C3I For Peace Operations: Lessons From Bosnia

Larry K. Wentz
Director, Center for Advanced Concepts and Technology
National Defense University
Fort McNair, DC 20319-5066

Abstract

Peace operations place different, and at times conflicting, demands on the supporting coalition military operation, the C3I infrastructure and the associated information collection, use and sharing. There are doctrine, culture and language differences that need to be coordinated and merged to achieve unity of effort. Unintended consequences accompany the use of advanced information technology and services. Information operations drive policy and doctrine. For Bosnia, the operation differed considerably from what the U.S. and other militaries had organized, equipped and trained for during the Cold War. Lessons from Bosnia provide a window to the future and an opportunity to improve the C3I support to peace operations.

1. Introduction

In February 1996, the Center for Advanced Concepts and Technologies (ACT) of the National Defense University (NDU) was tasked by the Assistant Secretary of Defense for C3I (ASD/C3I) to collect and report C4ISR lessons learned, analyses, and insights from the Bosnia experience. ACT's charge was broad, covering both the effectiveness of command arrangements and the effectiveness of the supporting C4ISR. The Joint Staff endorsed the effort and the J3 was designated the point of contact for the study.

This paper summarizes some of the study insights and lessons from Bosnia about the C2 structure, the information operations, the C3I implementation, the C3I networks, and the role of advanced technology. It concludes that there were several key problems that had to be overcome to make Operation Joint Endeavor (OJE) a military success. First, the Dayton Accord did not designate a single authority to synchronize the military, political, and humanitarian aspects of the mission and this was a risk to the success of the Implementation Force (IFOR). Second, 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 CIMIC units and personnel. The civil-military aspects did not receive sufficient emphasis during the planning and initial execution phase of the operation due to the emphasis on the military enforcement aspects of the Dayton Accord. Third, information operations for peacekeeping was also new for NATO. The NATO and SHAPE doctrines on public information and psychological operations had just been revised. The Public Information, Civil Affairs, and PSYOPS aspects of the IFOR information operations required special attention to ensure coordination and synchronization of related activities. Fourth, NATO had no ability to deploy forward it's C3I capabilities and therefore, had to rely on the national tactical systems of the framework nations (U.S. UK, and France), the UN VSAT network, and commercial products and services to extend NATO's strategic network into the Bosnian theater for which there was little to no commercial infrastructure.

The lessons from Bosnia re-enforced the importance of the information campaign as a force multiplier in peace operations. In addition, the humanitarian aspects of peace operations require close cooperation between the civil organizations and the military and this too, was re-enforced by the Bosnia experience. Finally, the IFOR operation was a success because of the professionalism, dedication and ingenuity of the men and women who were there and those who supported them.

2. Background

Operation Joint Endeavor was, of course, an operation 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 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 will involve, at least in practice, a consultative environment in which key parties will need to develop and maintain a common understanding of the mission, issues and progress towards meeting the end state. Planning and executing such operations are also 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 their desire to use systems that they are comfortable with, these operations typically begin with a "Kluge of Systems" with the inevitable interoperability challenges and security disconnects. This is simply the reality of such operations; NATO's Implementation Force (IFOR) had to address similar challenges in Bosnia.

In today's high technology environment, information operations determine the success or failure of the military operation. The "CNN effect" coupled with the "information revolution" creates 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 it's coalition member nations and as a matter of fact, the rest of the free world, provided an 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 emails to home from the troops in the field and Internet "home pages" were used by the 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 appraised 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 first-hand, 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. Finally, as a result of an improved ability to inform and influence, the Public Information Office and the IFOR Information Campaign became important tools of the Bosnia operation.

The intelligence community also faces challenges unique to supporting a coalition peace operation. Traditionally, intelligence tends to focus on the enemy. However, it is not always clear who and what is an enemy in a peace operation. Until recently, it has been the UN's view that information (intelligence) must be public to avoid misuse by any of the parties. The last several years of intensive involvement in complex operations has apparently changed their view. In combat as well as peace operations, the side with the best "situation awareness" has the greatest advantage. In a multinational setting such as Bosnia, there were, by definition, many sides. For IFOR, there were releasability issues related to sharing information and capabilities among 30 plus nations, which included the Russians, Partnership for Peace (PfP) nations, and others. Experience with other OOTWs, also clearly demonstrated that although nonintrusive means of collecting information were especially useful, human intelligence (HUMINT) was usually key. In Bosnia, the man and woman on the ground collecting first-hand information about the condition of roads and bridges, withdrawal of forces from the zones of separation, 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. In the end, information dominance was key to the success of the IFOR operation. 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 real "peacekeepers" in a peace operation are the humanitarian relief organizations that provide both 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 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 were more re-active than pro-active, especially during the early stages of the operation.

The humanitarian relief organizations tend to have limited communications and information system capabilities, especially in the theater of operation. Typically, they use the in-country telecommunications infrastructure to the extent possible but may also have their own HF and/or VHF radio's. These radio's, however, will most likely not be interoperable with the military systems they may come in contact with during peace operations. In Bosnia, the NGOs had reasonably good communications capabilities since they had already been in country for at least four years. They had access to the UN system and some of the PTT services in the country could be used as well. Some also had their own systems and they all had a common system to be used in case of emergencies. In regard to information capabilities, some organizations have laptop computers in the field and Internet home pages are being used more frequently outside of the theater of operation for sharing information. Finally, the humanitarian relief organizations also bring with them cultural and language differences that need to be dealt with by the military in order to avoid mis-understandings, unnecessary competition and mistrust.

Communicating and sharing information with the International, Non-Governmental and Private Voluntary Organizations (IOs/NGOs/PVOs) was a new experience for NATO. The need for the military and civil organizations to work together towards a common goal in Bosnia was not fully appreciated by the military. 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. On the other hand, many of the civilian agencies were consumed with problems in setting up their

own organizations and cooperation with IFOR was not their main concern. As a result, widespread civil-military coordination and cooperation did not really occur until the May 1996 timeframe.

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.

Coalition peace operations are accompanied by other doctrine, culture and language differences that challenge the overall coordination of the mission and ability to achieve unity of effort. Traditions, concepts, customs, and attitudes are sometimes not compatible and need to be coordinated. Although a common language (such as English or French) may be a requirement to participate, many of the players will not be able to speak or understand the language used, placing an added burden on the coordination activities. In Bosnia, PSYOPS and CIMIC doctrines differed. The U.S. approach to PSYOPS was to centrally manage and control at the highest level of command where as other nations, such as the Brits, 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 PSYOPS and CIMIC operations were run out of their respective headquarters in Sarajevo. Finally, with more than 30 different nations participating, there was a significant challenge to merge the cultural differences to achieve unity of effort and avoid "cultural clashes." Liaison activities (both officers and offices) became a very important way of doing business in IFOR and were used effectively to facilitate coordination and bridge the language gaps.

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 will be considerable.

3. Influencing Factors

Many factors influenced NATO and the coalition members preparation for and execution of the Operation Joint Endeavor mission. Some of these were:

- 1st time for a NATO-led out of area coalition operation supported by both NATO and non-NATO nations

- Limited NATO C3I capability to deploy out of area (the NATO Communications and Information Systems Contingency Assets Pool (NCCAP) and CJTF concepts were immature, they lacked SOPs for peace enforcement operation and they lacked agreed CONOPS and Doctrine for out of area operations)

- Dayton Accord did not designate a single authority to synchronize the military, political

and humanitarian aspects of the mission which handicapped coordination

- Uncertain planning environment (last minute mission change from withdrawal of UNPROFOR to peace enforcement, National plans close hold, Former Warring Faction (FWF) reaction to IFOR deployment unknown, torturous and mountainous terrain, land mines everywhere, snipers, potential for civil disorder, inadequate survey of facilities to be occupied by Hqs and communications and information system support activities)

- Limited theater infrastructure (telecommunications, power, material, facilities,...destroyed by the FWF activities)

- Operation different from what NATO and the participating nations organized, equipped and trained for during the Cold War

- Had to operate within the guidelines of NATO's peacetime procurement processes

- Ad hoc coalition, command arrangements politically driven, different abilities and experiences among coalition members and consultative environment (needed common understanding)

- National intelligence products and services provided to support the IFOR operation

- Extensive collaboration and sharing of information with coalition partners necessary to ensure mission success

- More extensive use of commercial products and services including accommodation of advanced technology test bed arrangements

- Peace enforcement and civil-military operations new for NATO, including working with the Non-Governmental and Private Volunteer Organizations

- Doctrine, culture and language differences of the some 30 participating nations

- "CNN effect" and "Information Operations" impact on military operations

- Parallel National C2 structures and systems and competing National agendas

4. C2 Structure

NATO's ability to influence events during the early preparation for IFOR deployment helped to avoid problems encountered by UNPROFOR and ensured a clearer definition of military tasks under a unified chain of command. This was largely attributable to the close involvement of NATO military planners with Contact Group negotiators prior to and during Dayton to ensure that realistic security tasks were incorporated. Consequently, the language hammered into the General Framework Agreement made it clear that IFOR "will 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 terms of reference highlight the paucity of authority for the High Representative. In any future operation that depends on the success of both military and civil tasks, NATO will want to ensure that its civil counterpart will also enjoy 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. The High Representative was not a UN Special Representative with UN authority. His political guidance came from a Steering Board of the Peace Implementation Council, which was not an internationally recognized political organization. Given the UNs 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, 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 also some U.S. related command arrangement shortfalls. Most significant was that the command relationships between NATO authorities, USCINCEUR and USAREUR were not well defined and this led to inefficiencies and confusion. At the center of this issue was how the Army (Component) fulfills its Title 10 responsibilities. The root cause of the problem was the absence of a U.S. JTF command equivalent that had the authority, expertise, and staffing to properly provide U.S. C2 and coordinated logistics for out of sector U.S service members. 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 inhibited flexible use of PSYOP elements at the tactical level. Another significant C2 shortfall was inadequate early coordination with humanitarian organizations, particularly NGOs.

4.1 IFOR Command Arrangements

The Allied Forces Southern Europe Headquarters (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 Allied Command Europe Rapid Reaction Corps (ARRC), NATO's rapid reaction force, was established as IFOR's Corps level land component command. The three framework nations (the U.S., UK 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. HQs IFOR was split between Naples and Sarajevo and the HQs ARRC was located at Ilidza near Sarajevo. The U.S.-led MND (N), with its HQs in Tuzla 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), with its HQs located in Banja Luka, was built around a British brigade along with troops from Canada, Netherlands and Denmark. Finally, the French-led MND (SE), with its HQs in Mostar was the smallest division and was comprised of troops from France, Italy and Portugal. Both the Brits 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 other 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 Combined Air

Operations Center (CAOC) in Vicenza and was responsible for the entire air effort, simplifying the C2 for air operations. The airlift movement control was exercised by the IFOR Regional Air Movement Control Center which was collocated with the CAOC, facilitating its 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.

An IFOR Commander for Support (C-SPT) was established in Zagreb, Croatia. His responsibilities included coordinating the sustainment, movements, medical, engineer 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.

4.2 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.

The integration of the 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 multi-national HQs and senior national officers were "dual hatted" as deputy commanders as was practiced in the Nordic-Polish Brigade.

The command arrangements for the Public Information Office (PIO), PSYOPS and CIMIC operations and some aspects of the Intelligence operations (e.g., Counter Intelligence) 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--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--conflicting IFOR and national doctrine, procedures and guidance on the nature and amount of information to be released to the media.

The CIMIC and PSYOPS operations also suffered command and control problems. The activities of the units deployed to the multinational divisions were managed and controlled from the headquarters operations in Sarajevo which caused operational problems for the local tactical commanders to which the units were attached. Finally, it was important that the activities of the PIO, CIMIC and PSYOPS be carefully coordinated. while at the same time preserving the objectivity of the PI and CIMIC

activities. A number of different coordinating mechanisms were used by IFOR, the ARRC, and the MNDs to accomplish this both internally and externally.

4.3 **Force Protection**

Force protection for U.S. forces will always be a significant issue in any military operation. In Bosnia, U.S. force protection took on a higher degree of importance than had been seen in other military operations. It was a formal part of the OPLAN mission statement and permeated all aspects of mission execution. Many IFOR participants believed that U.S. force protection measures were politically motivated and not based on a realistic threat assessment. 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 directly hampered civil-military cooperation activities and the ability for U.S. soldiers to move away from the peace enforcement only mindset. The second and third order effects of the stringent force protection measures were neither fully understood nor properly anticipated.

The Bosnia theater was more peaceful than expected. There have been few overt physical attacks on facilities and personnel. The FWF have generally been in compliance with the General Framework Agreement for Peace. One must be reminded, however, that the situation could change at a moment's notice for the worst.

Bosnia is a somewhat schizophrenic operational environment. On the one hand, it appears to be a hostile fire zone and on the other a garrison operation. 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 employed limited traditional lethal and physical protection such as heavily armed guards, tanks, barriers, sandbagged bunkers, and obstacle courses in access area. MND (N) relied on an electronic system to protect its high technology command center (referred to as Battlestar). The system, known as Shortstop and developed by Whittaker Corp., generated an electronic umbrella that would prematurely detonate a proximity-fused artillery shell should some hostility start again.

Upon arrival in country, IFOR made it very clear to the FWF at the outset that they were different than UNPROFOR and were there to enforce compliance with the Dayton Accord, including the use of force if necessary. Check points were bulldozed, road blocks shut down and 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 Zone of Separation, and unauthorized police check points. 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.

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 anytime 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.

5. Information Operations

Peace operations can place different and, at times, conflicting demands on information collection, use and sharing. On the one hand, the military views information (generally refereed to as intelligence) as a force multiplier and requires that it be protected and selectively released to coalition partners under well defined rules and control. On the other hand, the United Nations views the collection and storage of information to be public, open and transparent in order to avoid misuse by any of the parties and to preserve the impartiality and credibility of the UN. These competing principles can impose limitations on information collection and storage in support of UN-led peacekeeping operations. Fortunately, this was not the case for the NATO-led Operation Joint Endeavor.

5.1 Public Information

Public information is a critical element of mission accomplishment for peace operations. First, a successful public information campaign contributes to building and preserving public support for the operation. Second, the successful use of public information can help the commander achieve operational goals by influencing parties, resolving crisis, defusing misunderstandings and/or correcting misperceptions. Such use of the public information "weapon" is more critical in peace operations where the traditional military tools (weapons) have a less central role in military activities. For Operation Joint Endeavor, public information became a powerful tool in shaping the operational environment.

Upon arriving in theater, IFOR troops faced serious public information challenges. IFOR succeeded a discredited UN mission and needed to distance itself from the poor image the UN gained during the four years of UNPROFOR. A large number of media were already operating throughout Bosnia and Croatia independent of the military and were able to report instantaneously most incidents, in some cases before they were reported to IFOR. In addition to IFOR, there were seven other organizations tasked with implementing the Dayton agreement. Hence, cooperation was essential to enhance the credibility of IFOR and the international community among the international and local press.

From the outset of the operation, IFOR's public information activities achieved a generally high standard of information exchange with the media. International and national media coverage was generally positive or neutral. Reporters in theater expressed satisfaction with IFOR's policies and procedures and the military spokesmen achieved a high level of credibility.

IFOR effectively used public information to communicate to the parties their intentions and military power. It was used by the commanders to get the local population to behave less belligerently and to convince them that a brighter future awaited them if the Dayton agreement were fully complied with. Finally, IFOR relied heavily on public information to deter the FWF violations of the military annex to the Dayton agreement and attacks on NATO troops.

5.2 Civil-Military Cooperation

Civil humanitarian relief organizations are accustomed to autonomy and operating according to their own charters and core values. The military is an instrument of a national polity and follows its orders. Although it is not a natural relationship, these organizations need to be able to work together towards a common goal in support of the humanitarian aspects of peace operations.

For Bosnia, there were a number of factors that contributed to the lack of proper civil-military planning and operation. Before the IFOR deployment, there was no common understanding

of the capabilities, limitations, roles, and mission of CIMIC units and personnel. In the absence of an agreed NATO doctrine, IFOR commanders and staff had to incorporate civil-military tasks into their overall operations based upon personal knowledge and experience. The individual commander's execution of the CIMIC mission reflected the various national approaches of the participating nations. For example, the Russian approach tended to be more peace enforcement or counterinsurgency oriented. France and the UK were much more active in assisting civil organizations with direct support to local "hearts and minds" projects. The U.S. approach was more "high intensity" and stressed the need to achieve decisive "victory" and quick resolution of conflicts through securing popular support. The IFOR deployment illuminated the ground combat commanders limited knowledge and experience with civil affairs activities. This lack of knowledge was demonstrated in many areas, but was particularly obvious in the campaign planning stage. During the development of the OPLAN, there was only one Civil Affairs officer assigned to assist AFSOUTH in planning for the IFOR deployment. The campaign plan not only inadequately identified military tasks for CIMIC, but due to the lack of planing knowledge, negatively impacted CIMIC deployment, manning and communications, and the development of information and logistics support requirements.

Civil cooperation in Bosnia was unique in that members of the non-governmental and supra-governmental relief and development organizations were already actively engaged when the IFOR deployment commenced. In fact, there were an estimated 530 IO/NGO/PVO personnel in theater at D+1. This situation created its own set of problems. First, CIMIC assets were delayed in their deployment. As UNPROFOR forces withdrew or were transferred to IFOR, valuable CIMIC turnover opportunities were lost. Lacking any advanced information on how the CIMIC mission would be executed, the NGOs assumed that IFOR would continue, if not increase, the same type of support that UNPROFOR provided to them. The philosophy advanced by IFOR, however, was quite different from UNPROFOR's. IFOR refused to provide what it thought the NGO community could provide for themselves. There was a fear that providing such support would create a long term dependency on IFOR. Paramount in this philosophy was the promotion of self-sustaining activities in preparation for IFOR's eventual withdraw. The ARRC did send personnel in early to brief the NGOs on what to expect, educate them on what IFOR troops would being doing and related plans. This briefing was only given in Sarajevo and not in the field where a majority of the NGOs were located.

A Combined Joint Civil Military Cooperation staff element was implemented at IFOR headquarters to facilitate coordination of CIMIC activities and cooperation with the IOs/NGOs/PVOs. The CIMIC organization was to focus on liaison with the civilian organizations from the government down to the local opstina level to regenerate national regulations and institute some limited nation rebuilding. The structure was also to provide an avenue for the numerous aid agencies to deal with the military on support arrangements related to their projects in theater. CIMIC Centers were established at all levels of the IFOR command structure to provide a location for NGOs to meet with the military. In Sarajevo, both IFOR and ARRC had CIMIC activities and this created some confusion with the NGOs who preferred to deal with the one in-charge. A Joint Civil Commission was established to facilitate interactions between the military and civil agencies on Dayton Accord civil matters and humanitarian assistance activities. A Joint Military Commission was also established for dealing with the FWF on Dayton Accord military matters.

CIMIC activities at MND (N) best epitomize the combined impact that doctrine, command

structures, and mission interpretation have on the promotion, or prevention, of civil coordination. The CIMIC Center, which doctrinally was the central location for all NGOs to meet with the military, was located inside the gate at Tuzla, whereas most of the NGOs were downtown Tuzla. Since access to the base by non-IFOR personnel was strictly limited, the effectiveness of the CIMIC Center as a tool for coordinating NGO and military activities was greatly reduced. The force protection measures hampered CIMIC personnel in their ability to make on-site visits--required them to muster up four vehicles just to be able to leave the base and the heavy military presence (full battle gear) did not contribute to creating an impression among the local population that the internal situation was improving.

Despite these short comings, CIMIC personnel were able to effectively coordinate with the NGOs. Across the theater, CIMIC officers praised the efforts and working relationships with the NGOs at the tactical level. Successful coordination at the theater level, however, was less forthcoming. The lesson to be learned is that in operations where civil implementation of the overall objectives plays a key role, civil affairs assets have an important, timely role to play. This point was highlighted in the April, 1996 quote from Admiral Leighton Smith, COMIFOR, in which he said, "In November we never heard of CIMIC. We had no idea what you did. Now we can't live without you."

Under the Dayton Agreement, the Office of the High Representative (OHR) was tasked to coordinate the activities of the civilian organizations in Bosnia to ensure the efficient implementation of the civil aspects of the agreement. The OHR was also to remain in close contact with the commander IFOR to facilitate the discharge of their respective responsibilities. The civilian institutions began operation under considerable disadvantages. They had to be created, funded, and staffed in country after the military deployment occurred. This delay caused public pressure to be applied to IFOR, demanding that IFOR take on a larger role in implementing civil tasks. This public pressure resulted in a limited self-fulfilling prophecy. Once the OHR established itself in theater, the impression created was that where the OHR should have been taking the lead on projects, such as providing gas, electricity, and water, it was expecting that IFOR would take the lead. As a result, "mission extension" was a natural occurrence because of the competence and ability of the CIMIC organization.

5.3 PSYOPS

Psychological operations are an operational tool (under the G/J-3) designed to shape target audiences' perceptions so that they create the least possible interference with friendly forces. For the IFOR operation, the PSYOP campaign was called the IFOR Information Campaign because of political sensitivities to the use of the term psychological operations by some of the coalition partners (the French, in particular, due to political and historical reasons associated with the Algerian conflict in 1961).

The Combined Joint IFOR Information Campaign Task Force (CJIICTF) was established to take over the PSYOP aspects and focused its efforts on convincing the local population and FWF of the Dayton Agreement's good intention by laying out the truth. The PSYOP personnel (mostly U.S., UK, and Germany) remained under national command and control and product developed also required national approval. This parallel command relationship caused C2 problems in executing the IFOR Information Campaign.

A number of challenges were encountered in the execution of the PSYOP mission. The CJIICTF mission statement and "commander's intent" did not get distributed to all of the appropriate levels

of the command structure. Command relationships were not always clearly articulated and/or implemented. The product approval process was cumbersome and the product distribution slow. Finally, the communications support was limited and in some cases inadequate to support the mission. These limitations hampered the ability of some PSYOP teams to accomplish their mission since the scope, content, intent and execution of the PSYOP campaign was not always clearly explained to them and they did not always have the necessary tools to execute. Despite these short comings, the overall PSYOP mission, in general, was successful.

Tactical PSYOP teams were deployed and attached to the subordinate command elements they supported. The mission of the teams was to disseminate pre-approved PSYOP products to the local population, broadcast loudspeaker messages, and disseminate command information. The teams also conducted assessments of the area of operation and made contact with the local media sources to gain information for the CJIICTF.

The centralized PSYOP product approval, production, and distribution process was cumbersome and in many cases, did not meet the needs of the tactical PSYOPS mission. Products that had a high degree of receptivity at the strategic level and targeted for the broader Bosnia-Herzegovina population were not always well received at the tactical level and by the local population. Furthermore, a number of the products were too "American" and did not reflect the European advertising traditions prevalent in the Bosnia region of the world. There were also distribution problems which resulted in some time sensitive information getting to the local population too late to have the desired effect. The tactical teams needed some freedom and flexibility to tailor and produce products for use with their local population.

The command and control relationships needed to be more clearly articulated, disseminated to the elements involved, and consistently implemented. Additionally, changes, caveats, or exceptions also needed to be made clear to all organizations effected. In the cases where there was an absence of clear guidance, this hampered the execution of the PSYOP campaign. For example, if the PSYOP team chief was made a part of the battle staff, then they became a "player" in the planning and coordination of the mission and used effectively in the accomplishment of the mission. PSYOP teams were less effective in situations where they were subordinated to the S-5 and/or did not attend the commander's battle-update-briefs. Working for the S-5 essentially turned PSYOP into a Civil Affairs support activity. Hence, the team chief needs to be the principal PSYOP advisor to the commander in order to fully support their supported unit.

The tactical PSYOP teams relied almost solely on the units they supported for their communications. This left them, in many cases, with very limited to no means of communicating with their higher headquarters. FM communications was to be the means for the teams to communicate but in the mountainous environment of Bosnia, FM communications was nearly impossible. Other means such as VSAT, INMARSAT, and MSE were used for routine support and in the end, they had to, generally, rely on the use of others phones. In the data networking area, the supported unit's local LAN system did not have spare Ethernet cards and adapters for use by PSYOP personnel to connect their equipment to the LAN. They, also, did not bring any connection equipment with them when they deployed. Hence, here too they had to rely on others to access the LAN for communicating with higher headquarters. Internet was also used as a back up when they could get access. At times, it took several hours to reach headquarters elements and them to reach the deployed teams. The most reliable means of communication, the

courier, often took days. PSYOP teams were not high on the priority list for access to the supported units very limited tactical communications and they did not have their own organic tactical communications. The urban nature of the mission required the teams to split up and conduct operations often indoors as well as outdoors and in areas such as crowded markets. The lack of adequate communications for the dismounted operations became a force protection issue. Handheld radios were eventually delivered but without instructions on how to program them. They proved useless and were subsequently sent back.

5.4 **Information Coordination**

Coordination of the IFOR Information Campaign was ensured through several different mechanisms both internal and external. At the IFOR and ARRC headquarters level, a Joint Information Coordination Committee was set up to coordinate the activities of the PI, CIMIC, CJIICTF and major civilian agency spokesmen. This group met weekly to inform each other of ongoing activities and future plans. It also allowed them to ensure that their messages did not conflict and to prepare common strategies. The ARRC established a Chief Information Officer who was responsible for the daily coordination of the PI and CJIICTF activities. The ARRC established other coordination activities such as the ARRC Perception Group and the ARRC Information Coordination Group to review messages. strategies, and trends associated with the information campaign. Both formal and informal coordination mechanisms were also established at the multinational divisions.

Coordination also took place with the civilian organizations responsible for implementing the civilian annexes of the Dayton Accord. These organizations included the Office of the High Representative, the UN High Commissioner for Refugees, the Organization for Security and Cooperation in Europe, the UN Mission in Bosnia-Herzegovina, the International Police Task Force, the World Bank, and the International Criminal Tribunal--Yugoslavia. In early spring of 1996, the OHR, UNHCR, UNMIBH, OSCE, and to a lesser extent the World Bank agreed to participate with IFOR in the daily briefing to the press.

There was also a need for IFOR to accommodate daily national reporting to their respective national authorities. Contingents fulfilled this dual requirement by sending Situation Reports to IFOR and their respective MoDs. This did not happen, however, without creating some difficulties for IFOR. In some cases, information was formally released to the international press, both by contingents in theater and by home nations, without IFOR prior knowledge.

5.5 **Information Services**

The pervasive use of commercial off-the-shelf (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 email and a reduced reliance on formal messaging. The formal message traffic (the NATO TARE message network) by volume (Mega-Bytes per day) was less than 10% of the total IFOR daily data network traffic. The VTC was used daily by IFOR and ARRC command elements for collaboration and coordination. The VTCs were also used by subordinate elements to conduct day to day business. Powerpoint briefings were used to inform and were readily distributed over the data network. The data networks were also used for collaborative planning and distribution of wideband information such as images.

The new capabilities provided the opportunity to share information more efficiently and faster (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, who had a vested interest, in the dark. Generally, the problem was not the lack of information but rather finding the useful details among the wealth of information available.

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 sharing. This was particular true in the area of coordinating, integrating and fusing intelligence, surveillance, and reconnaissance capabilities and making this information available to the user who needed it when he needed it. 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 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 email, 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% probability 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 Hqs 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 level. Every U.S. base camp had telephone service and secure and non-secure data and email capabilities. On the other hand, the communications and information system support to the IFOR warfighter who was actually executing the peacekeeping mission, with few exceptions, changed very little and they continued to operate much as they had in the past. Operations were conducted using acetate-covered 1:50,000 maps, outmoded tactical equipment and sensor or reconnaissance systems organic to 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, of course, exceptions. Many innovative uses were made of the U.S. military's array of advanced technologies (mainly in the areas of Intelligence, Surveillance and Reconnaissance (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. Some of the technologies that made this possible are discussed later in the section on the role of advanced technologies.

5.6 **Operational Security**

Finally, the Operational Security (OPSEC) aspect of information operations is particularly challenging for peace operations where the

operational environment can be reasonably stable, as was the case in Bosnia. The lack of an obvious threat can create a relaxed security posture. During IFOR, an enormous amount of classified and unclassified material was produced; extra care had to be taken when dealing with mixed classifications of information. There was a lack of security devices such as secure telephones, safes, and shredders. Other types of OPSEC risks had to be managed as well. There were numerous television and print journalists questioning soldiers. The soldiers had to be briefed to ensure they did not release classified information to the media. On a daily basis, hundreds of local national workers entered IFOR areas of operation. It was a challenge to keep a close eye on these daily visitors. OPSEC is an operations function, not a security function per se. Therefore, there must be a proponent for OPSEC functions and the functions must be integrated into the planing and execution of the operation. OPSEC proponency for IFOR was not clearly defined.

6. C3I Implementation

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 System (CIS) ever built to support a major peace operation.

Peace enforcement had never been attempted by NATO. 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 and implementation activities. AFSOUTH and SACEUR OPLANs reflected differing perspectives on CIS management. The Dayton Agreement assigned frequency management responsibilities to IFOR even though it had no established capability. This caused CIS organizational problems at the outset for IFOR CJ6 and resulted in the ad hoc creation of a Theater Frequency Management (TFM) capability to address the Dayton Agreement tasking and a Combined Joint Communications Control Center (CJCCC) to facilitate coordination and focus the planning and management of the CIS aspects of the IFOR operation.

The operational scenario for Joint Endeavor was unclear and national planning was being kept close hold. Hence, who was going where, with what equipment, and when was unclear to the NATO planners. There was also a lack of timely political planning guidance which caused last minute changes to bring the CIS plan in line with new policy decisions.

The communications and information needs of operations such as the Public Information Office, IFOR Information Campaign, Engineers, PSYOPS, CIMIC, Counterintelligence, and HUMINT were not well understood at the outset of the operation. Therefore, the requirements were not articulated to the CIS providers so that adequate services could be made available to support their 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 Hqs IFOR at the Residency. The CIMIC and some HUMINT operations vehicles (not those in MND (N) since these vehicles were equipped with national systems) lacked radios for communicating while operating in the country. The Engineers also generated a requirement for force protection communications since they too were frequently scattered throughout the country. The Engineers, 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. For example, the PIO could also use the Internet to get English translations of Croatian and other international press releases and news articles. Timely transmission of Combat Camera and HUMINT digital camera and video products and the integration of these products into the information operations network were also problems faced early on in the operation. Adjustments had to be made after the fact resulting in service that was not as good as it could have been had the needs had been incorporated into the initial planning and implementation efforts.

Surveys of Hqs and communications sites were incomplete. 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.

To add to the operational challenges, critical portions of the Bosnian infrastructure such as power and telecommunications had been destroyed and there were land mines, booby traps and snipers to be dealt with. Hotels, restaurants and stores had been destroyed so the caring, feeding and billeting of the CIS support forces needed special consideration. Finally, there was no indication of how the FWF would react to the IFOR deployment.

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, preauthorized 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. Pragmatic and unconventional steps were taken to procure these 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" 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 Marine Expeditionary Unit remained an option and had to be considered in the development of the CIS architecture.

Due to the lack of Bosnian telecommunications infrastructure (including no cross-IEBL communications links), mountainous terrain, and the associated high cost of clearing land mines and providing force protection for mountain top radio relay sites, an extensive 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 (35 U.S. TACSAT, 5 NABS and 9 UK VSC-501). The terminals were collocated in urban areas at the major headquarters facilities and were provided force protection. 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 area of operation as well.

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, i.e., both for the providers and users of the information services. 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 were 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. In the early phases of the IFOR operation, CIS was in a permanent state of flux. The task of establishing a clear picture of the CIS architecture proved to be a major challenge. 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.

7. The IFOR C3I Networks

In preparation for the execution of OPLAN 40104, the extraction of UN forces, a leased E1 (2 MB/S) network was extended by SHAPE into Croatia and Hungary. By the end of May 95, 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. With the signing of the Dayton Peace Agreement on 14 December 95, 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.

IFOR CIS services were provided by a complex mixture of NATO, national, UN, and civilian or commercial networks and components. The NATO CRONOS Wide Area Network and the Interim ARRC CIS network (both client-server architectures, employing Microsoft office for office automation and providing email service) provided valuable crisis response and Command and Control capabilities for the IFOR operations. 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. The voice network was an ad hoc integration of NATO and national strategic networks, national tactical systems, the UN VSAT network, and the Croatian and BiH PTT networks where available. Unclassified INTERNET was also used frequently and demand for service increased throughout the operation. INTERNET use was not planned, its use simply grew with user demand.

The U.S. LOCE system was extended to Division Hqs 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 good quality. The air picture in the CAOC, made up from a variety of sources, was of particular high quality. However, there was no overall integrated maritime/air/land picture.

Network and system management of IFOR's Communications and Information networks

proved to be a major challenge. An IFOR organization structure had to be created, agreed, and staffed quickly. The U.S Joint Pub 6-05 provided the basis for the establishment of the Combined Joint Communications Control Center (CJCCC) to manage IFOR's networks. A Theater Frequency Management capability had to be established. 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 & Support Agency (NACOSA), the AFSOUTH ACOS CISD, the IFOR CJ6, the CJCCC, the ARRC G6, the MND G6's and national J6's, who's roles and relationships needed to be established and their activities in support of the operation coordinated. There were overlaps in 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. 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 exists for interfacing strategic and tactical digital 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 securevoice equipment and was used extensively by IFOR. A large number of the U.S. forces that deployed to Bosnia brought with them STU-IIIs which were not interoperable. The Interim Digital Interface PTARMIGAN (IDIP), designed by the UK 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 ADAMS movement control system and JOPES required a manual interface for exchanging information. NATO Exercises such as INTEROP 95 served to help 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.

Problems with viruses were experienced not only with the CRONOS and IARRCIS but also with most computers brought into the theater. Virus detection and correction measures were put in place as well as a user information awareness campaign. In addition to viruses, dust and dirt caused problems with disk drives creating the requirement for protective measures. Commercial power failures and fluctuations caused major CIS outages for those sites that did not have a UPS capability. 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, liaison teams were provide to non-NATO units assigned to IFOR such as the U.S. INTEL team with the Russian Brigade and the U.S. provided STU-IIB's for the PfP nations supporting the operation. In regard to the latter point, it was suggested that NATO consider the use of commercially available

security products to support future peace operation security needs.

7.1 Transfer of Authority

There was a Transfer of Authority (TOA) from AFSOUTH/IFOR to LANDCENT/IFOR on 7 November 96, from the ARRC to LANDCENT/IFOR on 20 November 96, and from IFOR to the Stabilization Force (SFOR) on 20 December 96. These TOA's were accompanied by a large personnel change along with changes in the CIS infrastructure. LANDCENT had been planning for the transition for several months with "right seat" handover training being initiated in late September 96. 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.

In addition to the withdrawal of the framework nation CIS systems, the TOA to LANDCENT also required some reconfiguration and redeployment of the CIS infrastructure, some of which was for AFSOUTH's use. Therefore, CIS equipment essential to the HQs of the LANDCENT Component Commander had to be replaced. NATO HQ staff needed to be convinced that equipment already procured for IFOR could not be used to meet LANDCENT requirements. This raised the significant and on-going challenge of equipment accountability. Despite the questions of eligibility, NATO common funding of CIS infrastructure was approved and procurement initiated. For strategic and theater CIS connectivity, a rationalization and re-balancing of the networks was necessary to reflect the move of the operational center to Sarajevo and the greatly reduced role of AFSOUTH.

There were also unintended consequences of the TOA to LANDCENT. 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 removed as well. 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.

7.2 Commercialization

IFOR's plan for the commercialization of their communications network was aimed at reducing the costs to NATO, allowing for the timely withdraw 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 Hqs locations, expand the commercial VSAT/IDNX network and lease E1 connectivity from the BiH and Croatian PTTs. The evolution of the commercial services network (referred to as the IFOR Private (Peace) Network (IPN)) was slower than IFOR would have liked. The main difficulties centered around the slow reconstruction of the BiH PTT infrastructure and the continued unwillingness of the FWF PTTs to provide cross-IEBL connectivity.

The CIS challenge for the future will be to transition major in-theater communications links from the tactical military systems to civilian leased bearers and establish a viable SFOR integrated digital services network based on commercial products and services--the objective of the IPN. The ability to achieve such a capability depends on the speed with which reconstruction of the internal national telecommunications infrastructure can take place, the political will of the national leadership and the Croatian and BiH PTTs to make it happen, and the timely availability of funding to support the reconstruction.

8. Role of Advanced Technologies

A wide range of the U.S. military's advanced technologies were deployed to the Bosnian 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 a phone call was made, a radio message sent, or something moved on a Bosnia highway within an "area of interest" the odds were that it was tracked.

Some of these technologies were also 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 Apache helicopter gun-camera videos were used to verify compliance with the Dayton accord. Digital cameras and hand-held video cameras were used by HUMINT teams to record compliance and/or non-compliance situations, to record the conditions of roads and bridges and to document intelligence and counterintelligence related events. Night-vision equipment and GPS range finders were used for night time surveillance operations. In fact, GPS continued to be an important capability and was also used for marking the Inter-Entity Boundary Line and the Zones of Separation, for vehicle tracking, and for precision navigation and position identification.

The Bosnia C2 Augmentation System was deployed to provide improved wideband connectivity and broadcast information services to accommodate 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 Hqs. UAVs, such as Predator and Pioneer, were used extensively for monitoring important areas of interest such as grave sites, troop movements and demonstrations. AWACS, JSTARS and other capabilities were employed to provide IFOR information that could be used to demonstrate to the FWF that they could be seen anytime of the day or night and under all weather conditions and that compliance would be closely monitored.

The Army fielded the most advanced telemedicine system in history to provide medical care to U.S. forces in Bosnia and Hungary. The high bandwidth system (up to 4 megabits/sec) supported applications such as telesurgery, telemedicine, telepsychology, and teledentistry.

The Joint Total Asset Visibility (JTAV) system, was another advanced capability deployed to Hungary and Bosnia to track assets, whether they are on order from a supplier, in transit or in storage. JTAV was not the only asset visibility system deployed. There was one developed by the Volpe Transportation Center that used RF tags and GPS and the International Transportation Information Tracking (Intransit) 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 commanders, in particular, reported that their deployment to Bosnia was followed by a virtual "flood" of new technologies. These technologies were generally inserted incompletely and imperfectly. Many of the new systems and

technologies were deployed without doctrinal support or concepts of operations. 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. Both initial operations and maintenance capabilities had to be provided by contractors or research personnel. Even so, these new technologies reportedly made excessive demands on 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. Hence, one of the major challenges the U.S. and IFOR faced was the integration of these capabilities and systems into the operation and being able to exploit them to the maximum extent possible. As noted earlier, the operational integration was not accomplished as effectively as the commanders in the field would have liked to minimize the impact on the day to day operations and to allow them to fully exploit the capabilities of the systems deployed.

There were Air Force and Army initiatives 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 Combined Air Operations Center (CAOC) in Vicenza, Italy and was used for rapid problem solving and system integration testing of new capabilities before operational deployment to the theater. There was a 24-hour hotline 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 Material 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 it's 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.

A clear lesson from Operation Joint Endeavor was that 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.

9. **Observations**

A lot has been learned from Operation Joint Endeavor that can be applied to Operation Joint Guard (SFOR) and future peace operations. Some have particular significance for future NATO operations and the realization of their CJTF and NCCAP concepts. Others can be applied to coalition peace operations in general. The following are some of the early findings and related C3I lessons learned:

- IFOR was a successful NATO military operation.
- NATO successfully implemented and maintained a complex military-civil C3I network.
- NATO and Russia worked together successfully in support of a major peacekeeping operation.

- In future operations that depend on the success of both civil and military tasks, NATO and others will want to ensure that their civil counterparts also receive the authority necessary to fulfill their responsibilities.

- In operations in which civil implementation of the of the overall objectives plays a key role, civil affairs assets have an important, timely role to play.

- The requirements of the PIO, CIMIC, PSYOPS, CI/HUMINT and other special activities need to be made known up front so that adequate CIS services can be provided.

- Public information is a critical element of mission accomplishment for peace operations and was an effective force multiplier for the IFOR operation.

- The current technology insertion process is incomplete and imperfect. It requires a more coherent and disciplined process to ensure that military value is achieved from the introduction of advanced technology in an operational environment.

- 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 in order to more effectively support the troops who are actually executing the mission.

- Advanced 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.

- Complex command arrangements and "Kluge of Systems" for the C3I laydowns are a reality for these types of operations. They need to be factored into the planning, implementation, and operation phases of similar future operations.

- Theater CIS infrastructure is likely to be limited in future operations. This needs to be reflected in the planning process.

- NATO needs the capability to more effectively deploy forward communications and information systems in support of peace operations. The realization of the NCCAP and CJTF concepts is a way to achieve this capability.

- Integration of what you get, not necessarily what you need is a way of life for such operations and needs to be factored into the planning for and training for similar future operations.

- A dynamic planning environment is a reality for such operations and needs to be made a part of the training for future operations.

- Interoperability continues to be a challenge. Even though progress is being made, there is still a long way to go to achieve seamless operations for the communications and information systems. Innovative exercises and adherence to standardization are means to this end.

- Security disconnects and releasibility issues exist as a result of the ad hoc integration of disparate systems. More extensive sharing of information and collaboration have become the norm for doing business. These are important considerations that need to be addressed as NATO moves into the "information age."

- OPSEC procedures and responsibilities need to be clearly defined and enforced to prevent security compromises.

- NATO's peacetime procurement process is too complex and slow to meet the demands of peace enforcement operations. Consideration needs to be given to appropriate modifications that will accommodate the requirements of the operational commander while satisfying procurement oversight requirements.

- Increased reliance on commercial products and services is a reality that needs to be more effectively incorporated into the CIS architectures, planning, procurement, contracting, and training for peace operations.

- Dust, commercial power failures, and software viruses are a reality, caused problems for IFOR operations and need to be factored into the planning for future operations to minimize their impact. While most of the viruses detected were relatively benign, their ubiquitousness underscores the vulnerability of the information systems to systematic hostile attack. NATO needs to carefully examine the Defensive Information Warfare needs of future information systems to be deployed in support of peace operations and incorporate the necessary defensive capabilities to reduce their vulnerabilities to potential hostile actions.

- Exercises and training are important. The nature of the deployment required personnel to be more flexible and multidisciplinary. Use of advanced technologies and commercial products and services required more extensive "on-the-job" training and the need to set up a special school at NATO's Latina training facility to provide the requisite skills for this operation. Exercises such as INTEROP 95 also demonstrated the value of setting up the expected C3I 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 to support out of area peace operations. Realization of the CJTF concept and accommodation of appropriate aspects of the IFOR CJCCC concept employed to support Operation Joint Endeavor are steps in the right direction to improve NATO's ability to more effectively respond and manage its deployed CIS resources for future operations.

10. **Bottom-line**

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. Realization of NATO's CJTF and NCCAP concepts are means to an end to strengthen the Alliance's ability to respond and improve its C3I capabilities in support of out of area operations.

A quality information campaign and effective use of civil-military cooperation are key to the success of OOTW operations. Agility and accommodation are also key as well as some plain old good luck.

C3I interoperability continues to be a challenge not only among the military coalition systems but also with the civil organization systems such as those used by the IOs, NGOs, and PVOs. Innovative exercises and adherence to international standards are means to improving the situation as the world moves into the "information age."

For the future, however, one should remember that potential adversaries of the NATO Alliance and the U.S., in particular, will not be so foolish

as to neglect glaring weakness in the C3I networks implemented in support of the IFOR operation. Active countermeasures against the C3I networks may be the case in future operations. 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.

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 Peace-keeping 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, DSA, and Michael Casey, CISA. *C4ISR Laydown.* CISA Architectures Directorate, Washington, D.C., 1997.

[Berry, 1996] Col Thomas Berry, USAF. *Operation Joint Endeavor: Executive Lessons Learned.* HQ Air Mobility Command, Scott AFB, Il, April 1996.

[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] Willian B. Buchanan. *Operation Joint Endeavor-Description and Lessons Learned (Planning and Deployment Phases).* IDA, Alexandria, Va, November 1996.

[Cook, 1996] Capt Rhonda Cook, USA. *AAR Operation Joint Endeavor 1st AD Intelligence Production.* HQ Task Force Eagle, Tuzla, BiH, 1996.

[CJCCC, 1996] Combined Joint Communications Control Centre. *CJCCC Information Book, CJCCC Onformation Book (D+180), and CJCCC Information Book (TOA LANDCENT).* HQ IFOR/AFSOUTH, Naples, Italy, 1996.

[Dziedzic, 1996] Col Michael Dziedzic, USAF. *CIMIC and IPTF in Bosnia (Draft).* National Defense University, Institute for Natioal Strategic Studies, Ft McNair, Washington, D.C., 1996.

[Feist, 1996] CAPT Peter Feist, GEN. *Joint Analysis Team Interim Reports: IFOR Lessons Learned.* JAT Press, Northwood, England, 1996.

[Gerald, 1997] LtCol Jeffrey Gerald, USAF, and John Christakos, Booz-Allen & Hamilton, Inc. *BC2A: Lessons Learned in Bosnia.* DARO, Washington, D.C., 1997.

[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, MITRE, and Anthony Simon, CISA. *Compendium of Operation JOINT ENDEAVOR Lessons Learned (Draft).* CISA Architectures Directorate, Washington, D.C., September 1996.

[Hairell, 1996] LtCol Oscar Hairell, USAF. *OJE Lessons Learned.* HQ USAFE, Ramstein AFB, 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.

[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.

[Mohr, 1996] Brad Mohr. *SOF Mission Support Lessons Learned.* HQ SOCOM, 1996.

[Nabors, 1996] BG Robert Nabors, USA. *Operation Joint Endeavor Lessons Learned. HQ* 5th Signal Cmd, 1996.

[Palmer, 1996] Maj Rolf Palmer. *LOCE Lessons Learned.* HQ USEUCOM, 1996.

[Phillips, 1996] LtCol Timothy Phillips, USMC. *JITC C4I Infrastructure Documentation Report for Operation Joint Endeavor.* JITC, Ft Huachuca, Az, June 1996.

[Rapaport, 1996] Richard Rapaport. *World War 3.1.* FORBES ASAP, October 1996.

[Riley, 1996] Col Steve Riley, USA. *Bosnia-Herzegovina After Action Review, Preliminary Panel Findings.* Army War College, 1996.

[Roberts, 1996] Cdr T Roberts, USN. *IFOR Intelligence Sharing: Successes and Challenges.* 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.

[Stewart, 1996] George Stewart. *CNA Involvement in Joint Endeavor.* Center for Naval Analysis, October 1996.

[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 Endeavour Lessons Learned.* SHAPE ACOS CISD, Mons, Belgium, October 1996.

[Walley, 1996/1997] Jim Walley. *Lessons Learned from Operation Joint Endeavor.* Center for Army Lessons Learned, 1996/1997.

[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.

[Wentz, 1996] Larry K. Wentz. *Managing The Peace Offensive: Coalition Operations Lessons Learned.* AFCEA Europe Brussels Symposium and Exposition, Brussels, Belgium, October 1996.

[Wentz, 1996/1997] Larry K. Wentz. *Bosnia C4ISR Lessons Learned Database, Briefings and Draft Reports.* National Defense University, Center for Advanced Concepts and Technology, Ft McNair, Washington, D.C., 1996/1997.