of leaving others in the dark.

Managing all of the information available to the commander and his staff was a serious problem. Users did not have adequate tools to search for available information. Likewise, there were inadequate tools for managing information collection, storage, and distribution. This was particularly true in the area of coordinating, integrating, and fusing intelligence, surveillance, and reconnaissance capabilities and making this information available to the user. There were other sources of information such as the Internet and local and international media that needed to be incorporated into the IFOR information database. In terms of sharing classified information, security releasability was also an issue that needed to be addressed early in the operation to ensure that information was given to those who needed it in a timely way without revealing sources and methods, but stringently protecting highly sensitive information. There were 36 coalition partners, some of which NATO had never shared classified information with before. A special category, IFOR-releasable, was established for the operation.

Although extensive use was made of e-mail, VTC, and data network services, voice communications still played a major role in conducting the IFOR information operation. This was true in spite of a grade of service that, at times, exceeded a 20-percent probab-

ity of blocking for call attempts. In addition, the end-to-end voice quality was marginal if the call had to be routed through several different tactical switched networks.

The IFOR information revolution largely stopped at the division level in Bosnia. In some cases, such as MND(N) and for the U.S. forces in Croatia and Hungary, higher bandwidth services were extended to the battalion. Every U.S. base camp had telephone service and secure and non-secure data and e-mail capabilities. The U.S. intelligence community extended 128kb/s service to brigades via Trojan Spirit II deployments to the brigade level. On the other hand, the communications and information system support to the IFOR warfighter, in general, changed little and they continued to operate much as they had in the past. Operations were conducted using acetate-covered 1:50,000 maps (seen in all command centers), outmoded tactical equipment, and sensor or reconnaissance systems organic to the national ground units. The command centers were located in urban buildings, tents, semi-destroyed buildings, or the back of armored vehicles.

Although the deployed high-technology systems generally supported the headquarters far more effectively than they supported the soldier on the ground, there were exceptions. Many innovative uses were made of the U.S. military's array of advanced technologies (mainly in the areas of ISR) to more effectively support both the headquarters and the soldier on the ground. In fact, Bosnia became a model for the U.S. doctrine known as Information Dominance. The operation also became an advanced information system technology test bed for both NATO and advanced technology-driven nations such as the United States.

IFOR CIS Commercialization

IFOR commercialization efforts came in several forms. First, commercial products and services were used to augment the military systems deployed, as was the case with the IDNX and VSAT. The NATO data network CRONOS and the U.S. data networks NIPRNET and SIPRNET were based on commercial products and

provided the strategic- and theater-level information services required for C2 operations. The NATO and U.S. VTC networks were also based on commercial products. Commercial products and services were also an integral part of advanced technology capabilities deployed to theater, e.g., the U.S. BC2A/JBS information services and broadcast network. Commercialization played a role in the IFOR exit strategy and was used to replace tactical military telecommunications systems with commercial products and services.

The use of commercial products and services had its challenges. Competitive bidding did not always realize the best product for price. Contracting arrangements differed among the different factions. There were no Radio Shacks/Tandys to buy spare parts or urgent capabilities. Maintenance support was complicated both in terms of adequacy of repair facilities, excessive repair cycles for assets under warranty, ready access to spares, and quality and use of vendor maintenance personnel. The latter included ethnic constraints such as the inability to easily use a Croatian maintenance person in a Serb area. Most vendors in theater would deal in cash only. Documentation and training packages in many cases were inadequate. Integration of commercial and military systems was not always straightforward. In spite of these difficulties, commercial products and services were used extensively and in many cases quite successfully.

IFOR's plan for the commercialization of their communications network was aimed at reducing the costs to NATO, allowing for the timely withdrawal of tactical systems, and reducing IFOR's dependence on the UN VSAT network. The plan was to install ERICSSON MD-110 digital switches at the major headquarter locations, expand the commercial VSAT/IDNX network, and lease E1 connectivity from the Croatian and BiH PTTs where available. The evolution of the commercial network (referred to as the IFOR Peace Network (IPN)) was slower than IFOR would have liked. The main difficulties centered on the slow reconstruction of the BiH PTT infrastructure and the continued unwillingness of the FWF PTTs to provide cross-IEBL connectivity.

The United States also had major commercialization efforts in Taszar and Kaposvar, Hungary, and Tuzla, Bosnia. In both the NATO and U.S. commercialization initiatives, a tactical military overlay system remained to support essential C2 requirements.

Some Unintended Consequences

There were unintended consequences associated with the TOA to LANDCENT and the removal of the ARRC CIS systems. The UK EUROMUX tactical system and the U.S. MSE tactical system did not replace the functionality of ARRC's PTARMIGAN system, e.g., secure voice conference capability and secure SCRA. The UK IARRCIS and THISTLE information systems, which were used by the ARRC to build and distribute the ground order of battle and other C2 and intelligence information, were pulled out and replaced with the NATO CRONOS and its prototype C2 and intelligence applications PAIS and CRESP. The ARRC's geographic support, which provided the map and boundary databases used by all IFOR command elements, was not removed but arrangements had to be made with the United Kingdom to lease the system to NATO. And finally, the CIS capabilities of the Allied Military Intelligence Battalion were also impacted by the withdrawal of ARRC equipment. These capabilities all required replacement to adequately support the SFOR operation.

Opportunities for Behavior Change— Lessons Learned

According to the Center for Army Lessons Learned, "A lesson is learned when behavior changes." Many of the IFOR experiences were not new and therefore were lessons yet to be learned. A major factor contributing to this situation was the inability to effectively share lessons already learned. The process is flawed. This point was made many times over by those interviewed by both the NDU/CCRP study team and the IFOR JAT. Frequently the

observation was made, “if I had only known this before I deployed.” Today’s information technologies certainly provide the means for enhanced collaboration, sharing, and knowledge building. For example, IFOR-related home pages on INTELINK (e.g., EUCOM and INTEL community) and the commercial Internet (e.g., IFOR, SHAPE, and Task Force Eagle) are excellent examples of capabilities in place to serve selected community needs. The real issue is one of community will, and of who assumes the leadership role to put such an enhanced capability in place to serve the broader community needs as a whole.

Certainly NATO and the participating nations have learned a lot from the IFOR experience. Some experiences have particular significance for future NATO operations and the realization of the NATO CJTF and NCCAP concepts. Others can be applied to coalition peace operations in general. Whether these experiences become lessons learned is yet to be determined, but some of the more important IFOR-related experiences to be considered are as follows.

- Warfighting and peace operations require different skills and capabilities. The go-to-war oriented doctrine, CONOPS, tactics/techniques/procedures, C4ISR capabilities, and intelligence operations had to be adapted to meet IFOR peace operation requirements.
- Information operations require a comprehensive and integrated strategy from the inception of the operation.
- The division of strategic, theater, and tactical became less distinct for—
 - C4ISR systems and services
 - Intelligence operations
 - Information Campaign
- The Information Age arrived and significantly changed the way NATO and the military conducted operations:
 - E-mail replaced the formal message handling systems

- VTC was used extensively for C2 and decision making
- PowerPoint briefings were the medium of choice for presentations
- Enhanced collaboration and information sharing took place

- In spite of progress, interoperability continues to be a challenge:
 - C4ISR systems and services (military and civil systems)
 - Intelligence operations
 - Doctrine, CONOPS, and TTP
 - Language differences
 - Cultural differences
 - NGO and IO interfaces

- The size of communications pipes was not sufficient to meet the demands of the Information Age operation (problems were experienced at all levels—strategic, theater, and tactical).

- Coordinated public affairs, civil affairs, PSYOP, and CI/HUMINT initiatives demonstrated synergistic value-added for intelligence operations and the information campaign in support of peace operations.

- Civil Affairs came of age, especially for NATO and the framework nations the United States, France, and the United Kingdom.

- CI/HUMINT became the intelligence source of choice for the tactical commanders.

- PSYOP use of leaflets, loudspeakers, and radio broadcasting has been overtaken by global television for “information societies.” The Internet has also emerged as a player.

- News media influence on peace operations—the “CNN Effect”—was experienced from the outset of the operation and must be accommodated by the military.

- Information Dominance was achieved and demonstrated. Commander and staff information overload was also demonstrated. This was especially true for the U.S. forces.
- Implications of modern commercial information technology has yet to be fully understood:
 - Operational C2 and decision making
 - Organizational structures and virtual headquarters
 - Insertion into and substitution for go-to-war capabilities
 - Human factors and use of information
 - Information discovery tools
 - Information protection
 - Lack coalition releasable COMSEC/INFOSEC capabilities
 - Lack configuration management and network virus and intrusion detection/protection capabilities
- Exercises such as *INTEROP 95* and *Mountain Shield* helped to work out many of the integration and interoperability issues in advance of the deployment and also provided excellent training for the organizations that deployed in support of the operation.
- Information management and management of information needs require careful consideration.

Bosnia was, in many regards, a living prototype of a post-Cold War operation. It was the kind of operation we may expect to see more of in the future and if we learn the correct lessons from the operation and act upon them, the payoff could be considerable. One should not forget, however, that potential adversaries of the NATO alliance and the United States, in particular, will not be so foolish as to neglect glaring weaknesses in the C2 and intelligence arrangements and C4ISR systems and services implemented in support of

the IFOR operation. Doctrine and tactics based upon an assumed freedom to communicate and information dominance may not be sufficient the next time around, even for peacekeeping operations.

The experiences from Bosnia reinforced the importance of information dominance and the information campaign as force multipliers in peace operations. The public information campaign and the IFOR Information Campaign in support of force protection and implementation of the military aspects of the Dayton Accords were successes. The IFOR Information Campaign in support of civil reconstruction, economic recovery, and humanitarian activities was less successful. No one organization was responsible for orchestration, an integrated information campaign that addressed the political, civil, economic, and humanitarian aspects of the operation.

The political, civil, economic, and humanitarian aspects of peace operations require close cooperation between the civil organizations and the military. This, too, was reinforced by the Bosnia experiences.

Agility and accommodation continue to be keys to success as well as some plain old good luck. Overall, the IFOR operation was a military success because of the professionalism, dedication, and ingenuity of the men and women who were there and those who supported them.

End Notes

¹CNN World Wide Web home page: The Balkan Tragedy, 1996/7.

²LTC David Perkins, USA, and Mark Jacobson, USAR.

³Col. Kenneth Allard, USA (Ret.), Col. Michael Dziedzic, USAF, Pascale Siegel, and Larry Wentz.

⁴Fellow Travel, an end of tour paper by Tony Boardman, UK, Headquarters SFOR, 1997.

⁵*The World Factbook* 1992 and 1995, Central Intelligence Agency.

⁶“Policing the New World Disorder: Peace Operations and the Public Security Function,” Robert Oakley, Michael Dziedzic, Eliot Goldberg, NDU Press, 1997.

⁷“Policing the New World Disorder: Peace Operations and the Public Security Function,” Robert Oakley, Michael Dziedzic, Eliot Goldberg, NDU Press, 1997.

⁸“Policing the New World Disorder: Peace Operations and the Public Security Function,” Robert Oakley, Michael Dziedzic, Eliot Goldberg, NDU Press, 1997.

⁹Chapter 6, *Bosnia and the IPTF*, Col. Mike Dziedzic and Andy Blair.

¹⁰IDA report: *Operation Joint Endeavor-Description and Lessons Learned*, November 1996.

¹¹Bosnia Country Handbook Peace Implementation Force (IFOR), DoD-1540-16-96, December 1995.

¹²IFOR Fact Sheets and IDA report: *Operation Joint Endeavor-Description and Lessons Learned*, November 1996.

¹³IDA report: *Operation Joint Endeavor-Description and Lessons Learned*,

November 1996.

¹⁴IFOR Fact Sheets and IDA report: *Operation Joint Endeavor-Description and Lessons Learned*, November 1996.

¹⁵There were numerous after action reports, lessons learned briefings, and interviews that served as the basis for this chapter. Those of particular importance were *USAREUR Headquarters After Action Review (1997)*, *After Action Report Operation Joint Endeavor 1st AD Intelligence Production (1996)* (Capt. Rhonda Cook, USA), Center for Army Lessons Learned reports, U.S. Naval War College report on IFOR C4I and Information Operations, Army War College After Action Reviews, JS (J2) BOSNIA Intelligence Lessons Learned Working Group, IFOR Joint Analysis Team reports, SOCOM SOF Mission Support Lessons Learned, USEUCOM Lessons Learned reports, DCI report on IFOR Intelligence Sharing: Successes and Challenges, Defense Science Board Task Force on Improved Application of Intelligence to the Battlefield, Chapters 5 through 10 of this book and their authors and other interviews and reports.

¹⁶The author would like to thank the many individuals who commented on this chapter in its various stages of development and specifically Lt. Col. Bob Butler, USAF; LTC Mike Furlong, USA (Ret.); Col. Dave Hunt, USA; Col. Don Klemm, USA; LTC Dave Perkins, USA; CAPT Wayne Perras, USN (Ret.); and Tom Rausch, MITRE.

¹⁷USAREUR Headquarters After Action Report, *Operation Joint Endeavor*, May 1997.

¹⁸General Framework Agreement for Peace in Bosnia and Herzegovina. Art. I, § 2.

¹⁹General Framework Agreement for Peace in Bosnia and Herzegovina. Art. VI, § 3.

²⁰“Combined Joint Civil Military Cooperation (CIMIC),” Briefing to Admiral T. Joseph Lopez, 24 July 1996.

²¹“Combined Joint Civil Military Cooperation,” IFOR AFSOUTH Fact Sheet, August 20, 1996.

²²David R. Segal and Dana P. Eyre. *U.S. Army in Peace Operations at the Dawning of the Twenty-First Century*. U.S. Army Research Institute for the Behaviour and Social Sciences, May 1996, p. 24.

²³COMARRC Policy Guidance Number 8 - Civil Tasks, March 1996. Page 2, ¶ 4.

²⁴The 96th Civil Affairs Battalion, which was to act as the U.S. CIMIC enabling force, was scheduled to deploy at D-13. Deployment did not occur until D-Day.

- ²⁵We wish to acknowledge the careful scrutiny and incisive suggestions we received on earlier versions of this chapter from Deputy IPTF Commissioner Robert Wasserman, Maj. Don Zoufal, Col. Larry Forester, Jim Hooper, Lynn Thomas, and Glen MacPhail.
- ²⁶Article 1, Annex 11, General Framework Agreement for Peace.
- ²⁷Observations provided by Deputy Commissioner Robert Wasserman.
- ²⁸On 25 Sep 1996, Mr. Ed van Thijn, Coordinator for International Monitoring, publicly asserted that the postponed municipal elections should be put off for at least 4 more months until the minimal essential conditions could be satisfied. OSCE Mission Chief, Amb Robert Frowick, in contrast, has insisted on going forward with the elections in late November. "Monitor Wants Bosnian Elections Postponed," *Washington Times*, 25 Sep 1996.
- ²⁹The "Principals" were the High Representative, IFOR/SFOR commander, IPTF commissioner, and the Special Representative of the Secretary General who leads UNMIBH. In addition to this core group, when the issues of the day concerned the OSCE or the UNHCR, the heads of these organizations were also included.
- ³⁰"Report of the Secretary General Pursuant to Security Council Resolution 1026 (1995), Document No. S/1995/1031, 13 December 1995, p.7.
- ³¹If one does the math, this comes out to 1,492. Presumably the additional 229 monitors were added because of a planning assumption that roughly 13 percent would be sick on leave or otherwise unavailable for duty. It is also worth noting that this figure was not adjusted after the Federation downsized from 32,750 to 11,500. Indeed, some 200 officers were added to create a superstation in Brcko after the decision was made in March 1997 to place that contested city under international administration.
- ³²Kevin F. McCarroll and Donald R. Zoufal, "Transition of the Sarajevo Suburbs," *Joint Forces Quarterly*, Summer 1997, pp. 7-10.
- ³³Memorandum for the Record, Subject: "UNMIBH Logistical Support to IPTF," from D/Chief logistics Officer to IPTF Deputy Commissioner, 29 July 1996, pp. 2 & 9.
- ³⁴*Ibid.*, p. 8. The impact of these logistical shortcomings was also chronicled by an IFOR officer visiting Kiseljak in late June. In his estimation the IPTF station there was "severely under-equipped," the number of vehicles was inadequate, and the commander lacked the means to communicate with officers on vehicular patrols. Consequently, patrolling had been restricted for safety reasons. IFOR Memorandum, 26 June 1996, "Discussion with IPTF Officer in Kiseljak," p. 3.

³⁵Ibid., p. 7.

³⁶Ibid., pp. 4 & 8.

³⁷Op. Cit. in Note 3, p. 7.

³⁸“All shortages reflect the minimum number to marginally accomplish the mission using common assets, and presuming no equipment failures, losses, or repairs.” Ibid., p. 10.

³⁹Ibid., p. 10.

⁴⁰Ibid., pp. 4 & 7.

⁴¹IPTF Memo, “UNMIBH Logistical Support to the IPTF.” p. 7.

⁴²Memorandum for the Director, Joint Logistics Operations Centre, from Chief of the Supply and Services Division, “Support to the UN Mission in B-H (UNMIBH), 27 Jan 95.

⁴³FAX No. 151-2275, from Chief Medical Officer UNTOFY, to SRSG UNMIBH Sarajevo, “Medical Support to UN Personnel UNMIBH/UNIPTF,” 15 Mar 1996.

⁴⁴Interoffice Memorandum to the Special representative of the Secretary General and the Civ-Pol Commissioner, from United Nations Peace Forces Headquarters (FMEDO), “Medical Support to UN Mission Areas in the Former Yugoslavia after 31 January 1996,” 25 January 1996.

⁴⁵Op. Cit. in Note, pp. 1 & 6.

⁴⁶Ibid., p. 6.

⁴⁷*The Dayton Peace Accords*, Annex 1A, Article I, Paragraph 1.

⁴⁸Kevin F. McCarroll and Donald R. Zoufal, “Transition of the Sarajevo Suburbs,” *Joint Forces Quarterly*, Summer 1997, p 8.

⁴⁹*The Dayton Peace Accords*, Annex 11, Article III. In addition, the Report of the Secretary General to the Security Council of 13 December 1995 prior to the deployment of the IPTF states that “.International Police Task Force monitors may be involved in local mediation if conflict arises as a result of actions by local police.” Report of the Secretary-General Pursuant to Security Council Resolution 1026 (1995), Document No. S/1995/1031, 13 December 1995, paragraph 27.

⁵⁰The following incidents, summarized by Somers and Reeves, are illustrative:

An example of such a violation is the groundless, ethnically motivated arrest of the Bosniac police chief of Jablanica by Croat police officers on 18 July

1996 after having been brought to Croat-dominated territory for an official police coordination meeting. The Chief was immediately arrested and detained by Croat authorities in West Mostar. An investigative judge commenced criminal proceedings while the Chief remained in detention. IPTF was required to stand by helplessly and attempt to negotiate his release from this ethnically motivated human rights violation. No form of police disciplinary action or prosecution against these Croat officials has resulted from this incident.

In a separate but equally illustrative incident, the Police Chief of Pale, in the Republika Srpska, while intoxicated in a public restaurant, fired his pistol through the windows and doors while other restaurant patrons were present. He subsequently used his loaded pistol to push another patron out of a chair by pushing the pistol against the patron's cheek. Again, no criminal charges were filed. No police disciplinary action was taken against this officer, even after the IPTF Commissioner wrote a strongly worded letter of protest to high ranking government officials.

The ongoing case of the four Serbs who were reported as missing persons on the Trnovo Road in Federation territory in July 1996 is illustrative of the continuation of ethnic hostilities through abuse of the criminal justice system. These four persons were discovered accidentally by IPTF monitors in October to be in the Sarajevo Centar Jail. They were being held without charges or bail. As of the date of this study, these persons have neither been charged nor released. It appears that the Federation police may have abducted or directed the abduction of these people for the purpose of conducting a future prisoner exchange. It is even more disturbing to note that one of these persons had been seriously wounded in the abduction and was denied medical attention for a significant period of time. Somers and Reeves, pp. 17, 24-25.

⁵¹As the Secretary General noted in his 13 December 1995 report to the Security Council prior to deployment of the IPTF, "Its effectiveness will depend, to an important extent, on the willingness of the parties to cooperate with it in accordance with Article IV of annex 11 to the Peace Agreement." Report of the Secretary-General Pursuant to Security Council Resolution 1026 (1995), Document No. S/1995/1031, p. 7, paragraph 27.

⁵²Somers and Reeves, pp. 17-18.

⁵³The IPTF Commissioner's Guidance calls upon Bosnian police forces to investigate police misconduct and discrimination scrupulously, and to use external auditors to ensure that written policies are enforced in practice and an independent review mechanism for allegations of police misconduct. Commissioner Guidance, pp. 2, 9, 16, 18.

⁵⁴Interview with Maj. Fred Solis, member of the IPTF Special Projects Division,

which had responsibility for the vetting program. September 1996.

⁵⁵Confirmation of the “re-vetting” process as an IPTF power is found in the Commissioner’s Guidance for Democratic Policing in the Federation of Bosnia-Herzegovina, Part 1, May 1996. This document specifically states that all police officers “not selected for duty in that Canton or its Opstinas, or selected for duty at the Federal level, will be demobilized.” P. 5.

⁵⁶AMEMBASSY SARAJEVO Message, Date-Time Group 051727 AUG 97, UNCLASS SARAJEVO 005266.

⁵⁷The training consisted of a 1-week “Human Dignity” course and a 3-week introduction to international policing standards and the reorganized Federation police structure. IPTF Workshop conducted at the National Defense University on 26-27 June 1997.

⁵⁸Pre-election briefing in CIMIC headquarters by IFOR Liaison Officer assigned to the IPTF, 13 Sep 96.

⁵⁹They still had to depend on their own comm net: 73 base radios with 10-mile radius, and 178 hand-held radios, one-mile range.

⁶⁰3 October 1996 Memorandum from LTC Mike Bailey to Amb Oakley, Subject: “To provide you with thoughts regarding the IPTF.”

⁶¹26 September 1996 Memorandum from LTC Mike Bailey to Mr. Michael Arietti, Subject: “Bosnia Trip Report.”

⁶²“Commissioner’s Guidance Notes for the Implementation of Democratic Policing Standards in the Federation of Bosnia-Herzegovina,” in *Commissioner’s Guidance for Democratic Policing in the Federation of Bosnia-Herzegovina* (Sarajevo: United Nations Mission in Bosnia-Herzegovina, 1996), pp. 1-2.

⁶³*Commissioner’s Guidance for Democratic Policing in the Federation of Bosnia-Herzegovina*, (Sarajevo: United Nations Mission in Bosnia-Herzegovina, 1996), p. 1.

⁶⁴Ibid.

⁶⁵Ibid.

⁶⁶“The human rights abuses take many forms, ranging from willful blindness toward enforcing laws to overt criminality. A common form of misconduct is police participation and/or complicity in the kidnapping of members of ethnic minorities in order to amass candidates for the prisoner exchanges which occur on a regular basis with the full knowledge of the international community, including IPTF.” Somers and Reeves.

⁶⁷“The pre-trial period of the criminal process is, in most cases, subject to abuse, fails to conform to the European Convention on Human Rights, and requires the most immediate corrective measures.” “As long as prison officials continue to allow limitless periods of detention of uncharged individuals, without bring this detention to the attention of judicial authorities, rule of law will elude the Entities.” “...we were concerned that approximately 50 percent of judges from Republika Srpska and Bosnian Croat courts were not aware of the European Convention on Human Rights and the fact that the fundamental freedoms set out in it were to be incorporated into the legal system. A common response to questioning on this point was that the system already had appropriate safeguards on the subject of Human rights. We found it did not. We also found in general terms that there was a lack of continuing education for judges and possibly as a result of this, a lack of knowledge on the part of all judges concerning changes in the legal system brought about by GFAP, specifically the role of the Human Rights Chamber and its relationship to the legal system.”

⁶⁸HQ ACE, p. 23, Section 11.1.1.

⁶⁹In this article, the author refers to information activities to describe the coordination and synchronization of public information and psychological operations in support of *Operation Joint Endeavor*. The author chose the term information activities instead of information operations for two reasons. First, NATO does not have an information operations doctrine. Second, according to the U.S. Army’s FM 100-6, information operations refers to operations linking together public affairs, civil affairs, psychological operations, command and control warfare, and electronic warfare. Such encompassing information operations did not take place during *Operation Joint Endeavor*.

⁷⁰Department of the Army, *Field Manual 46-1: Public Affairs*, draft version, November 1996.

⁷¹During UNPROFOR and IFOR missions, major military operations were rare. One of them took place in March 1996, when IFOR seized arms and ammunitions from the Bosnian government. IFOR also seized many documents linking the Bosnian government to Iran. Since then, IFOR military operations have been limited in scope. For example, IFOR is backing up IPTF’s inspections of police stations.

⁷²Colonel Tim Wilton, UKA, ARRC chief Public Information Officer, Sarajevo, October 1996.

⁷³The PSYOP campaign was called IFOR Information Campaign because of po-

litical constraints. During the planning phase of *Joint Endeavor*, it appeared that the term “psychological operations” generated reluctance among some of the partners in the coalition. To ease those concerns, the PSYOP campaign was labeled IFOR Information Campaign. There is, however, no doubt that the IFOR Information Campaign was a PSYOP campaign. The CJICTF only comprised PSYOP personnel and assets and conducted operations according to NATO’s definition of Psychological Activities. Interview with LtCol John Markham, USA, SHAPE PSYOP staff officer, Mons, 19 December 1996.

⁷⁴The PI and PSYOP policies in use at the time of planning were outdated. Both documents dated back to the 1980s and were more relevant to conventional warfighting in central Europe than to a peace operation in the Balkans.

⁷⁵When AFSOUTH and SHAPE began planning for *Joint Endeavor*, two contingency plans already existed: OPLAN 40103 (NATO support for implementation of the Vance-Owen peace plan) and OPLAN 40104 (NATO support for a UN withdrawal from Bosnia-Herzegovina). Both plans were extensive. According to interviews conducted in theater, PI planners relied heavily on annex P to OPLAN 40104.

⁷⁶Some of these concepts were not new and had already been tested in real-world operations (during *Operations Restore Hope* and *United Shield* in Somalia, for example). The requirements and mechanisms were more complex and more comprehensive, however, during *Joint Endeavor*.

⁷⁷ Interview with Capt. Mark Van Dyke, USN, IFOR chief PIO, Sarajevo, 17 October 1996.

⁷⁸Interview with Colonel Serveille, FRA, IFOR deputy chief PIO, Sarajevo, 22 October 1996.

⁷⁹While the MND(SW) operated in an intimate and rather collegial atmosphere, it is notable that the PI office was in a separate building from most of the command groups.

⁸⁰According to Colonel Charles de Noirmont, FRA, IFOR deputy chief PIO, Admiral Smith threatened the major international organizations with withdrawing IFOR support for the Holiday Press Center (where the daily briefings were organized) before the agencies agreed to take partial charge and chair the daily briefing three times a week. Interview with the author, Paris, November 1996.

⁸¹On rarer occasions, U.S. embassy personnel attended the JICC.

⁸²Captain Mark Van Dyke, USN, IFOR Chief Public Information Officer, “Public Information In Peacekeeping: The IFOR Experience,” paper presented

before NATO's Political-Military Steering Committee Ad Hoc Group on Co-operation in Peacekeeping, Seminar on Public Relations Aspects of Peacekeeping, Brussels, Belgium, NATO Headquarters, 11 April 1997. Available at <http://www.nato.int/ifor/afsouth>.

- ⁸³LtCol Furlong, USA (Ret.), Deputy Commander CJHICTF, comment to the author, September 1997.
- ⁸⁴Interview with Colonel Icenogle, USA, MND(N) Joint Information Bureau Director, Tuzla, October 1996. However, some of the U.S. officers in NATO posts did not participate in this teleconference.
- ⁸⁵For example, ordnance exploded in a tent, killing and wounding Italian and Portuguese soldiers. In such a case, where two nations were involved in the incident, only NATO had authority to release information about the circumstances of the incident. In that case, both nations issued statements describing the incident and pointing the finger at the other for responsibility. Interview with LtCol Hoehne, USA, SHAPE chief media officer, Mons, 18 December 1996.
- ⁸⁶Interview with LtCol Paul Brooks, UKA, MND(SW) chief PIO, Banja-Luka, October 1996.
- ⁸⁷In this case, however, IFOR's public announcement angered the IO/NGO community because they did not receive advance warning from IFOR.
- ⁸⁸On 9 January 1996, a Bosnian Serb sniper shot a woman on the Sarajevo tramway. The French immediately fired back at his position. At the daily briefing, the press accused IFOR of standing by and not doing anything. At first, IFOR PI could not counter those accusations because it was not aware of the French response. When they finally became aware of it, the issue was no longer of interest to the media and was reported incorrectly internationally. Simon McDowall, Sarajevo CPIC director, interview with the author, London, February 1997. (For an account of the incident, see Olivier Tramond, "Une mission inédite exécutée par le 3e RPIMA à Sarajevo: La création d'une zone de séparation en milieu urbain," *Les Cahiers de la Fondation pour les Etudes de Défense*, 6/1997, p. 53.)
- ⁸⁹This conflict also reflected the somewhat traditional tension between higher and subordinate headquarters. For example, it seems that the ARRC concurred with the U.S. approach that a unified campaign against the Bosnian Serbs was the best approach. Meanwhile, all divisions felt they should have more freedom to conduct operations relevant to their respective AORs. For example, in summer 1996, Gen. Jackson, UKA, MND(SW) commander, refused to disseminate an edition of *The Herald Of Peace* (approved by COMIFOR and COMARRC) featuring a front-page article on indicted war criminals with photographs of Mladic and

Karadzic. Gen. Jackson felt the article was insensitive to the Bosnian Serbs. After flag-level involvement at IFOR, ARRC, and EUCOM, it was decided that a division could no longer unilaterally block the dissemination of COMIFOR's approved products. In that case, COMARRC sided with the CJIICTF against the division's commander.

⁹⁰The French reluctance stemmed from political and historical reasons. After the defeat in Indochina (1954), the French military constituted a PSYOP capability and used it extensively during the Algerian conflict. When many of the PSYOP officers supported the *coup des généraux* in 1961 (a rebellion against the legitimate government), the Ministry of Defense dissolved all the PSYOP units. This issue remains extremely sensitive to many government officials and general officers. However, as a result of IFOR operations, the French command for special operations (Commandement des Opérations Spéciales—COS) is now developing a PSYOP doctrine and capability.

⁹¹Interview with Major Chris Bailey, USA, PSYOP liaison officer to MND(SE), Mostar, October 1996.

⁹²The Nation Security Decision Directive (NSDD) 130 states: "While U.S. international information activities must be sensitive to the concerns of foreign governments, our information programs should be understood to be a strategic instrument of U.S. national policy, not a tactical instrument of U.S. diplomacy. We cannot accept foreign control over program content." Under this directive, DoD has consistently refused to place its PSYOP forces under 'foreign' control. The definition of 'foreign' has been extended to include NATO.

⁹³When LtCol Furlong briefed the Deputy Commander in Chief of U.S. Forces in Europe (DCINCEUR) on 6 December 1995 regarding the IFOR product approval process, DCINCEUR agreed to delegate approval authority to COMIFOR and to rely on COMCJIICTF's day-to-day judgment in case of conflict between the NATO and U.S. operations. If a conflict of interest appeared between IFOR and EUCOM's (i.e., USG) PSYOP campaigns, DCOMCJIICTF was to call EUCOM J3 to raise the issue and promote a mutually satisfying solution. According to LtCol Furlong, only one conflict occurred during *Joint Endeavor*.

⁹⁴Ariane Quantier from the UNHCR thought the French (who headed the division) wanted to control her message. On the other hand, PIOs working at the division thought that cooperation was only possible if all speakers agreed to a common message.

⁹⁵For example, Nik Gowing (BBC TV) and Kurt Schork (Reuters) publicly praised IFOR efforts to provide relevant information in a timely fashion. Rémy Ourdan, reporter for the French daily *Le Monde*, thought that IFOR had

been forthcoming with its operations. A *New York Times* reporter commented that *Joint Endeavor* was the “better military-media relationship he had ever seen.”

⁹⁶The author would like to thank the many individuals who commented on this chapter in its various stages of development: LTC James Treadwell; LTC Anthony Cucolo; LTC Mike Furlong; Major Steve Collins, JFKSWCS; Major Wayne Mason, JFKSWCS; Major Chris Ives, 2D POG; Major Richard Gordon, Royal Army Education Corps; Major Jack Guy, ACOM; SFC David Gates, 321st POC; SFC Robert Drennan, and SGT Jason Sherer, 346th POC (A); and the students and instructors at the Military Psychological Operations Course, Class 3/97 (Defense Intelligence and Security School, UK). While their guidance and assistance have helped the development of this chapter, I alone am responsible for its failings and shortcomings.

⁹⁷Even though the larger conflict is over, the propaganda methods that helped to inflame it have not disappeared. See Jane Perlez, “Serbian Media is a One Man Show,” *New York Times*, Sunday, August 10, 1997. For a more complete overview of the use of propaganda during the war in the Former Yugoslavia see Mark Thompson, *Forging War: The Media in Serbia, Croatia, and Bosnia-Herzegovina*, London, 1994 and Pedrag Simic, “The Former Yugoslavia: Media and Violence,” *RFE/RL Research Report*, Vol. 3 No. 5, February 4, 1994.

⁹⁸PSYOP are “Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives.” *Joint Pub 1-02*. Indeed, one contentious issue for the PSYOP units in Bosnia was that NATO and USEUCOM did not allow the use of the term “PSYOP.” Instead, PSYOP elements were given politically acceptable euphemisms such as Military-Civil Relations or Information Operations, and in the case of the PSYOP Task Force (POTF), the term Combined Joint IFOR Information Task Force (CJIICTF).

⁹⁹Though the majority of the personnel deployed to support Task Force Eagle were assigned to the 346th POC, a significant number of personnel from the 321st POC and the 350th POC deployed as part of the 15th POB force package. Elements from the 7th POG were also attached. The practice of patching together ad hoc force packages from available reservists rather than maintaining strict unit integrity has been standard during reserve PSYOP deployments in recent years.

¹⁰⁰During the IFOR mission there was no direct PSYOP support to the Russian

brigade in MND(N). The Russian LNOs at HQ TFE would receive IIC products to that Russian troops could disseminate them in their sector. Additionally, in some instances that were approved by the Joint Chiefs of Staff (JCS), U.S. loudspeaker teams supported Russian troops during crisis situations in Jusic and Celic. Another problem that the PSYOP community will have to consider is the role that "Command Information" platforms, such as the Finnish and French radio stations (not to mention the U.S. AFRTS and AFN) system, play in the information campaign. After all, there is no way to prevent the local population from picking up these broadcasts as well and thus they may impact upon the same target audiences as the PSYOP campaign.

¹⁰¹MG Meigs took over from MG William Nash as COMEAGLE when the 1st Infantry Division took over from the 1st Armored Division in November 1996. MG Meigs made these comments during an interview on the ABC News program, *Nightline*, aired on June 3, 1997. The particular segment focused on the difficulties involved with keeping the peace in Brcko, Bosnia.

¹⁰²Recent incidents in Brcko (August 29, 1997), where SFOR troops eventually had to use non-lethal means to break up a public disturbance, should not detract from the successes during the IFOR mission. They may indeed be the exceptions that prove the rule.

¹⁰³Much of this paper is based on the operations and intelligence files of BPSE 210 and DPSE 20, including not only materials that originated in the DPSE but those documents sent down from the CJIICTF to the DPSEs and CJIICTF. BPSE and DPSE SITREPS are available at the History and Museums Division, U.S. Army Special Operations Command, located at the JFK Special Warfare Center and School, Ft. Bragg, NC. Additional information was acquired through interviews and discussions with personnel from the 2nd and 4th POG.

¹⁰⁴For a focused discussion on the overall IFOR Information Campaign see the preceding chapter by Pascale Combelles Siegel.

¹⁰⁵CJIICTF Product Dissemination Summary, 20 May 1997. *The Herald of Progress*, a more sophisticated monthly periodical, replaced *The Herald of Peace* in February-March 1997.

¹⁰⁶The outgoing DPSE commander had forwarded his e-mail address through 4th POG to 2nd POG but because 2nd POG did not have any e-mail capability, this information was not passed down to the deploying units. The 11th POG, on the other hand, made great use of electronic mail and conducted a leader's reconnaissance prior to their deployment to Bosnia in January 1997. This resulted in a much smoother transition than the previous rotation had encountered.

- ¹⁰⁷Some at the CJIICTF believed that the CJIICTF and the CPSE had briefed the incoming tactical units. This definitely was not the case. Those stationed in Sarajevo at the CJIICTF often had different perceptions about what happened in MND(N) than those stationed in MND(N) and vice versa. This certainly reinforces this author's belief that clear and concise communication of intent between the COMCJIICTF through his COMCPSE to the COMDPSE in MND(N) was at best problematic.
- ¹⁰⁸This disconnect between not only the CPSE and the DPSE but between the DPSE and the BPSEs reflects not only the lack of organic communications equipment within the tactical PSYOP units but the difficulty PSYOP had working within the CJ-3 to S-3 channels in a combined-joint operation. It also may indicate a failure on the CPSE's part to ensure that its subordinate elements had access to all information that it sent out over communications systems such as WARLORD.
- ¹⁰⁹For an assessment of the role of Force Protection Teams see David D. Perkins, "Counterintelligence and Human Intelligence Operations in Bosnia," *Defense Intelligence Journal* 6-1 (1997): pp. 33-61.
- ¹¹⁰Furthermore, a look at the DPSE and SITREPs indicates that a great deal of information passed on to the DPSE did not always make it to the CPSE and CJIICTF. Attached elements such as FPTs and Civil Affairs had a somewhat better reporting system. Reports were made to the supported unit the same way any organic staff element would. While summaries of the day's events went up, details were sent as separate reports. In the case of FPTs each summary referenced a specific FPIR. This report was sent under separate cover but could be accessed by all if required. This meant that the same daily SITREP was sent to all concerned.
- ¹¹¹In particular, each nation had intelligence that was releasable only to its own military. Some intelligence was only releasable to NATO and not non-NATO members participating in IFOR/SFOR, such as the Russians. Although there was a great deal of intelligence available through U.S.-only channels, because of the coalition nature of the mission the CJIICTF did not have direct access to the JDISS or other assets usually available in a SCIF. The only access the CJIICTF had to this traffic was by sending a representative to the NIC in order to "pull down" useful intelligence—often a difficult process in itself.
- ¹¹²Former CJIICTF personnel insist that some of this information, to include Basic PSYOP Studies, was sent down to DPSE level. If this was the case, the DPSE was not aware that such information was available. In any case the information was not readily available to either the BPSEs or the supported units in MND(N). Still, some CJIICTF personnel indicated that they did not think such information was useful at the tactical

level. This again reflects the lack of solid communications between the elements of the PSYOP task force and the problems of continuity inherent during the rotation of forces into and out of theater. Interviews with CJIICTF personnel, May and September 1997, and with DPSE 20 personnel, 1997.

- ¹¹³One issue that will have to be discussed within the PSYOP community is the requirement to have trained 37F personnel act simply as “drivers” for PSYOP products, especially given the personnel-intensive nature of this operation and the shortage of trained and deployable 37F personnel. Despite clear personnel shortages in MND(N), there were never any replacements or additional TPTs provided by the CJIICTF using the Red Ball soldiers. It is the opinion of this author that this use of PSYOP troops, given the operational situation in theater, was not the most efficient use of valuable resources.
- ¹¹⁴In some instances, however, products were delivered within a matter of days if not hours. In MND(N) this was sometimes done by sending products such as loudspeaker or radio scripts via electronic means from the CJIICTF through the CPSE and to the DPSE.
- ¹¹⁵Despite the availability of some products announcing the Bosnian elections of September 1996, guides intended to explain the voting registration process did not arrive in MND(N) until after voter registration had ended. In addition products requested in July 1996 to support the RFCT’s “Spirit of the Posavina” campaign (a campaign designed to promote multiethnic unity and Civil Affairs actions in the Posavina Corridor) did not arrive until late November 1996 after the RFCT had already re-deployed to Germany. Likewise, after incidents involving IFOR soldiers and RS soldiers at Donja Mahala and Zvornik in late 1996, PSYOP elements in MND(N) waited 2 days before receiving approved scripts to give to local radio stations (and the IFOR station in Brcko). In the meantime local RS radio stations had already put their own “spin” on the story and broadcast it to listeners in the AOR.
- ¹¹⁶There is also some confusion as to whether or not products produced and developed specifically for NGOs and IGOs such as the UNHCR and the OSCE had to go through the same approval process as products developed specifically for IFOR units. To the best of this author’s knowledge, these products did not have to go through the approval process but were still disseminated by U.S. TPTs.
- ¹¹⁷On at least two occasions, supported unit commanders refused to allow the HoP to be disseminated in their AOR. In one case this was due to an article discussing the deadline for voter registration appearing in an issue that was delivered several days after the deadline for registration had

already passed. Similarly, one HoP article highlighted that the start of the “Atlanta 96” Summer Olympics was near. This article, however, appeared in an issue that was dated after the Olympics had already come to a conclusion. Although some CJIICTF members insist that the DPSE had the authority to keep products from being disseminated in their AOR, the DSPE commander was not aware of this authority if he did have it.

¹¹⁸Though some would argue that this set a dangerous precedent by deliberately trying to bypass the PSYOP product approval process, the fact remains that these PAO “products” were approved properly albeit through a different approval chain. In addition, by November, 1996, the CJIICTF gave PSYOP units the authority to use “open source” press releases as legitimate messages that did not have to be screened through the usual approval process. The PSYOP community will have to wrestle with this potentially volatile issue and in conjunction with its counterparts in the Public Affairs (not to mention LIWA and JC2WC) community discover solutions. If no solution is found, it is likely that such “work arounds” will be utilized in future situations that mirror the ones in Bosnia.

¹¹⁹What the BPSE did in these instances, with the approval of the DPSE commander, was to assist and guide the MPAD’s development of the BN commander’s radio addresses to the local population—in essence a mini Information Control Group run by the PAO at the BN level. After the BN Commander approved the script (using of course the “guidelines” given to him by his own superiors) the messages were sent to Task Force Eagle (Division) for approval by the Joint Information Bureau (JIB). Using this method the BNs were even able to develop “pre-approved” scripts for contingencies and these scripts could be adjusted and altered as necessary so long as they fit within the “information campaign” guidelines. The reason that these “work arounds” were possible is because to a great degree the PSYOP messages and the “open source” press releases were (or would have been in contingencies) identical. This is often the case with U.S. “white” propaganda operations that have historically been straightforward information campaigns.

¹²⁰In defense of the Product Development Center, finding themes, symbols, language, and grammar that would not offend any one segment of the local population was a lose-lose proposition. The purposeful politicization of the language and grammar in the Balkans meant that no matter what dialect IFOR chose to use, *someone* would take offense.

¹²¹The *HoP*, as with all IIC products, usually seemed somewhat bland when compared with the local competition. This is because the local papers were often shrill and polemic and not interested in objectivity. The lengthy approval process also tended to water down content.

¹²²The prototype of the monthly *Herald of Progress* (unnamed at the time of development) was begun at the end of September by the CJIICTF. The full production of this product was delayed by the deployment of LANDCENT, which directed that *The Herald of Peace* should continue unchanged through at least December 1996. Another program that developed during this time period was the “our message, their medium” approach, whereby weekly contact would be maintained through articles printed by local newspapers. The British responded to this with the publication of a regional product designed for MND(SW). The popularity of *MOSTOVI* (Bridges) among the local population resulted in the newsheet becoming a full-blown newspaper by mid-1997.

¹²³One of the local, family-owned FM stations seemed to have increased its listening audience by broadcasting in stereo. Casual listeners tuned into the station because as they were scanning through their channels the “FM Stereo” light went on their receiver and that attracted their attention. A technical note—there are ways to broadcast and make the stereo light go on individual receivers without actually broadcasting in stereo.

¹²⁴The ability of the PSYOP elements within the 2nd BDE, 1st A.D. AOR to get messages to a local radio station during the Mahala-Zvornik civil disturbances in early Autumn 1996 prevented a small incident involving Serbian Police and IFOR troops from turning into a potentially bloody military confrontation and civil disturbance. Likewise, in the RFCT/TF 1-18 AOR, planning for some contingencies included use of both local and IFOR-run radio stations for tactical purposes.

¹²⁵Throughout the deployment the issue arose within TFE as to whether or not the local population would be more receptive to messages broadcast over local radio stations (in line with the concept of “our message, their medium”). Within the RFCT/TF 1-18 AOR, the local radio stations had larger audiences, greater technical capacity, and more suitable entertainment formats for reaching a number of different target audiences. The PSYOP elements in the RFCT/TF 1-18 AOR sector had brief success by using the local stations, but this effort was hamstrung and eventually ended by directives from the CJIICTF. Subsequently, the local commanders turned again to the Public Affairs organizations in order to put out information over the local radio stations.

¹²⁶Interviews with PSYOP personnel and a look at BPSE and DPSE SITREPS indicate that on several occasions in November and December 1996, the DPSE did not forward negative criticism of products to the CPSE and CJIICTF.

¹²⁷Though the members of the CJIICTF staff vehemently disagree with this assessment, neither the COMCJIICTF nor the COMCPSE during this time

period gave any indications that they had any more than a basic understanding of the dynamics of planning and executing an information campaign. In addition the CJIICTF was likely hamstrung due to budgetary and time constraints and thus had to take the common denominator approach to target audience analysis.

¹²⁸Though there was no use of the Internet—one of the newest media for PSYOP—as a dissemination platform during the IFOR mission, the CJIICTF did consider the problem. This may have been an excellent medium for dissemination to certain key (urban elite) communicators. Students in Serbia have already had limited experience with the Internet as an effective means of persuasive communication, and called their recent uprising in Belgrade “the Internet revolution.” See “The Internet Revolution,” *Wired Magazine*, May 1996. The use of the Internet by the CJIICTF was held up at one time over the legality of using it because by law PSYOP products may not be available to the United States and the U.S. public could easily have accessed PSYOP Internet sites. Other assessments by the CJIICTF determined that the audience might have been too small to be worth the effort. Other U.S. Government entities, however, did use the Internet as a platform for dissemination. During the SFOR mission, the 1st Infantry Division considered its World Wide Web home page as one of several ways to convey information to target audiences. See LTC Garry J. Beavers and LTC Stephen W. Shanahan, “Operationalizing IO in Bosnia-Herzegovina,” *Military Review* (forthcoming).

¹²⁹Guidance on complex issues was often lacking, particularly in the latter part of the deployment. For example, many Muslims and Serbs in the RFCT/TF 1-18 AOR were very upset at the announcement that German troops would be arriving en masse in Bosnia. The typical response was, “you might as well send the Ustache,” a reference to the Croat Fascists puppet state of the Nazi Reich. Despite several requests for the “party line,” the BPSE could get no answer from the DPSE, CPSE, or CJIICTF on what to say. Eventually, the TPTs used the public affairs guidance provided by the BN MPAD.

¹³⁰Unfortunately, some may only remember Colonel Fontenot for remarks he made in December 1995 which irritated the FWF and thus did not support all objectives of the operational PSYOP campaign. Despite the FWF reaction to the suggestion that they may have killed people based upon race or ethnicity, Fontenot’s ability to intimidate the FWF probably helped to enhance the safety and security of U.S. troops in the sector—a primary PSYOP, U.S., and IFOR objective. A more comprehensive discussion of PSYOP and force protection issues appears later in this chapter. See also Thomas Ricks, “U.S. Brings to Bosnia the Tactics that Tamed the Wild West,” *The Wall Street Journal*, December 27, 1995.

- ¹³¹One of the intangibles that may have affected the ability of the key leaders to communicate effectively with the target audiences was the capability and the personality of the interpreters used by these individuals. It may be no coincidence then that Colonel Fontenot, the most effective communicator in the region, had one of the best interpreters in the region. The success of the TPTs was also determined to a large degree by the capability of its interpreters. An important lesson for the PSYOP campaign was that an engineered mix of local and DoD (U.S. national) linguists provided the best way to create products that could span the difficulties imposed by cross-cultural communication.
- ¹³²Specifically, in October 1996 the COMCJIICTF ordered the DPSE commander to cease all radio contracting activities with local radio stations. This was ordered as a precaution against any pecuniary responsibilities falling upon the PSYOP chain. The COMCJIICTF also asserted at this time that the local radio broadcasts were COMCJIICTF's responsibility. Though he was correct, the matter was complicated by the fact that the TFE contracting office had set up these contracts with 1st A.D. funds.
- ¹³³The force protection measures appear to have been largely a political decision in light of the U.S. experience in Somalia, where U.S. policy took a sharp turn after 18 American soldiers were killed in a single engagement in 1993. Indeed this decision was itself based on the larger belief that the U.S. public no longer expects its soldiers to die in battle. For an interesting take on the issue of "clean" conflicts, see Paddy Griffith, "The Politics of Getting Hurt," *Command*, summer 1994, pp. 8-13.
- ¹³⁴Specifically, the PSYOP element in the RFCT/TF 1-18 AOR experienced a severe degradation in mission capability during the final 6 weeks of their deployment due to the replacement in late December 1996 of all but one of the BPSE/TPTs vehicles with unserviceable vehicles from the 7th PSYOP Group in MND(SW). Some of the vehicles suffered from what TF 1-18 mechanics cited as the "criminal neglect" of basic PMCS and damage due to improper engine maintenance. This was also exacerbated by a lack of repair parts for U.S. vehicles in the British sector. The vehicle swap, ordered by the CJIICTF, brought missions to a virtual standstill in one sector and limited capability throughout the TF 1-18 AOR. By the time the BPSE was replaced in February 1997 all the elements vehicles were still not mission capable.
- ¹³⁵An additional point should be made that the first two rotations of PSYOP soldiers to the RFCT/TF1-18 AOR (from 4th POG and 2nd POG) both noted in their AARs that the weapons they carried were perhaps not always suitable for a STABOPS environment. They argued that rather than carrying only M-16A2s, soldiers on TPTs should also carry 9mm pistols so that M-16s would not have to be lugged through crowded markets and

brought into meetings with local political officials—indeed those situations where a pistol might be a better weapon in tactical terms. PSYOP soldiers in MND(SW) carried both M-16A2s and 9mm pistols and found this to be a satisfactory arrangement. See BPSE 940, 4th Psychological Operations Group AAR and BPSE 210 AAR.

- ¹³⁶Although some in IFOR may have believed the U.S. approach to be “ham handed,” this warfighting focus was understood and respected by the local faction military and thus reinforced their acceptance of the IFOR forces. In the words of one experienced peacekeeper, “...you want to make progress, you want belligerents to listen, obey, conform, then you got to carry the biggest stick; and every now and then, shake it at them, or pound one of them.” Furthermore, the heavy, hard, and “armed to the teeth” approach convinced the local population that IFOR could indeed provide the people of the Posavina Corridor with one of Maslow’s most base needs: security. The velvet touch really only proves useful in a more mature environment—not the type of environment during the initial IFOR mission. My thanks to LTC Anthony Cucolo for these insights.
- ¹³⁷The particulars of the OPORD also meant that PSYOP would not “rate” a MSE or LAN line from the supported unit; therefore, even the availability of the necessary equipment would not have guaranteed operability of that system. The BN commanders determined priority for these lines unless otherwise dictated from above by division or COMIFOR.
- ¹³⁸Ironically, in the last month of the deployment, handtalkies were delivered to the BPSE; however, they proved useless without instructions on how to program them to the correct frequencies and were subsequently returned to the CJIICTF.
- ¹³⁹During the period June 1996-February 1997, the CPSE’s role was somewhat ambiguous. In theory, the CPSE acted as the PSYOP Support Element to the ARRC, and as the link between the DPSEs and the CJIICTF. The CPSE, however, proved to be more of an appendage to the operation than a true conduit between the DPSEs and the CJIICTF. Per COMCJIICTF’s instructions, guidance to the DPSE would sometimes come directly from the CJIICTF. Similarly, at times the CPSE did not evaluate information that came up from the DPSEs but merely passed it on to the CJIICTF. Finally, the COMCPSE did not, as a general rule, attend the supported unit’s Information Coordination Group meetings held by COMARRC. Instead, representatives from the CJIICTF (either the DCOMCJIICTF or the CJ3 of the CJIICTF) would attend these meetings.
- ¹⁴⁰During the follow-up rotation (February-September 1997) a Theater PSYOP Support Element (TPSE), as well as a DPSE, was based at MND(N). Thus, the COMTPSE could help deconflict the operational PSYOP cam-

paigned as orchestrated by the CJIICTF with the needs of TFE. The DPSE commander could then truly provide tactical support to the MND without also having to engage in theater PSYOP planning.

¹⁴¹On the other hand, the vast majority of the PSYOP soldiers in theater were commended by various commands, to include COMEAGLE. These were not, by any means, gratuitous comments. MG Nash often commented on the quality of the tactical PSYOP soldiers (particularly the reservists) and their ability to contribute immensely to the success of the TFE mission. Indeed, the need to balance OPTEMPO with the recruitment, training, and retention and quality of personnel issues is one that must be addressed by both the RC and AC PSYOP forces.

¹⁴²Commanders, to include both COMEAGLEs, expressed their displeasure not only in daily Battle Update Briefs but in their comments during debriefings and to various historical and assessment teams. For example see Chapter 3, "Psychological Operations Support to Peace Operations," *BHCAAT 9 Initial Impressions Report* (For Official Use Only).

¹⁴³Indeed, during a variety of CTC exercises (CMTC, JRTC) to include those at Hohenfelz designed to train-up the 1st A.D. and the 1st I.D. for Bosnia, the PSYOP community had taught the maneuver elements to expect a much more responsive tactical PSYOP effort.

¹⁴⁴In the absence of what Major General Meigs felt was adequate PSYOP support, the 1st I.D. turned to the Land Information Warfare Activities (LIWA) cell to help coordinate and conduct its Information Operations campaign. See Beavers and Shanahan, "Operationalizing IO in Bosnia-Herzegovina." MG Meigs also overcame what he believed to be a lack of support from the CJIICTF by taking a broad interpretation of the guidelines for Command Information in order to put out the information he felt would help his mission in the AOR.

¹⁴⁵Interviews with TFE PSYOP personnel.

¹⁴⁶A MIST team is a five-man PSYOP element with production, linguistic, and area specialties. It usually will support a U.S. ambassador and country team with expertise and advice, as well as print, audio, and A.V. information products. Though by doctrine it would have been based in Sarajevo, it could have been used to support U.S.-only objectives and thus might have been used for TFE in the PSYOP planning role as opposed to a DPSE purpose built tactical coordination element.

¹⁴⁷Indeed, in June of 1996 the USACAPOC Commander stated to deploying troops that as the mission in Bosnia was a new one for the community the PSYOP troops would be "creating doctrine" as they went about their job.

¹⁴⁸This statement is based on comments made by former Deputy Undersecretary

of Defense (Policy) Craig Alderman to then Director for Psychological Operations, OSD, Col. Alfred H. Paddock, Jr. Conversation with Dr. Alfred H. Paddock, Jr., summer 1997.

¹⁴⁹There were numerous after action reports, lessons learned reports, briefings, and interviews that served as the basis for this chapter. Those of particular importance were USAREUR Headquarters After Action Report, 5th Signal Command Lessons Learned Book for *Operation Joint Endeavor*, History of the 7th Signal Brigade's involvement in *Operation Joint Endeavor*, USEUCOM Lessons Learned, NACOSA briefing on *Operation Joint Endeavor* Communications and Lessons Learned, IFOR CJ6 Lessons Learned, ARRC Communications and Information Systems Lesson Learned, IFOR C-Support Lessons Learned, CJCCC Information Book, Air Mobility Command Lessons Learned, USAFE Lessons Learned, IFOR Joint Analysis Team report, CISA *Operation Joint Endeavor* Lessons Learned report, Army War College AAR, SOCOM SOF Mission Support Lessons Learned, JITC C4I Infrastructure Documentation Report for *Operation Joint Endeavor*, Center for Army Lessons Learned reports, and DISA-EUR Lessons Learned.

¹⁵⁰The author would like to thank the many individuals who commented on this chapter in its various stages of development. In particular—from 5th Signal Command, BG Robert Nabors, USA, Col William Ritchie, USA, and Charles Smith; From NACOSA, GP CAPT Derek Ainge, RAF; The Air Force Historian office: Dr. Jay Smith; William Randall of DISA-EUR; Major Frederick Mooney, USAF; LTC David Perkins, USA; Col Fred Stein, USA (Ret.); and Patrick Deshazo and John Jannis, MITRE.

¹⁵¹There were a number of key interviews that set the stage for the NDU study and this chapter in particular: USEUCOM (J6): BG Randy Witt, USAF, and CAPT Tom Cooper, USN; BG Robert Nabors, Charles Riggs and 5th Signal Command staff; USAREUR: Col Fred Stein, USA; NACOSA: Gp Capt Ainge, RAF, and staff; SHAPE CISD: Kent Short; IFOR CJ6: CDRE Peter Swan, RN, and staff; AFSOUTH (CSG): Col Bob Hillmer, USAF, and in Zagreb Maj Flores, USAF; CJCCC: Col Rodawowski, USA, Col Dempsey, USA, and Lt Col Stan Howard, USAF; IFOR CJ6 (Sarajevo): Maj Fred Mooney, USAF; ARRC G6: LTC Lester, LTC Grey, and Maj Brand, UKA; MND(SE) G6: LTC DeMaillard, French Army; MND(SW) G6: Maj Pickersgill and Capt Allen, UKA; C-Support G6: LTC Rowe and Capt Bennett, USA; and the IFOR Joint Analysis Team: CAPT Peter Feist, GEN, Wg Cdr Nigel Reed, UKAFO, Cdr Magnussen, NON, Cdr Finseth, NON, Lt Cdr Jon Hill, USNR, and Lt Cdr Carol Clark, USNR.

¹⁵²IFOR Fact Sheets.

¹⁵³IFOR Fact Sheets and IDA report: *Operation Joint Endeavor-Description and Lessons Learned*, November 1996.

Appendix A: The Dayton Peace Agreement Summary¹⁵²

The Dayton Proximity Talks culminated in the initialing of a General Framework Agreement for Peace in Bosnia and Herzegovina. It was initialed by the Republic of Bosnia and Herzegovina, the Republic of Croatia, and the Federal Republic of Yugoslavia (FRY). The Agreement was witnessed by representatives of the Contact Group nations—the United States, Britain, France, Germany, and Russia—and the European Union Special Negotiator. The Dayton Peace Agreement and its annexes are summarized below.

General Framework Agreement

Bosnia and Herzegovina, Croatia, and the Federal Republic of Yugoslavia agree to fully respect the sovereign equality of one another and to settle disputes by peaceful means.

The FRY and Bosnia and Herzegovina recognize each other, and agree to discuss further aspects of their mutual recognition.

The parties agree to fully respect and promote fulfillment of the commitments made in the various annexes, and they obligate themselves to respect human rights and the rights of refugees and displaced persons.

The parties agree to cooperate fully with all entities, including those authorized by the United Nations Security Council, in implementing the peace settlement and investigating and prosecuting war crimes and other violations of international humanitarian law.

Annex 1-A: Military Aspects

The cease-fire that began with the agreement of October 5, 1995, will continue.

Foreign combatant forces currently in Bosnia are to be withdrawn within 30 days.

The parties must complete withdrawal of forces behind a zone of separation of approximately 4 km within an agreed period. Special provisions relate to Sarajevo and Gorazde.

As a confidence-building measure, the parties agree to withdraw heavy weapons and forces to cantonment/barracks areas within an agreed period and to demobilize forces which cannot be accommodated in those areas.

The agreement invites into Bosnia and Herzegovina a multinational military Implementation Force, the IFOR, under the command of NATO, with a grant of authority from the UN.

The IFOR will have the right to monitor and help ensure compliance with the agreement on military aspects and fulfill certain supporting tasks. The IFOR will have the right to carry out its mission vigorously, including with the use of force as necessary. It will have unimpeded freedom of movement, control over airspace, and status of forces protection.

A Joint Military Commission will be established, to be chaired by the IFOR commander. Persons under indictment by the International War Crimes Tribunal cannot participate.

Information on mines, military personnel, weaponry, and other items must be provided to the Joint Military Commission within agreed periods.

All combatants and civilians must be released and transferred without delay in accordance with a plan to be developed by the International Committee of the Red Cross.

Annex 1-B: Regional Stabilization

The Republic of Bosnia and Herzegovina, the Federation, and the Bosnian Serb Republic must begin negotiations within 7 days, under Organization for Security and Cooperation in Europe (OSCE) auspices, with the objective of agreeing on confidence-building measures within 45 days. These could include, for example, restrictions on military deployments and exercises, notification of military activities, and exchange of data.

These three parties, as well as Croatia and the Federal Republic of Yugoslavia, agree not to import arms for 90 days and not to import any heavy weapons, heavy weapons ammunition, mines, military aircraft, and helicopters for 180 days or until an arms control agreement takes effect.

All five parties must begin negotiations within 30 days, under OSCE auspices, to agree on numerical limits on holdings of tanks, artillery, armored combat vehicles, combat aircraft, and attack helicopters.

If the parties fail to establish limits on these categories within 180 days, the agreement provides for specified limits to come into force for the parties.

The OSCE will organize and conduct negotiations to establish a regional balance in and around the former Yugoslavia.

Annex 2: Inter-Entity Boundary

An Inter-Entity Boundary Line between the Federation and the Bosnian Serb Republic is agreed.

Sarajevo will be reunified within the Federation and will be open to all people of the country.

Gorazde will remain secure and accessible, linked to the Federation by a land corridor.

The status of Brcko will be determined by arbitration within 1 year.

Annex 3: Elections

Free and fair, internationally supervised elections will be conducted within 6 to 9 months for the Presidency and House of Representatives of Bosnia and Herzegovina, for the House of Representatives of the Federation and the National Assembly and presidency of the Bosnian Serb Republic, and, if feasible, for local offices.

Refugees and persons displaced by the conflict will have the right to vote (including by absentee ballot) in their original place of residence if they choose to do so.

The parties must create conditions in which free and fair elections can be held by protecting the right to vote in secret and ensuring freedom of expression and the press.

The OSCE is requested to supervise the preparation and conduct of these elections.

All citizens of Bosnia and Herzegovina aged 18 or older listed on the 1991 Bosnian census are eligible to vote.

Annex 4: Constitution

A new constitution for the Republic of Bosnia and Herzegovina, which will be known as “Bosnia and Herzegovina,” will be adopted upon signature at Paris.

Bosnia and Herzegovina will continue as a sovereign state within its present internationally recognized borders. It will consist of two entities: the Federation and the Bosnian Serb Republic.

The Constitution provides for the protection of human rights and the free movement of people, goods, capital, and services throughout Bosnia and Herzegovina.

The central government will have a Presidency, a two chamber legislature, and a constitutional court. Direct elections will be held for the Presidency and one of the legislative chambers.

There will be a central bank and monetary system, and the central government will also have responsibilities for foreign policy, law enforcement, air traffic control, communications, and other areas to be agreed.

Military coordination will take place through a committee including members of the Presidency.

No person who is serving a sentence imposed by the International Tribunal, and no person who is under indictment by the Tribunal and who has failed to comply with an order to appear before the Tribunal, may stand as a candidate or hold any appointive, elective, or other public office in the territory of Bosnia and Herzegovina.

Annex 5: Arbitration

The Federation and the Bosnian Serb Republic agree to enter into reciprocal commitments to engage in binding arbitration to resolve disputes between them, and they agree to design and implement a system of arbitration.

Annex 6: Human Rights

The agreement guarantees internationally recognized human rights and fundamental freedoms for all persons within Bosnia and Herzegovina.

A Commission on Human Rights, composed of a Human Rights Ombudsman and a Human Rights Chamber (court), is established.

The Ombudsman is authorized to investigate human rights violations, issue findings, and bring and participate in proceedings before the Human Rights Chamber.

The Human Rights Chamber is authorized to hear and decide human rights claims and to issue binding decisions.

The parties agree to grant UN human rights agencies, the OSCE, the International Tribunal, and other organizations full access to monitor the human rights situation.

Annex 7: Refugees and Displaced Persons

The agreement grants refugees and displaced persons the right to safely return home and regain lost property, or to obtain just compensation.

A Commission for Displaced Persons and Refugees will decide on return of real property or compensation, with the authority to issue final decisions.

All persons are granted the right to move freely throughout the country, without harassment or discrimination.

The parties commit to cooperate with the ICRC in finding all missing persons.

Annex 8: Commission to Preserve National Monuments

A Commission to Preserve National Monuments is established.

The Commission is authorized to receive and act upon petitions to designate as National Monuments movable or immovable property of great importance to a group of people with common cultural, historic, religious, or ethnic heritage.

When property is designated as a National Monument, the Entities will make every effort to take appropriate legal, technical, financial, and other measures to protect and conserve the National Monument and refrain from taking deliberate actions which might damage it.

Annex 9: Bosnia and Herzegovina Public Corporations

A Bosnia and Herzegovina Transportation Corporation is established to organize and operate transportation facilities, such as roads, railways, and ports.

A Commission on Public Corporations is created to examine establishing other Bosnia and Herzegovina Public Corporations to operate joint public facilities, such as utilities and postal service facilities.

Annex 10: Civilian Implementation

The parties request that a High Representative be designated, consistent with relevant UN Security Council resolutions, to coordinate and facilitate civilian aspects of the peace settlement, such as humanitarian aid, economic reconstruction, protection of human rights, and the holding of free elections.

The High Representative will chair a Joint Civilian Commission comprised of senior political representatives of the parties, the IFOR commander, and representatives of civilian organizations.

The High Representative has no authority over the IFOR.

Annex 11: International Police Task Force

The UN is requested to establish a UN International Police Task Force (IPTF) to carry out various tasks, including training and advising local law enforcement personnel, as well as monitoring and inspecting law enforcement activities and facilities.

The IPTF will be headed by a Commissioner appointed by the UN Secretary General.

IPTF personnel must report any credible information on human rights violations to the Human Rights Commission, the International Tribunal, or other appropriate organizations.

Appendix B: Chronology of IFOR Events¹⁵³

In the light of the Peace Agreement initialed in Dayton on 21 November 1995, the North Atlantic Council (NAC) authorized on 1 December 1995 the Supreme Allied Commander Europe (SACEUR) to deploy Enabling Forces into Croatia and Bosnia-Herzegovina. This decision demonstrated NATO's preparedness to implement the military aspects of a Peace Agreement, and to help create the conditions for a lasting peace in the former Yugoslavia. The NAC also gave provisional approval to the overall military plan.

On 1 December 1995, SACEUR tasked the Commander-in-Chief Southern Europe to assume control of assigned NATO land, air, and maritime forces as the Commander IFOR, and to employ them as part of the enabling force. Movement of these forces began on 2 December 1995.

On 5 December 1995, NATO Foreign and Defense Ministers endorsed the military planning for the Implementation Force (IFOR). On the same day the Acting Secretary General announced that 14 non-NATO countries—which had expressed interest in participating—would be invited to contribute to the IFOR: Austria, Czech Republic, Estonia, Finland, Hungary, Latvia, Lithuania, Pakistan, Poland, Romania, Russia, Slovakia, Sweden, and Ukraine.

All the NATO nations with armed forces (Belgium, Canada, Denmark, France, Germany, Greece, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, and United States) pledged to contribute forces to IFOR. Iceland provided medical personnel to IFOR.

The Peace Agreement (General Framework Agreement for Peace in Bosnia and Herzegovina) was formally signed in Paris on 14 December 1995.

On 15 December 1995, the United Nations Security Council—acting under Chapter VII of the Charter of the United Nations—adopted the resolution 1031, which authorizes the Member States to establish a multinational military Implementation Force (IFOR), under unified command and control and composed of ground, air, and maritime units from NATO and non-NATO nations, to ensure compliance with the relevant provisions of the Peace Agreement. Member States are also authorized to take all necessary measures to carry out the tasks identified by the same resolution.

On 16 December 1995, the NAC approved the overall plan for the Implementation Force and directed that NATO commence *Operation Joint Endeavor* and begin deploying the main Implementation Force into Bosnia that same day. The Force had a unified command and was NATO-led, under the political direction and control of the NAC and under the overall military authority of NATO's Supreme Allied Commander Europe, General George Joulwan; the responsibility as Commander-in-Theater was assigned to Admiral Leighton W. Smith, Commander-in-Chief Allied Forces Southern Europe, who assumed command of IFOR. The IFOR operated under clear NATO Rules of Engagement, which provided for robust use of force if necessary.

The transfer of authority from the Commander of UN Peace Forces to the Commander of IFOR took place on 20 December, effective at 1100 hours local time. On that day, after all NATO and non-NATO forces participating in the operation came under the command and/or control of the IFOR commander, over 17,000 troops were available to IFOR.

On 21 December, the first meeting of the Joint Military Commission (JMC) took place in Sarajevo. The JMC was a consultative body for COMIFOR. Based on the terms of the Peace Agreement, the JMC was the central body to which the signatories brought any military complaints, questions, or problems. JMCs were formed at various levels, in order that problems could be solved at the lowest possible level.

On 19 January 1996 withdrawal of the forces of all parties behind the zones of separation, which included Sarajevo and Gorazde, was completed.

On 3 February 1996, the parties had fulfilled their obligations to withdraw from areas to be transferred. Some reported violations were attributed mainly to ignorance and lack of leadership rather than deliberate non-compliance. The parties were urged to fully comply with all aspects of the peace agreement.

On 18 February 1996, the parties reaffirmed in Rome their commitment to the Peace Agreement. In particular, specific statements were approved on the work of the Joint Civil Commission Sarajevo; on the status of the implementation of the Federation of Bosnia and Herzegovina; on the situation in Mostar; on the normalization of relations between the Republic of Croatia and the Federal Republic of Yugoslavia; and on agreed measures to strengthen and advance the peace process.

On 18 February 1996, SACEUR reported to the Secretary General of NATO the completion of the initial deployment of IFOR. Thirty-two nations had been part of the deployment, with some 50,000 troops provided by NATO nations and approximately 10,000 from non-NATO contributors. The movement of IFOR had involved more than 2,800 airlift missions, some 400 trains, and more than 50 cargo ships.

On 26 February 1996, the Secretary General of NATO transmitted to the UN Secretary General a progress report on the Implementation Force. The report included an assessment of the Commander of IFOR that Bosnian Serb forces had withdrawn from the zones of separation established in the Peace Agreement. The

UN Security Council announced on 27 February that the economic sanctions imposed on the Bosnian Serb party were suspended indefinitely.

On 14 March 1996, the Chairman of the UN Security Council Committee established pursuant to resolution 724 (1991) issued a statement confirming the termination of the embargo on delivery of weapons and military equipment to former Yugoslavia, except heavy weapons, whose delivery will continue to be prohibited until the fulfillment of terms established with UNSC resolution 1021 (1995).

On 18 March 1996, the parties to the GFAP met in Geneva and expressed their determination to provide the political leadership necessary to ensure the complete fulfillment of the spirit and the letter of the Agreement and of the commitments made in Rome on 18 February 1996.

On 20 March 1996—91 days after TOA—COMARRC completed his assessment of compliance with the military aspects of the GFAP. While assessment of overall compliance is in progress, IFOR expressed satisfaction for the military co-operation which had been provided, as an indicator of an intention to comply.

On 23 March 1996, the parties further reaffirmed in Moscow their commitment to the Peace Agreement.

On 30 March 1996, Muslim and Croat partners in the Bosnian Federation signed an agreement aimed at strengthening the new institution. The agreement marked progress on critical aspects necessary to establish a functioning Federation, including the merging of customs, a joint military command, and amendments to the constitutions.

April 28, 1996, was D+120, the last deadline in the military annex of the Peace Agreement. It was assessed that as of that date the parties were on their way toward compliance with the requirements for cantonment of heavy weapons and forces and their mobilization. Full compliance had not been achieved yet but that seemed to reflect practical difficulties, rather than an absence of intent. IFOR will continue actively to monitor progress towards full compliance.

On 29 April 1996, the NAC issued a declaration on IFOR's role in the transition to peace.

On 3 June 1996, the NAC—after a meeting in Berlin, at Foreign Ministers level—issued a statement indicating that, given the magnitude and complexity of the preparations for elections in Bosnia and Herzegovina, IFOR would be maintained at approximately its current force levels until after the elections and would retain its overall capability until December, when its mandate comes to an end.

The Peace Implementation Council met in Florence on 13-14 June 1996. All the parties reaffirmed their commitment to the GFAP.

On 18 June 1996, the UN Security Council lifted the heavy weapons embargo on the former Yugoslavia. As a consequence, the NATO/WEU embargo enforcement *Operation Sharp Guard* was suspended.

On 1 July 1996 Bosnia's first free elections since the end of the war were held in Mostar.

On 31 July 1996, Adm. T. Joseph Lopez relieved Adm. Leighton Smith as COMIFOR.

On 19 August to 24 August 1996, IFOR destroyed 252 tons of Bosnian Serb munitions under a operation code named *Volcano*.

On 27 August 1996, the Chairman of the Provisional Election Commission, OSCE Head of Mission to Bosnia and Herzegovina, Ambassador Robert Frowick, announced that the 14 September municipal elections in Bosnia would be postponed.

On 30 August 1996, the NATO Airborne Early Warning E-3a Component flew its 50,000th flying hour in support of operations in the former Yugoslavia.

On 14 September 1996, nationwide elections, under the direction of OCSE, were held in Bosnia Herzegovina.

On 18 September 1996, the Secretary General of NATO announced that the NAC agreed to new command arrangements for IFOR, to allow for the phased withdrawal of Headquarters ARRC

and Headquarters AFSOUTH from Bosnia and Herzegovina and their replacement by a Headquarters based on Allied Land Forces Central Europe (LANDCENT).

On 1 October 1996, the United Nation Security Council adopted the resolution 1074, which provided for the termination of sanctions against Federal Republic of Yugoslavia, following the occurrence of the elections provided for in the Dayton Peace Agreement. As a consequence, NATO and WEU terminated *Operation Sharp Guard*.

On 22 October 1996, the OSCE announced that the municipal elections in Bosnia and Herzegovina, which were to be held in November, would be further postponed.

The TOA from the Commander of the AFSOUTH/IFOR to the Commander of the LANDCENT/IFOR occurred on 7 November 1996 and from the Commander of the Allied Rapid Reaction CORPS (ARRC) to the Commander of the LANDCENT/IFOR on 20 November 1996.

On 10 December 1996, the North Atlantic Council, meeting in Ministerial Session, issued a statement on Bosnia and Herzegovina announcing that NATO was prepared to organize and lead a Stabilization Force (SFOR) to take place of IFOR, authorized by a UN Security Council Resolution under Chapter VII of the UN Charter.

On 12 December 1996, the UN Security Council adopted Resolution 1088 authorizing the establishment of SFOR as the legal successor to IFOR for a planned period of 18 months.

SFOR was activated on 20 December 1996. Its mission was to deter fresh hostilities and to stabilize peace.

Appendix C: References

- [Abrams, 1996] LTG John Abrams, USA. *Operation Joint Endeavor Lessons Learned*. HQ V CORPS, May 1996.
- [Ahlquist, 1996] Captain (N) Lief Ahlquist. *Co-operation, Command and Control in UN Peacekeeping Operations*. Swedish War College, 1996.
- [Ainge, 1996] GP CAPT Derek Ainge, UK RAF. *Operation Joint Endeavor Communications Links*. NACOSA, Mons, Belgium, 1996.
- [Allard, 1995] Kenneth Allard. *Somalia Operations: Lessons Learned*. National Defense University Press, Ft McNair, Washington, D.C., January 1995.
- [Allard, 1996] Kenneth Allard. *Information Operations in Bosnia: A Preliminary Assessment*. National Defense University, Institute for Strategic Studies, Strategic Forum, Washington, D.C., November 1996.
- [Asbery, 1997] Johnny Asbery and Arnie Rausch, DSA, and Michael Casey, CISA. *C4ISR Laydown*. CISA Architectures Directorate, Washington, D.C., 1997.
- [Bell, 1996] Martin Bell. *In Harms Way*. Penguin Books, 1996.
- [Berry, 1996] Col Thomas Berry, USAF. *Operation Joint Endeavor: Executive Lessons Learned*. HQ Air Mobility Command, Scott AFB, IL, April 1996.
- [Boardman, 1997] Tony Boardman, UK. *Fellow Traveller*. HQ SFOR, Iidza, BiH, 16 March 1997.
- [Bonnart, 1996] Frederick Bonnart. *NATO'S SIXTEEN NATIONS: IFOR The Mission Continues...* Moench Publishing Group, Bonn, FRG, 1996.

- [Brewin, 1996] Bob Brewin. *BOSNIA The Role of I.T. in Operation Joint Endeavor*. Federal Computer Week, Falls Church, VA, April 1996.
- [Buchanan, 1996] William B. Buchanan. *Operation Joint Endeavor-Description and Lessons Learned (Planning and Deployment Phases)*. IDA, Alexandria, VA, November 1996.
- [Casey, 1997] Mike Casey, CISA, and Arnie Rausch and John Asbery, DSA. *IFOR C4ISR Laydown*. CD produced by CISA, 1997.
- [CJCCC, 1996] Combined Joint Communications Control Centre. *CJCCC Information Book, CJCCC Information Book (D+180), and CJCCC Information Book (TOA LANDCENT)*. HQ IFOR/AFSOUTH, Naples, Italy, 1996.
- [Cook, 1996] Capt Rhonda Cook, USA. *AAR Operation Joint Endeavor 1st AD Intelligence Production*. HQ Task Force Eagle, Tuzla, BiH, 1996.
- [Crouch, 1997] General William Crouch, USA. *USAREUR HEADQUARTERS AFTER ACTION REPORT (Volumes I and II)*. HQ USAREUR, Heidelberg, Germany, May 1997.
- [C-SUPPORT, 1996] C-SUPPORT Staff. *Excerpts from Lessons learned*. IFOR C-SUPPORT, Zagreb, Croatia, 1996.
- [Davidson, 1996] Lisa Davidson, Margaret Daly Hayes, James Landon. *Humanitarian and Peace Operations: NGOs and the Military in the Interagency Process*. Advanced Concepts, Technologies, and Information Strategies, Institute for National Strategic Studies, National Defense University, Washington, D.C., December 1996.
- [Davis, 1996] David Davis and Alexander Woodcock. *Analytic Approach to the Study of Future Conflict*. The Lester B. Pearson Canadian International Peacekeeping Training Centre, Clementsport, NS, Canada, 1996.
- [Deutch, 1996] John Deutch. *Revision of Director of Central Intelligence Directive 1/7, "Security Controls on the Dissemination of Intelligence Information."* Director of Central Intelligence, Washington, D.C., April 1996.
- [Dziedzic, 1996] Col Michael Dziedzic, USAF. *CIMIC and IPTF in Bosnia (Draft)*. National Defense University, Institute for National Strategic Studies, Ft McNair, Washington, D.C., 1996.
- [Feist, 1996] CAPT Peter Feist, GEN. *IFOR Joint Analysis Team Three Interim Reports and One Final Report*. JAT Press, Northwood, England, March/June/December 1996 and April 1997.
- [Fields, 1997] Craig Fields. *Report of the 1996 Defense Science Board Task Force on Improved Application of Intelligence to the Battlefield*. Office

- of the Secretary of Defense, Washington, D.C., March 1997.
- [Forster, 1996] Col Larry Forster and Col Steve Riley, USA. *Bosnia-Herzegovina After Action Review I and II*. Army War College Peacekeeping Institute, Carlisle Barracks, PA, April 1996/1997.
- [Gerald, 1997] LtCol Jeffrey Gerald, USAF, and John Christakos, Booz-Allen & Hamilton, Inc. *BC2A: Lessons Learned in Bosnia*. DARO, Washington, D.C., 1997.
- [Gjelten, 1995] Tom Gjelten. *SARAJEVO DAILY*. Harper Perennial, 1995.
- [GMU, 1997] George Mason University Center for National Security Law and The Lester B. Pearson Canadian International Peacekeeping Centre. *Strengthening the United Nations and Enhancing War Prevention*. GMU, Fairfax, VA, April 1997.
- [Gow, 1996] Jams Gow, Richard Paterson, and Alison Preston. *BOSNIA BY TELEVISION*. British Film Institute, 1996.
- [Grey, 1996] LTC A J Grey, UKA. *ARRC Communications and Information Systems Lessons learned*. HQ ARRC, Sarajevo, BiH, June 1996.
- [Griffith, 1997] LtCol Laura Griffith, USAF. *BOSNIA Intelligence Lessons Learned Working Group*. DIA/J2, Washington, D.C., 1997.
- [Hahm, 1996] William Hahm, Jennifer Chatfield, and Frank Franks, MITRE, Larry Wentz, NDU/CCRP and Anthony Simon, CISA. *Compendium of Operation JOINT ENDEAVOR Lessons Learned*. CISA Architectures Directorate, Washington, D.C., May 1997.
- [Hairell, 1996] LtCol Oscar Hairell, USAF. *Operation Joint Endeavor Lessons Learned*. HQ USAFE, Ramstein AFB, 1996.
- [Hartley, 1996] D.S. Hartley III. *Operations Other Than War: Requirements for Analysis Tools Research Report*. CINCPAC J53, Research and Analysis Division, Camp H. M. Smith, HI, December 1996.
- [Hayes, 1996/1997] Richard Hayes, James Landon, and Richard Layton. *Draft Reports on IFOR C2 Structure, CIMIC, Information Operations and Other C4ISR Lessons Learned Activities*. Evidence Based Research, Inc., Vienna, VA, 1996/1997.
- [JAT, 1996] IFOR Joint Analysis Team. *Observer Handbook*. JAT Press, Northwood, England, 1996.
- [Johnston-Burt, 1997] CDR Tony Johnston-Burt, RN. *IFOR'S C4I and Information Operations: A Multinational Perspective*. Naval War College, Newport, Rhode Island, 1997.

- [Joulwan, 1996] General George Joulwan, USA. *OPERATION JOINT ENDEAVOR: Joint After Action Review*. HQ USEUCOM (ECJ37-UCLL), December 1996.
- [Keiler, 1997] CDR Doug Keiler, USN. *Bosnia Bandwidth Allocation Study (Draft)*. National Defense University, Advanced Concepts, Technologies, and Information Strategies, Ft McNair, Washington, D.C., 1997.
- [Kurspanhic, 1997] Kemal Kursphic. *AS LONG AS SARAJEVO EXISTS*. The Pamphleteer's Press, 1997.
- [Last, 1997] David M. Last. *Theory, Doctrine and Practice of Conflict De-Escalation in Peacekeeping Operations*. The Lester B. Pearson Canadian International Peacekeeping Centre Press, Cornwallis Park, Clementsport, NS, 1997.
- [Maass, 1997] Peter Maass. *LOVE THY NEIGHBOR*. Vintage Books, 1997.
- [MacKenzie, 1993] Major General Lewis MacKenzie, Canadian Forces. *PEACEKEEPER*. Douglas and McIntyre, 1993.
- [Mackinlay, 1996] John Mackinlay. *A Guide to Peace Support Operations*. Thomas J. Watson Jr. Institute for International Studies, Brown University, Providence, RI, 1996.
- [Marks, 1996] Edward Marks. *Complex Emergencies: Bureaucratic Arrangements in the U.N. Secretariat*. Institute for National Strategic Studies, National Defense University, Washington, D.C., October 1996.
- [Merrill, 1995] Christopher Merrill. *THE OLD BRIDGE*. Milkweed Editions, 1995.
- [Mohr, 1996] Brad Mohr. *SOF Mission Support Lessons Learned*. HQ SOCOM, 1996.
- [Nabors, 1997] BG Robert Nabors, USA. *Lessons Learned Book: Operation Joint Endeavor*. HQ 5th Signal Command, 1997.
- [Nabors, 1997] BG Robert Nabors, USA. *AFCEA Briefing: Operation Joint Endeavor Communications*. HQ 5th Signal Command, 1997.
- [NDU/CCRP, 1996] NDU/CCRP Bosnia Study Team. *Bosnia C4ISR Project Progress Reports (1st and 2nd)*. National Defense University, Center for Advanced Concepts and Technology, Ft McNair, Washington, D.C., July/October 1996.
- [Owen, 1995] David Owen. *Balkan Odyssey*. Harcourt Brace and Company, 1995.

- [Palmer, 1996] Maj Rolf Palmer. *LOCE Lessons Learned*. HQ USEUCOM, 1996.
- [Pfaltzgraff, 1997] Robert Pfaltzgraff, Jr. and Richard Shultz, Jr. *War in the Information Age: New Challenges for U.S. Security*. Brassey's, 1997.
- [Phillips, 1996] LtCol Timothy Phillips, USMC. *JITC C4I Infrastructure Documentation Report for Operation Joint Endeavor*. JITC, Ft Huachuca, AZ, June 1996.
- [Pistor, 1997] Charles Pistor. *USEUCOM Combined Communications Operations Manual*. Joint Interoperability Engineering Organization, Defense Information Systems Agency, Ft Monmouth, NJ, 1997.
- [Rapaport, 1996] Richard Rapaport. *World War 3.1*. FORBES ASAP, October 1996.
- [Roberts, 1996] Cdr T Roberts, USN. *IFOR Intelligence Sharing: Successes and Challenges Briefing*. DCI, 1996.
- [Rogers, 1996/1997] LtCol Gary Rogers, USAF. *EUCOM JULLS*. HQ USEUCOM, 1996/1997.
- [Seiple, 1996] Capt Chris Seiple, USMC. *The U.S. Military/NGO Relationship in Humanitarian Interventions*. Peacekeeping Institute, Center for Strategic Leadership, U.S. Army War College, Carlisle, PA, 1996.
- [Siegel, 1996/1997] Pascale Combelles Siegel. *Information and Command and Control in Peace Operations: The Case of IFOR in Bosnia-Herzegovina*. Evidence Based Research, Inc., Vienna, VA, 1996/1997.
- [Silber/Little, 1997] Laura Silber and Allan Little. *YUGOSLAVIA: DEATH OF A NATION*. Penguin Books, 1997.
- [Smith, 1997] Dr. Jay Smith. *Bosnia Conflict*. Office of History, Air Force Command, Control, Communications and Computer Agency, Scott AFB, IL, 1997.
- [Stewart, 1996] George Stewart. *CNA Involvement in Joint Endeavor*. Center for Naval Analysis, Alexandria, VA, October 1996.
- [Strobel, 1997] Warren Strobel. *LATE-BREAKING FOREIGN POLICY: The News Media's Influence on Peace Operations*. United States Institute of Peace Press, 1997.
- [Swan, 1996] Commodore P W H Swan, RN. *Operation Joint Endeavor-CJ6 Lessons Learned*. HQ IFOR/AFSOUTH, Naples, Italy, November 1996.
- [Trewin, 1996] Wg Cdr I A Trewin, UK AF. *Operation Joint Endeavor Lessons*

- Learned*. SHAPE ACOS CISD, Mons, Belgium, October 1996.
- [Walley, 1996/1997] Jim Walley. *Operation JOINT ENDEAVOR: Task Force Eagle Initial Observations; Title 10 Sustainment and Force Protection; and three Task Force Eagle Continuing Operations reports. Operation JOINT GUARD: Task Force Eagle Initial Impressions and Task Force Eagle Continuing Operation*. Center for Army Lessons Learned, Ft Leavenworth, KS, May/August/September 1996 and March/April 1997 and for Joint Guard report 1997.
- [Wentz, 1991] Larry K. Wentz. *DCA Grey Beard Lessons Learned: Desert Shield/Desert Storm*. MITRE, McLean, VA, August 1991.
- [Wentz, 1992] Larry K. Wentz. *The First Information War: Communications Support for the High Technology Battlefield*. AFCEA International Press, Fairfax, VA, October 1992.
- [Wentz, 1993/1994] Larry K. Wentz. *DISA Grey Beard Panel: Lessons Learned Operation Restore Hope (1993) and A U.S. Perspective of UN Operations (1994)*. MITRE, McLean, VA, September 1993/1994.
- [Wentz, 1996] Larry K. Wentz. *Managing The Peace Offensive: Coalition Operations Lessons Learned*. AFCEA Europe Brussels Symposium and Exposition, Brussels, Belgium, October 1996.
- [Wentz, 1996] Larry K. Wentz. *C3I Observations: A View from the Theater*. National Defense University, Center for Advanced Concepts and Technology, Ft McNair, Washington, D.C., March 1996.
- [Wentz, 1997] Larry K. Wentz. *C3I for Peace Operations: Lessons from Bosnia*. National Defense University, Center for Advanced Concepts and Technology, Ft McNair, Washington, D.C., May 1997.
- [Wentz, 1996/1997] Larry K. Wentz. *Unifying the Analysis of Bosnia C3I Lessons Learned*. National Defense University, Center for Advanced Concepts and Technology, Ft McNair, Washington, D.C., 1996/1997.

World Wide Web URLs

(current as of 5 December 1997)

1. NATO official home page: <http://www.nato.int/home.htm>
2. NATO *Operation Joint Endeavor* (IFOR) information home page: <http://www.nato.int/ifor/ifor.htm>
3. Task Force Eagle: <http://www.tfeagle.army.mil/>.

4. TALON—Task Force Eagle’s on-line magazine:
<http://www.tfeagle.army.mil/talon/index.html>.
5. Center for Army Lessons Learned: <http://call.army.mil/call.html>
6. USAREUR: <http://www.hqusareur.army.mil>
7. USAFE: <http://www.usafe.af.mil/index.html>
8. US Navy News, Bosnia Operations:
<http://www.navy.mil/navpalib/bosnia/bosnia1.html>
9. USEUCOM: <http://www.eucom.mil>
10. U.S. Department of Defense BosniaLink: <http://www.dtic.mil/bosnia/>
11. U.S. Department of State Policy on Bosnia home page:
<http://www.state.gov/www/regions/eur/bosnia/index.html>.
12. USAID: <http://www.info.usaid.gov/>
13. NGO Sites: <http://www.interaction.org/ia/sites.html>
14. World Vision:
<http://www.worldvision.org/worldvision/master.nsf/stable/home>
15. InterAction: <http://www.interaction.org/ia/mission.html>
16. Disaster Response Internet Directory:
<http://www.interaction.org/ia/disaster/director.html>

IFOR Basic Documents

November 15, 1995, SHAPE OPLAN 40105

Joint Endeavor

AFSOUTH OPLAN 40105

ARRC OPLAN 60105

December 2, 1995, JCS EXORD for the U.S. Enabling Force

Joint Endeavor

December 2, 1995, USCINCEUR OPLAN 4243

Balkan Endeavor

December 6, 1995, SACEUR OPLAN 40105

Decisive Endeavor

December 14, 1995, Paris
The General Framework Agreement for Peace in Bosnia and Herzegovina (a.k.a. The Dayton Peace Agreement).

December 16, 1995, JCS EXORD for the U.S. Main Body
Joint Endeavor

December 16, 1995, SACEUR OPLAN 10405
Joint Endeavor

January 26, 1996, Vienna
OSCE Agreement on Confidence- and Security-Building Measures in Bosnia and Herzegovina.

February 18, 1996, Rome
The Rome Statement reflecting the work of the Joint Civilian Commission Sarajevo Compliance Conference.

March 18, 1996, Geneva.
Agreed Measures.
Statement on the Federation of Bosnia and Herzegovina.

March 23, 1996, Moscow.
The Final Document of the Contact Group Ministerial Meeting.

June 13-14, 1996, Peace Implementation Council, Florence.
Chairman's Conclusions.
Chairman's Summary.

June 29, 1996, Lyon G7/G8 Summit.
Decisions concerning Bosnia and Herzegovina.

December 4-5, 1996, Peace Implementation Conference, London
Official Summary of Conclusions.
Conclusions: Bosnia and Herzegovina 1997: Making Peace Work.

Appendix D: Acronyms

A

ABCCC	Airborne Command and Control
ACC	Air Component Commander
ACE	Allied Command Europe
ACFL	Agreed Cease-Fire Line
AD	Architectures Directorate
ADAMS	Allied Deployment and Movement System
ADCI/MS	Associate Director of Central Intelligence for Military Support
ADSI	Air Defense System Integrator
AFMSS	Air Force Mission Support System
AFSOUTH	Armed Forces Southern Command
AIFS	Allied Information Flow System
AMC	Air Mobility Command
AMCC	Allied Movement Control Center
AMIB	Allied Military Intelligence Battalion
AMS	Automated Manifesting System
AOCG	Airlift Operations Coordination Group
AOR	Area of Responsibility
AOT	Area of Transfer
APOD	Aerial Port of Debarkation
ARL	Air Reconnaissance Low
ARRC	ACE Rapid Reaction Corps
ASAS	All Source Analysis System
ASD/C3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order

AUTODIN Automatic Digital Network
AWACS Airborne Warning and Control System
AWE Advanced Warfighting Experiments

B

BC2A Bosnia C2 Augmentation
BCT Brigade Combat Team
BDA Battle Damage Assessment
B-H Bosnia-Herzegovina
BMC Broadcast Management Center
BHAAR Bosnia-Herzegovina After Action Report
BTIC Bosnia Technology Integration Cell

C

C2 Command and Control
C2IPS C2 Information Processing System
C3I Command, Control, Communications, and Intelligence
C4I Command, Control, Communications, Computers, and Intelligence
C4IFTW Command, Control, Communications, Computers, and Intelligence for the Warfighter
C4ISR Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAAT Combined Arms Assessment Team
CALL Center for Army Lessons Learned
CAOC Combined Air Operations Center
CAP Combat Air Patrol
CARS Contingency Airborne Reconnaissance System
CCIRM Collection Coordination Intelligence Requirements Management
CCITT International Telephone and Telegraph Consultative Committee
CCRP Command and Control Research Program
CEWI Combat Electronic Warfare Intelligence
CHS Combat Support Hospital
CI Counterintelligence
CIA Central Intelligence Agency
CIAP Command Intelligence Architecture/Planning Program
CIC Counterintelligence Corps
CICG Commanders Information Coordination Group
CIMIC Civil Military Cooperation

CINC	Commander-in-Chief
CINCAFSOUTH	Commander-in-Chief, Allied Forces Southern Europe
CINCIFOR	Commander-in-Chief, Implementation Force
CINCSOUTH	Commander-in-Chief, Southern Region
CINCUSNAVEUR	Commander-in-Chief, U.S. Navy Europe
CIS	Communications and Information Systems
CISA	C4I Integration Support Activity
CISCC	Communications Information Systems Control Center
CISD	Communications and Information Systems Division
CISD	Command Intelligence Strategy Document
CJCCC	Combined Joint Communications Control Center
CJCMIC	Combined Joint Civil Military Cooperation
CJIICTF	Combined Joint IFOR Information Campaign Task Force
CJTF	Combined Joint Task Force
CNA	Center for Naval Analysis
COMAIRSOUTH	Commander, Air Forces Southern Europe
COMIFOR	Commander, Implementation Force
COMINT	Communications Intelligence
COMNAVSOUTH	Commander, Allied Naval Forces Southern Region
COMSEC	Communications Security
COP	Common Operation Picture
COTS	Commercial off-the-Shelf
CPIC	Combined Press Information Center
CRC	Control and Reporting Center
CRESP	Crisis Response Prototype
CRONOS	Crisis Response Operations in NATO Operating Systems
CSA	Chief of Staff of the Army
CSCE	Conference on Security and Cooperation in Europe
CSCI	Commercial Satellite Communications Initiative
CSS	Common User Data Network

D

DASH	Deployable Automation Support Host
DCI	Director of Central Intelligence
DCSINT	Deputy Chief of Staff for Intelligence
DDN	Defense Data Network
DDP	Detailed Deployment Plans
DHS	Defense HUMINT Service

DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISE	Deployable Intelligence Support Element (USAREUR)
DISN	Defense Information System Network
DITDS	Defense Intelligence Threat Data Base System
DoD	Department of Defense
DPA	Dayton Peace Accords
DSCS	Defense Satellite Communications System
DSN	Defense Switched Network

E

E1	European and CCITT Digital Standard (2.048 Mbps)
EAC	Echelons Above Corps
EBRD	European Bank for Reconstruction and Development
ECB	Echelons Corps and Below
ECHO	Evolutionary Capability for Headquarters Operation
EDP	Electronic Data Processing
ELS	Exportable Logistics System
E-mail	Electronic Mail
ENGCC	Engineer Coordination Center
ESC	Electronic Systems Center
EU	European Union
EUCOM	European Command
EW	Electronic Warfare

F

FAX	Facsimile
FDDI	Fiber Distributed Data Interface
FERN	Free Elections Radio Network
FMS	Foreign Military Sales
FOUO	For Official Use Only
FPB	Force Protection Branch
FPIR	Force Protection Information Report
FPT	Force Protection Team
FRAGO	Fragmentary Order
FTP	File Transfer Protocol
FWF	Former Warring Factions
FY	Former Yugoslavia

G

GCCS	Global Command and Control System
GFAP	General Framework Agreement for Peace
GMF	Ground Mobile Force
GOTS	Government off-the-shelf
GPS	Global Positioning System
GRCS	Guardrail Common Sensor
GSM	Ground Station Module
GSR	Ground Surveillance Radar

H

HF	High Frequency
HLWG	High Level Working Group
HCG	HUMINT Coordination Group
HAC	HUMINT Analysis Cell
HUMINT	Human Intelligence

I

IARRCIS	Interim ARRC Information System
ICARIS	Integrated C4I Architectures Requirements Information System
ICC	IFOR Coordination Center
ICRC	International Committee of the Red Cross
ICTY	International Criminal Tribunal for the former Yugoslavia
IDA	Institute for Defense Analyses
IDIP	Interim Digital Interface PTARMIGAN
IDNX	Integrated Digital Network Exchange
IEBL	Inter-Entity Boundary Line
IEC	Interstate Electronics Corporation
IEW	Intelligence Electronic Warfare
IFOR	Implementation Force
IIC	IFOR Information Campaign
IIR	Intelligence Information Report
IMARSAT	International Maritime Satellite
INFOSEC	Information Security
INSCOM	Intelligence and Security Command
INSS	Institute for National Strategic Studies
INTSUM	Intelligence Summaries
IO	International Organization
IP	Internet Protocol
IPB	Intelligence Preparation of the Battlefield

IPL	Intelligence Priority List
IPN	IFOR Private (Peace) Network
IPTF	International Police Task Force
ISARC	Intelligence, Surveillance, and Reconnaissance Cell
ISB	Intermediate Staging Base
ISR	Intelligence, Surveillance, and Reconnaissance
ISR	Intelligence, Surveillance, and Reconnaissance
ITV	Intransit Visibility
IVSN	Initial Voice Switched Network

J

JAC	Joint Analysis Center
JAT	Joint Analysis Team
JAWS	Joint Analytical Workstation
JBS	Joint Broadcast Service
JCC	Joint Civil Commission
JCO	Joint Commission Officer
JDISS	Joint Deployable Intelligence Support System
JIB	Joint Information Bureau
JIEO	Joint Interoperability Engineering Organization
JITC	Joint Interoperability Test Command
JLOC	Joint Logistics Operations Center
JMC	Joint Military Commission
JMCC	Joint Movement Control Center
JNA	Yugoslav Army
JOC	Joint Operational Cell
JOPES	Joint Operations, Planning and Execution System
JRC	Joint Reconnaissance Center
JSTARS	Joint Surveillance Target Attack Radar System
JTAV	Joint Total Asset Visibility
JTF	Joint Task Force
JTF-PP	Joint Task Force - Provide Promise
JULLS	Joint Universal Lessons Learned System
JWICS	Joint Worldwide Intelligence Communications System
JWID	Joint Warfare Interoperability Demonstration

K

KCC	Contracting Coordination Center
-----	---------------------------------

L

LAN	Local Area Network
-----	--------------------

LANDCENT	Land Forces Central Europe
LES	Large Extension Node
LIWA	Land Information Warfare Agency
LMDS	Local Multipoint Distribution Service
LNO	Liaison Officer
LOCE	Linked Operations-Intelligence Centers Europe
LOS	Line of Sight

M

MAE	Medium Altitude Endurance
MASH	Mobile Army Surgical Hospital
MASINT	Measurement and Signature Intelligence
MCS	Maneuver Control System
MDCI	Multi-Discipline Counterintelligence
MEDCC	Medical Coordination Center
MEDCOC	Medical Co-ordination Center
MI	Military Intelligence
MIDS/IDB	Military Integrated Data System/Intelligence Database
MIST	Mission Information Support Team
MITT	Mobile Integrated Tactical Terminal
MNC	Major NATO Command
MND	Multinational Division
MND(N)	Multinational Division-North (US-led, Tuzla-based)
MND(SE)	Multinational Division-Southeast (France-led, Mostar-based)
MND(SW)	Multinational Division-Southwest (UK-led, Banja Luka-based)
MNMF	Multinational Maritime Force
MORS	Military Operations Research Society
MPA	Maritime Patrol Aircraft
MPAD	Mobile Public Affairs Detachment
MRE	Meal Ready-to-Eat
MSE	Mobile Subscriber Equipment
MWR	Moral, Welfare, and Recreation

N

NABS	NATO Air Base
NAC	North Atlantic Council
NACCIS	North Atlantic Command Control Information System
NACISA	NATO CIS Agency

NACOSA	NATO CIS Operating and Supporting Agency
NAEWF	NATO Airborne Early Warning Force
NAI	Named Area of Interest
NAI	NATO Analog Interface
NAMSA	NATO Maintenance and Supply Agency
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation, Command and Control Agency
NCCAP	NATO CIS Contingency Assets Pool
NCCMC	National Collection Management Cell
N-D	Non-doctrine, Non-doctrinal
NDU	National Defense University
NES	Network Encryption System
NGO	Non-Governmental Organization
NIC	National Intelligence Cell
NICS	NATO Integrated Communications System
NIDS	NATO Integrated Data Service
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Intelligence Support Team
NMJIC	National Military Joint Intelligence Center
NRL	Naval Research Laboratory
NSA	National Security Agency
NSE	National Support Element

O

OAB	Operational Analysis Branch
OHR	Office of the High Representative
OJT	On-the-Job-Training
OOA	Out Of Area
OODA	Observation, Orientation, Decision, and Action
OOTW	Operations Other Than War
OPCOM	Operational Command
OPCON	Operational Control
OPLAN	Operation Plan
OPORD	Operations Order
OPSEC	Operational Security
ORBAT	Order of Battle
OSC	Objective Supply Capability
OSCE	Organization for Security and Cooperation in Europe
OSINT	Open source Intelligence
OSO	Operational Support Office
OSS	Office of Strategic Services
OTG	Operational Task Group

P

PABX	Private Access Branch Exchange
PAIS	Prototype ACE Intelligence System
PAT	Permanent Maritime Analysis Team
PBX	Private Branch Exchange
PIP	Partnership for Peace
PI	Public Information
PIC	Peace Implementation Council
PIO	Public Information Office
PIR	Priority Intelligence Requirements
PME	Professional Military Education
POC	Points of Contact
POP	Point of Presence
POTF	PSYOP Task Force
PSYOP	Psychological Operations
PTT	Post Telephone and Telegraph
PVO	Private Voluntary Organization

R

R&S	Reconnaissance and Surveillance
RAF	Royal Air Force
RAMCC	Regional Air Movement and Coordination Center
RAP	Recognized Air Picture
RCC	Regional Control Center
REL IFOR	Releasable to Implementation Force
REL NATO	Releasable to North Atlantic Treaty Organization
REL	Releasable to
REMBASS	Remotely Monitored Battlefield Sensor Systems
RF	Radio Frequency
RFCT	Ready First Combat Team
RFI	Requests For Information
RITA	Reseau Integre de Transmissions Automatique
RS	Republik Srbska
RSSC	Regional Space Support Center
RVT	Remote Vehicle Terminal

S

SACEUR	Supreme Allied Commander, Europe
SAR	Synthetic Aperture Radar
SAT	Satellite
SATCOM	Satellite Communication

SCI	Sensitive Compartmented Information
SCSG	Satellite Communication Sub-Group
SEAD	Suppression of Enemy Air Defense
SEN	Small Extension Node
SFOR	Stabilization Force
SGT	Satellite Ground Terminal
SHAPE	Supreme Headquarters Allied Powers Europe
SHF	Super High Frequency
SIPRNET	SECRET Internet Protocol Router Network
SITREP	Situation Report
SOCOM	Special Operations Command
SOF	Special Operations Forces
SOP	Standard Operating Procedure
SPIRIT	Special Purpose Integrated Remote Intelligence Terminal
SPOD	Sea Port of Debarkation
SSO	Stability and Sustainment Operation
STAGNAG 4206	NATO Standardization Agreement, Digital Telephony
STAGNAG 5040	NATO Standardization Agreement, Analog Telephony
STAGNAG	NATO Standardization Agreement
STAMIS	Standard Army Management Information Systems
STC	SHAPE Technical Center
STEP	Standard Tactical Entry Point
STONS	Short Ton
STU	Secure Telephone Unit
SWO	Staff Weather Office

T

T1	North American Digital Signal (1.544 Mbps)
TACOM	Tactical Command
TACON	Tactical Control
TACSAT	Tactical Satellite [Terminal]
TADIL	Tactical Data Information Link
TARE	Telegraph Automatic Relay Equipment
TAV	Total Asset Visibility
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCS	Temporary Change of Station
TDDS	Tactical Data Dissemination System
TENCAP	Tactical Exploitation of National Capabilities Program
TFCICA	Task Force CI Coordinating Authority

TFE	Task Force Eagle
TFM	Theater Frequency Management
TFMC	Theater Frequency Management Cell
TIBS	Tactical Information Broadcast System
TNOC	Theater Network Operations Center
TOA	Transfer of Authority
TOC	Tactical Operations Center
TOE	Table of Equipment
TPN	Tactical Packet Network
TRI-TAC	Tri-service Tactical Communications
TROJAN SPIRIT	TROJAN Special Purpose Integrated Remote Intelligence Terminal
TRRIP	Theater Rapid Response Intelligence Package
TS	Top Secret
TSCM	Technical Surveillance Countermeasures
TSGT	Transportable Satellite Ground Terminal
TSGT	Transportable Satellite Ground Terminal
TSO	Telecommunications Service Order
TSSR	TROPO/SATELLITE Support Radio
TTA	Tactical Terminal Adapter

U

UAV	Unmanned Aerial Vehicle
USCIRF	USAREUR Combat Intelligence Readiness Facility
UHF	Ultra High Frequency
UN	United Nations
UNCRO	UN Confidence Restoration Organization
UNHCR	UN High Commissioner for Refugees
UNMIBH	United Nations Mission in Bosnia-Herzegovina
UNPREDEP	UN Preventive Deployment
UNPROFOR	United Nations Protection Force
UNSCR	UN Security Council Resolution
UNTAES	UN Transitional Administration for Eastern Slavonia
US	United States
USACAPOC	U.S. Army's Civil Affairs and Psychological Operations Command
USAFE	United States Air Forces Europe
USAID	United States Agency for International Development
USAREUR	United States Army Europe
USEUCOM	United States European Command
USG	U.S. Government

UWF Unified Weather Forecast

V

VHF Very High Frequency
VSAT Very Small Aperture Terminal
VTC Video Teleconference

W

WAN Wide Area Network
WEU Western European Union
WWMCCS World-Wide Military Command and Control System
WWW World Wide Web

X

X.25 Packet Switch Protocol

Z

ZOS Zone of Separation

About the Contributing Editor

Larry K. Wentz is on special assignment to the National Defense University (NDU) as the acting Director of the Command and Control Research Program. Prior to his assignment to NDU, he held the positions of Director of Joint Operations for the MITRE Washington C3 Center and Technical Director of MITRE's Joint and Defense-Wide Systems Division and led the U.S. National Expert support to the NATO Communications and Information System Agency (NACISA) for more than 18 years. He has extensive experience in NATO C3 and C4I support to Coalition Joint Task Force operations, including leading a number of Lessons Learned studies for operations such as *Desert Shield*, *Desert Storm*, and *Restore Hope*. He is currently leading an NDU study of the C2 Structure and supporting C4ISR for the Bosnia operation, *Joint Endeavor*. Mr. Wentz has a BSEE from Monmouth College and an MS in Systems Engineering and Operations Research from the University of Pennsylvania. He has completed the Executive Management Program at the University of Pennsylvania's Wharton Business School and the Harvard John F. Kennedy School of Government Program for Senior Executives in National and International Security. Mr. Wentz was awarded the AFCEA Meritorious Service Award for his contributions to international C3 and was a contributing author to the AFCEA Information Press book, *The First Information War*.

About the Authors

Richard L. Layton is the Director of the Military Studies Division at Evidence Based Research, Inc. He retired from the U.S. Army after over 20 years of service, during which time he served overseas in Vietnam as an Infantry Officer, in Korea as a counter-intelligence officer, in Japan as a Special Forces Platoon Leader, and in Hawaii as a theater-level intelligence analyst. His assignments in the United States included counter-intelligence officer, force structure/plans officer—U.S. Army Intelligence and Security Command, and plans officer and executive officer for the Deputy Chief of Staff for Intelligence, Headquarters, Department of the Army. Since retirement he has been analyzing the evaluation of command and control of military systems and processes. Currently he directs work in decision making, Bosnia operations, peace and coalition operations, information warfare, operations other than war, Joint Vision 2010, and Defense Advanced Research Projects Agency's functional architecture for the Command and Control Research Program at the National Defense University.

James J. Landon is an analyst at Evidence Based Research, Inc. His current projects focus on civil-military relations, multinational peacekeeping and humanitarian assistance operations, and coalition command and control. He is a member of the NATO Joint Analysis Team (JAT) supporting the IFOR/SFOR deployment to the former Yugoslavia where he is involved in analyzing multinational CIMIC doctrine and operations and the implementation of the civil aspects of the Dayton Peace Agreement.

Andrew Bair serves as Senior Advisor to the Special Representative of the President and Secretary of State for Implementation of the Dayton Peace Accords. Previously, he served two tours with the United Nations in the former Yugoslavia as a political officer, first during 1993 in the UN-protected areas in Croatia and, most recently, in Bosnia during 1995-1996 as the Special Assistant to the UN Chief of Mission there. Afterward, Mr. Bair served as the Political Advisor to the Commissioner of the UN's International Police Task Force. From 1988 to 1994 Mr. Bair was Senior National Security Analyst and Manager of the Center for National Security Negotiations of Science Applications International Corporation. Mr. Bair holds an M.A. from and is currently a doctoral student at The George Washington University, Washington, D.C.

Michael J. Dziedzic specializes in peace operations and security affairs in the Western Hemisphere at the Institute for National Strategic Studies, National Defense University. Previously, he was a member of the faculty at the National War College, served as Air Attache in El Salvador during the implementation of the peace accords, and was a professor in the Department of Political Science at the U.S. Air Force Academy. His writings include *Mexico: Converging Challenges* and articles on Mexican defense policies, the transnational drug trade, and hemispheric security matters.

Pascale Combelles Siegel is an independent researcher based in Arlington, Virginia, where she works on media and defense issues. She is currently completing her dissertation in political science on 'Ideological conflict and practical reliance: The U.S. military-media relationship in times of conflict since Grenada.' From January to June 1997, Mrs. Combelles Siegel participated in NATO's Joint Analysis Team final report on operations *Joint Endeavor* and *Joint Guard*. All data used in her chapter were collected prior to this assignment.

Mark R. Jacobson earned his M.A. at King's College, London, and is a doctoral candidate at Ohio State University, where he is completing his dissertation on U.S. psychological warfare during the Korean War. During his USAR career he has completed psychological operations courses in the United States and the United Kingdom and in 1996 deployed in support of *Operation Joint Endeavor*, where he served with the PSYOP elements supporting 1st Armored Division and 1st Infantry Division.

Lieutenant Colonel Perkins, USA, is currently detailed to the Office of the Vice President, National Security Affairs, as a Military Advisor to the Vice President. He is assigned to the CI and HUMINT Directorate, Office of the Deputy Chief of Staff for Intelligence, Department of the Army. He has participated in various contingency operations including deployment to Panama, *Operation Just Cause*, and Bosnia Herzegovina during *Operation Joint Endeavor*, where he was the G2X (CI/HUMINT Mission Manager) in support of Task Force Eagle. Lieutenant Colonel Perkins holds a Bachelor of Arts degree in Psychology from the University of Vermont and a Master's degree in Criminal Justice from George Washington University.

Colonel Kenneth Allard, U.S. Army (Ret.), retired in 1996 from his position as Senior Military Fellow at the Institute for National Strategic Studies after serving on a special assignment in Bosnia with the U.S. 1st Armored Division. Col. Allard is also the author of two NDU Press books, *Command, Control, and the Common Defense* and *Somalia Operations: Lessons Learned*. A consultant and media commentator on information assurance and national security issues, he serves as a Senior Associate at the Center for Strategic & International Studies and an Adjunct Professor at Georgetown University.