Information, Analysis, Intelligence:
A Critical Challenge for 21st Century Operations

Version published as
"Intelligence Challenges of Civil-Military Operations,"
Military Review, September/October 2001, pages 45-52

by

Adam B. Siegel

Senior Analyst

Northrop Grumman Analysis Center

1000 Wilson Blvd., Suite 2407
Arlington, VA 22209
703-875-0005
siegead@mail.northgrum.com

Abstract

The international community has intervened many times in recent years amidst complex emergencies deriving from some form of armed conflict. In these operations, military commanders have discovered numerous obstacles and requirements different from what they might have expected in a "traditional" war-fighting operation. The arenas of information, assessment and intelligence present some of the greatest changes. This article examines some of these changes, with a particular emphasis collecting information on and analyzing changes in the civil sector as part of the military operation. The article suggests some command and control developments to deal with the information, analysis, and intelligence challenges that a military commander will encounter in a complex emergency.

Setting the Scene[1]

It is the summer of 1994. You are a US Army officer. You have a problem. Although a career artillery officer, you are assigned to run a brigade Civil-Military Operations Center (CMOC) if the United States invaded Haiti. You know nothing about Civil Affairs, about Haiti, or about CMOCs—time to start your crash course.

As you progress in your self-education, you realize that you have no information on the civilian actors in the Brigade's area of operations. You know nothing about the mayors, the school principals, local administrators of public services, relief agencies, or even where international relief agencies have warehouses.

You go to the Brigade intelligence officers. They don't have anything for you nor do other intelligence organizations. You call elsewhere in the government and are only given information about activities in Port-au-Prince, nothing about the areas where your Brigade will operate. You start looking elsewhere and contact relief

[1] This vignette is based on the experiences of a US Army officer and events in Haiti during Uphold Democracy. The author witnessed many of these events. Discussions with US and allied officers indicate that this vignette resembles issues faced from Albania to East Timor over the past decade.

organizations. They give you phone numbers for relief workers in Haiti. You start to call them. Someone from the Brigade intelligence staff tells you to stop — you're threatening operational security.

The intervention begins. Your brigade deploys to Haiti. You have essentially no information about the judges, principals, criminals, and so on in the civilian society. Time to start another crash course.

Several days after arrival in Haiti, a US Army gate guard arrests a Haitian for trying to sell marijuana to soldiers. It isn't until after the Haitian is on an Army helicopter en route to Port-au-Prince that you learn of this. You ask the question: does anyone even know whether this is illegal in Haiti? After all, to that time no one has been able to provide you an English-language version of the Haitian law code.[2]

This has been the reality of all too many officers' experiences with intelligence support in the 1990s. If they need to know something about enemy capabilities or need a satellite photo, the support is there. If they need to better understand the civil sector within which the force will be operating, it may not be.

Introduction

Over the past decade, international military forces have been ordered to intervene amidst complex emergencies, situations combining conflict with substantial humanitarian suffering. Whether by "blue-helmet" UN forces (such as Cambodia, Namibia, Bosnia 1992–1995) or multinational coalitions under some form of UN mandate (Somalia 1992–1993; Haiti 1994–1995; Bosnia, 1995—on; and, Kosovo, 1999—on), these operations have presented military commanders a set of challenges different from those likely in a "traditional" war-fighting operation.

In this vein, the information, analysis, and intelligence challenges are similar to many of the other issues faced by militaries around the world as they grapple with the reality and difficulties of "inter-agency" and "inter-organizational" operations.

Unlike the multinational forces that drove Saddam Hussein out of Kuwait in spring 1991, the majority of recent international military operations have been predicated on a civil-military partnership as key to a successful outcome. In these operations, as well, the civil-military "team" has had to be concerned with problems other than the size, capabilities, and intentions of "enemy" combat forces, but have also had to track numerous issues in the civilian sector.

In essence, three fundamental intelligence challenges exist in peace-support operations that might not have been expected in a NATO-Warsaw Pact confrontation or some other "traditional" war-fighting operation:

1. *Civil-Sector Issues*: Unlike warfare, developments in the civil sector are critical for the development of the military operation.
2. *New Partners and Sources*: A military force will not work in isolation from other elements of a "civil-military" intervention. In addition, the intelligence community cannot work in isolation from other elements of the force.
3. *Numerous Partners and Sources*: In addition to a qualitative change, a quantitative change exists. Intelligence managers have to be concerned with many more issues, organizations, and sources than emerge in a conventional war context.

The concept that these types of operations create new demands on the intelligence staff does not originate here, although perhaps this article conceives of these new demands in a different

[2] It turned out the attempted marijuana sale was illegal. A bilingual, English-Creole version of the Haitian law code was on sale in bookstores in Haiti.

fashion. In any event, to this time, it does not seem that these issues have been fully confronted and dealt with in the preparations for and execution of military operations in complex contingencies.

While this paper focuses mainly on the NATO experience in Bosnia-Herzegovina, it seems relevant for other military forces planning for or conducting an intervention in a complex humanitarian emergency.

Is a caveat *required?*

Every situation is unique and the "unique" nature of any situation should create a pause before assuming lessons are appropriate for other situations. While this paper is informed by the author's study of numerous operations, it derives heavily from the author's experience in and around NATO operations in Bosnia-Herzegovina in 1996 and 1997. With this in mind, how "unique" is the NATO experience compared to other interventions?

After multiple years of a civil war with multiple layers of outside intervention, including a UN force, European Community monitors, and numerous relief agencies on the ground, NATO operations in Bosnia-Herzegovina began with a substantial and well-developed international presence. This included, we can assume, an intelligence presence on the ground by many of the NATO nations involved in the UN operations in the former Yugoslavia. That this was a "NATO" operation (with non-NATO participation) meant that this was an alliance-run operation, structured around over four decades of NATO development of both hard (technical) and soft (doctrinal and procedural) interoperability. While augmented with additional staff, the four and three-star headquarters running the operations in Sarajevo derived from already existing multinational, alliance command structures.

These characteristics seem to differ from many of the interventions into complex emergencies around the world in the 1990s. Whether in Northern Iraq, Haiti, or in Somalia, the US-led interventions began without a major international presence on the ground before the introduction of the international force. There were not long-term, established military operations with well-developed intelligence infrastructures in place for the military force to rely on to support the operation. Nor were these interventions conducted by alliance military forces, but by coalitions with a headquarters heavily dominated by the United States military.

Differences also exist across the societies in which international interventions occurred. Yugoslavia was a European nation, even if with a leg on each side of the iron curtain, and a modern, industrialized society. Haiti, Liberia, Cambodia, Rwanda, and many of the other environments for international operations were not nearly as well developed (in terms of institutions, education of the population, infrastructure, and so on). In addition, the fundamental problem was not derived from a total absence of a governmental structure, as was the case in Somalia or Liberia.

Despite the appearance of differences, however, important similarities exist. Despite being a NATO operation, for example, over ten NATO nations had "National Intelligence Cells" in the middle of the headquarters, each of which had its own rules and procedures for sharing information with NATO and the other nations involved in operations on the ground in Bosnia. While a NATO operation, each of the national elements (especially the US, French, and British divisional commanders) maintained a significant degree of independence and, reportedly, were often "convinced", rather than commanded, by higher headquarters to take certain courses of action.

In terms of the environment for the interventions of the 1990s, every international military intervention (whether involving the U.S. military or not) has operated in an environment with other international actors on the scene, whether these were international organizations (IOs), governmental

organizations (GOs), or non-governmental organizations (NGOs). And, these other organizations were often on the ground to greet the military forces as they arrived.

In short, although this paper relies heavily on the Bosnia situation (as this author's "fighting the last war"), the "unique" nature of the NATO operation does not invalidate the relevance of the concepts examined in this paper for other military interventions.

Thoughts on Definitions

This article refers to information, assessment, and intelligence. For clarity of purpose, these words are used with the following meaning:

- Information: unprocessed data, from whatever source, that may relate to the force's requirements.
- Analysis: Processing information into intelligence.
- Intelligence: Processed information to support the commander's decision-making.

As discussed below, the differentiation between these three can prove critical for understanding and developing appropriate staff and inter-organizational relationships in a civil-military operation.

Civil-Sector Issues

In a peace support operation, complex emergency, or humanitarian assistance operation, the intelligence community will have to collect information on and analyze a wide set of issues that would not be of concern in a "combat" operation.

In Somalia, military commanders required information on, for example, refugee health concerns, concerned themselves with the development of tribal consuls, and worried about the effects of food distribution on the local economy. In Haiti, military commanders worried about the reconstitution of the local police and judicial system, and on the potential flow of drugs through Haiti. In Bosnia, commanders had to concern themselves with organized crime, governmental formation, house evictions, refugee voting patterns, and reconstruction progress. These are simply examples, of course, and many of these issues are common to these and other operations.

All of these challenges required information that a military force would not expect to focus on in a 'combat' operation and analysis techniques not necessarily resident in a typical military force. These 'new' concerns did not, however, replace traditional concerns (such as developing 'enemy' orders of battle) but were additional tasks.

New Partners

One of the most notable challenges from traditional to peace support operations comes in the nature of partners for information collection and analysis. Rather than simply dealing with mainly other "intelligence professionals" (with the limited exception of other military personnel, such as scouts), a command's intelligence office will be working with numerous external agencies and "unusual" internal staff elements.

In Somalia, "new" partners included UN organizations and governmental relief and development agencies. In Haiti, the US-led multinational force worked with the International Police Monitors (IPMs) and elements of the U.S. Justice Department.

In Bosnia, these "new" external partners included the International Police Task Force (IPTF), UN Mission in Bosnia-Herzegovina (UNMIBH), the Office of the High Representative (OHR), and the European Community Monitoring Mission (ECMM). Internally, the intelligence officers worked with elements such as the Engineers, Civil-Military Task Force (CMTF), and analytical cells working for the Chief of Staff. Psychological Operations (PSYOP) and Public Information / Public Affairs (PI or PA) personnel also have a potential role to play.

All of these information sources and intelligence partners emerge in a complex emergency due to the requirement for the military force not to execute a "military mission" of defeating an enemy but to work as part of a team to execute a civil-military operation.

Numerous Sources and Partners

In addition to the qualitative challenges of having to examine civil sector issues and of dealing with new information and intelligence partners, the intelligence component of a military force will also have a quantitative challenge: numerous intelligence sources, intelligence partners, and "clients" for information.

An operation in which the military acts as the lead or sole agency (i.e., war fighting) can have a relatively clean intelligence architecture, with a clear concept of who is responsible for which tasks and who has authority. Such clarity might be impossible to achieve in a multinational peace support operation.

In Bosnia-Herzegovina, the senior NATO intelligence officers have had to manage a complex network of information sources and intelligence partners.[3] In addition to a multinational staff, these included the Allied Military Intelligence Battalion (AMIB), national intelligence centers (NICs) collocated with the SFOR headquarters in Sarajevo, national civilian intelligence agencies, civilian organization information sources, and numerous staff elements (from the CMTF to the "Factions' Liaison Officer"). Thus, the SFOR CJ-2 had to coordinate with more staff divisions, sources, and external agencies than would have occurred in a more 'traditional' operation.

In other words, in addition to 'new' types of information sources and intelligence partners, intelligence officers will have to deal with many more sources and partners than might be the case in a more conventional conflict. Future peace support operations are likely to pull together a similar assortment of intelligence organizations, agencies, and assets that will present a challenge for integration and management.

The Intelligence Challenge?

These three challenges create a far different working environment for the intelligence organization within the military command than many military personnel have prepared and trained for through their careers. The "intelligence challenge" is only part and parcel of the larger challenge for military professionals of having to adapt to the demands of involvement in the civil-military operations that seem to dominant the current international military environment.

A number of obstacles exist to providing adequate intelligence support to the military commander in the Bosnias and Somalias of the world. When considering an operation, many military officers and civilian defense officials seem comfortable distinguishing between the "military mission" and the "civilian mission". This type of distinction certainly occurs within the U.S. debate. Many of the concepts related to "mission creep" derive from the thought that military tasks should be finite and not involve the military in the civilian sector to any significant extent.

In reality, these operations are "civil-military missions" and there is not such a thing as a military success but civilian failure, instead there is simply a question of whether the international community achieves the objectives involved in deciding to deploy an international military force.

Intelligence staffs operating within the conception of separate missions as a basic philosophy will likely resist serious examination of the civilian sector. This will leave them poorly prepared to deal with the questions that the commander will inevitably ask about civil society.

---

[3] In this context, the reference is to the Implementation Force (IFOR) and Stabilization Force (SFOR) CJ-2 in the November 1996 through mid-1997 period.

The following pages raise some of the issues related to these challenges of preparing for and answering these questions, and suggest some approaches to deal with these issues.

Different issues of concern

If an intelligence officer has prepared through his career for "warfare", as many officers have, the reality of the contingencies of the 1990s will have many surprises. The war-fighting mission does not require analysis of governmental corruption, police brutality, organized crime, refugee movement patterns, international development funding capacity, what is happening in the local economy and how might that effect local stability, or the organization of "spontaneous" riots. While many intelligence processes, such as "Intelligence Preparation of the Battlefield"[4], remain relevant for dealing with these questions but will have to be applied in a different manner. One challenge for the intelligence staff will be to determine what questions are relevant for the new situation, which can help with overall mission accomplishment. In no small part, as the commander is likely to be caught in the same conceptual trap of separating the "military" and "civilian" missions, the intelligence staff will need to help the commander understand the questions he should be asking them to tackle.

Different analytical requirements

As the intelligence staff will have to cope with a new set of questions, so too they will have to develop different analytical methods to support the commander's intelligence requirements for decision-making.

Essentially every military organization has some form of intelligence structure. When considering a typical tactical unit, a brigade, the commander might have a Major as his "S-2" with perhaps 20 officers and enlisted personnel in the "2-shop". For the most part, in a tactical combat force, these personnel have trained to support combat operations, with understanding "enemy" combat capabilities and the tactical assessment of "enemy" intentions. In a complex contingency, however, the Brigade commander will require other types of intelligence to support his decision-making. What will be the population's voting patterns? Where will refugees try to rebuild houses? Will the local schools be able to open on time? Can the police competently handle crowd control? These are real examples that this author has seen Brigade commanders ask their intelligence officers in Haiti and Bosnia. Traditional intelligence techniques, training, and sources do not necessarily lend themselves to answering these questions.

If it is true that there is a fundamental difference between developing an understanding of "enemy" orders of battle, intentions, and tactical movements and the sort of situations encountered in peace support operations (like refugee movements and criminal activity) then there is likely a fundamental difference in the expertise and education required to develop that understanding. To be blunt, most tactical military units do not have the intelligence capacity to tackle these questions—and they shouldn't.

Most nations have intelligence personnel (either civilian or military) with experience dealing with many of the relevant economic and political questions that will emerge in an operation assisting in a transition from war to peace. These personnel, however, frequently specialize in "strategic" questions and are not typically conceived as supporting tactical military staffs (especially not down to Brigade level). In addition, these specialists are often limited in number; thus deploying them to the tactical environment is difficult.

This suggests that military intelligence staffs, at essentially all levels, will require augmentation to deal with new issues.

---

[4] For a lengthy description, see: Headquarters, Department of the Army, *Intelligence Preparation of the Battlefield*, FM 34-130, 8 July 1994

In some cases, the intelligence staff has "out sourced" such questions. It was not the intelligence section of the Allied Rapid Reaction Corps (ARRC) headquarters that developed a means to track developments in the civilian sector in Bosnia in 1996, but the Operational Analysis Branch (OAB). For SFOR, the Chief of Staff's Assessment Cell developed relationships with those in international organizations collecting and analyzing information, not the intelligence staff. Such "out sourcing" is not inappropriate — as discussed below, it can be quite appropriate — but should be done in a coordinated fashion to insure that the intelligence staff has full information available to it in developing intelligence.

New sources required

With new issues requiring assessment and investigation come new types of sources that will be critical for supporting the intelligence staff within the command. Some of this sounds mundane (even if not always practiced), such as the critical nature of "open source" information for understanding many of the environments in which military forces will operate in the coming years. Western reporters will have covered much of the "battlefield" and will provide a window (even if blurred by a bias or inadequate research) on the situation.

The numerous international agencies and non-governmental organizations are potentially rich sources of information and databases for the intelligence staff to build on. In an operation with an established government (such as Bosnia), the government ministries might provide information that will help build the overall intelligence picture.

Of course, in the 1990s, one cannot write of open or new sources without discussing the Internet and the value added of examining the Internet. Through the Internet, the intelligence staff will literally have a world of data at their fingertips to support analysis. Information technology advances have made accessing the Internet relatively easy from anywhere in the world—demographic data, recent press reports, historical material, maps … all available.

A critical comment on these sources, whether from open sources, partner agencies, the local government, or individuals, is an obvious one—credibility and reliability of sources and, therefore, data will have to be constantly judged to avoid creating a false picture of the situation through reliance on skewed information.

New "sources", however, are not only outside the force, but inside it as well. Other staff sections will gather information about the situation during the performance of their duties. In fact, the nature of most peace support operations indicates that changed nature of staff responsibilities will increase the amount of information staff elements will gather. In a combat operation, for example, the public affairs staff will rarely be on the front lines and will not (except by disaster) behind the enemy's lines. In Haiti or Bosnia, on the other hand, public affairs officers (PAOs) frequently escorted reporters throughout the theater and frequently observed things that no other member of the force (and certainly no one in the headquarters) observed. The intelligence staff does not have the habit of seeking information support from PAOs and thinking of PAOs as tactical information gatherers (like scouts or patrols). On the other hand, the PAO is very leery of being associated with "intelligence". Unless the headquarters has established procedures or relationships that ensure the movement of this information, it is all too likely that this information will never be incorporated into the intelligence picture to support command decision-making.

Unclear C2 lines

Inherent in the new relationships is that the intelligence manager will have to be skilled in partnerships, in collaborative relationships with unclear lines of responsibility and authority. When considering major armed conflict, the "2" (the intelligence officer) clearly understands who he

works for (the commander), who works for him (the military's intelligence assets), and whom he has the authority to call on for intelligence support (typically national or allied intelligence organizations).

This changes greatly in a complex emergency involving multinational forces as such clarity will not necessarily exist. While the intelligence staff will continue to work for the military commander, often they will have other (even if secondary) customers (or consumers) for their work. In some cases, the command will pass along intelligence products while in others the intelligence personnel will be directed to support outside organizations. On a rather mundane level, military forces have provided security briefings to NGO meetings in complex humanitarian emergency situations around the world. If national restrictions have hampered the movement of intelligence material between allied and coalition partners in some operations, briefings to an open audience like NGOs suggests even more problems. In such an environment, an intelligence professional would have no choice but to assume that any briefed material is immediately compromised. With this in mind, NGO personnel in Bosnia viewed the threat briefings as marginally beneficial as they received more complete information from the IPTF and each other.[5]

With the presence of more significant partner agencies, such as those in Bosnia, the intelligence staff might be directed to provide far more than the occasional briefing to a NGO forum. With a partner agency such as the IPTF, is it appropriate to ask the intelligence staff to assist them establish their own intelligence mechanisms. In other words, should military intelligence staff be used as expert consultants to develop methods for other organizations to collect information, process and analyze that information to produce intelligence, and then on the use of that intelligence to support both the partner agency and the military force?

With partner agencies, as well, a serious question emerges as to what information and what intelligence should the intelligence staff share. With a public briefing to NGO staffs, clearly the information is no longer secure. In other words, that material is publicly released. Is this the case for distribution of material distributed to partner agencies? The realities of the civil-military partnership suggest that unless the military force shares such information and intelligence, eventually the well will dry up in the other direction.

Some organizations are more open for such partnerships and countries are increasingly involving them on the ground in conjunction with military operations. These are civilian intelligence organizations, which might work independent of the force or provide augmentation to military intelligence staffs.

One seeming fallacy of examinations of civil-military relationships in these complex emergencies is to compare the confused nature of the civilian organizations (without structure, unclear authorities) with the clarity of the military command and control structure. This black and white contrasting comparison distorts the actual nature of at least one side of the equation. Multinational forces such as those in Bosnia are inappropriately described as "the" military. In fact, there are many "militaries". In Bosnia in 1996 and 1997, the "militaries" included:

- NATO IFOR/SFOR forces;
- National support elements / commands;
- A UN mission;
- Military forces assigned to support the Organization for Security and Cooperation in Europe (OSCE) mission.

[5] Many IO/NGO staff personnel commented to this author that they appreciated NATO security briefings more as a sign of NATO interest in NGOs than for the information they provided

By suggesting four militaries, this list lends more clarity to the actual environment than existed in reality. The IFOR force included elements from 33 nations, and often from more than one service in each country. Thus, there were multiple national and service cultures at play in Bosnia. In terms of intelligence, while the main headquarters had a NATO intelligence staff, at this same headquarters over ten nations maintained national intelligence centers (NICs). As each nation has specific regulations on the sharing of intelligence material, there was only an incomplete movement of information, analysis, and intelligence between these NICs and the NATO force.

In fact, even within the military staff itself, the traditional military concept of C2 as "Command and Control" might shift into the civil-military operational concept of "Coordinate and Cooperate." The commanding officer is unlikely to grant the "2 shop" authority over staff sections providing information. Thus, the clarity of "who works for" the "2" is diluted in a complex contingency operation. Without directive authority, the intelligence staff will have to develop cooperative relationships within the staff (and with external organizations) to ensure an adequate and timely flow of information into the intelligence process.

Changing Staff Relationships

In addition to the introduction of numerous outside organizations with whom the military intelligence staff (again, the "2" in many military organizations) has to deal with, the "2" will need to deal with different staffs within the headquarters and the overall military command than would occur during a traditional "combat" operation. Typically, intelligence personnel have little relationship with (and provide even less support to) staff sections other than the "3" (current operations) or "5" (plans) in supporting the commander. This should change in a civil-military operation responding to a complex emergency. Intelligence personnel will likely have to take the lead to establish relationships with other staff sections to ensure an adequate flow of information to support intelligence analysis. This has to be an educative process, on both sides, as to the importance and value of such contacts. In many cases, this will also be a very sensitive process.

Lawyers, doctors, civil affairs, and public affairs officers are uncomfortable being associated with "intelligence" activities. In a war-fighting environment, this rarely will have an impact on the intelligence staff's ability to support the commander. These sensitivities remain, however, in the environment of a peace support mission in which these (and other staffs, such as engineering, logistics, purchasing, personnel, etc…) will collect information as part of their normal business that could be critical for developing a robust intelligence picture of the situation.

At the same time that intelligence personnel will have to work to develop new sources within the staff to support the commander, they will need to adapt themselves to supporting other parts of the HQ than the "3", "5" and the commander.

All of this suggests that staff relationships should be different in a peace support operation than in a traditional combat operation. On-the-ground experience and discussions with personnel engaged in other operations indicates that this all too rarely happens. As one civil affairs officer from the Joint Task Force 190 staff in Haiti phrased it:

> "The intelligence guys remained behind their barriers and none of us had the clearances to go in and talk with them. On the other hand, it isn't as if they came and spoke with us."[6]

[6] Comments to the author, spring 1998. On the other hand, the author saw a more integrated relationship on the brigade level in Haiti.

In Haiti and elsewhere, intelligence staffs have frequently remained isolated from elements of the command staff. This hampered operational success both by limiting the flow of information into the intelligence staff to support analysis and, as importantly, limiting intelligence support to "new" customers.

New clients

With the new sources and new partners, the intelligence staff also has new "clients" for their products and might have to develop new products to support these new clients.

In past operations, the United States (and other countries) have experienced the problem of having intelligence material prepared as "NOFORN" (no foreign distribution) which restricted the ability to share material with partners in a coalition operation. In civil-military operations, the issues will not just be sharing of "classified" material with military partners but also an issue of how to share "sensitive but unclassified" material with civilian organizations.

The problem will be multi-layered. NGOs in Bosnia-Herzegovina found briefings from the IPTF more valuable because they were often more forthcoming than material from IFOR/SFOR, which had to be "cleared for public release" before discussing in the open NGO meetings (where the military had no control over who the attendees were).

Clearly, the same rules could not be applied to discussions with the leadership of the UN High Commissioner for Refugees, Office of the High Representative, World Bank, OSCE, and other major civilian organizations on the ground as partner organizations with the NATO military force.

The problems are not just external but internal as well. Some intelligence officers are very reluctant to discuss sensitive material with those, such as Civil Affairs or Public Affairs officers, who regularly interact with outside organizations. And, just as intelligence personnel might not have the habit of using these "new" staffs for supporting intelligence, these other staff elements might not have the habit for asking for intelligence support. Thus, the lawyers, contracting officers, and doctors (for example) might need education as to how to ask for intelligence support.

Despite all of these tensions, an intelligence staff will have to be prepared to provide intelligence support all of these different types of new "clients".

- For NGOs, will the intelligence staff provide material on the security situation and potential threats to NGO staff and activities?
- For the World Bank, will intelligence personnel be asked to support fiscal audits to determine whether local governments are diverting funds to illegal arms purchases? Will they help the World Bank understand and track corruption?
- For election monitors, will the intelligence staff be asked to assist in assessing how "fair" an election was?
- With the command's contracting officers, will the intelligence staff need to investigate ownership of buildings so that a command does not rent a building owned by a war criminal or drug lord?

Clearly, a wide range of potential—even likely if not actual—tasks exist for the intelligence staff to support new clients both within the military force and external to it.

Coordinating intelligence

With all these different actors on the ground, the military intelligence manager will face a significant new challenge in how to coordinate information collection, analysis, and intelligence production to support the commander and the new clients. Even without examining "new" clients, there is the difficult challenge of weaving together the numerous different civilian, military, national, and multinational intelligence organizations that will be involved in an

operation to create a unified picture to support the commander.

Balancing new with the old

Amidst all these challenges, the intelligence professional will face yet another: the new requirements are additive responsibilities, they do not replace the "traditional" requirement to maintain a constantly up-to-date understanding of any potential threats to the force (i.e., "enemy" capabilities, deployments, and intentions). Clearly, in many of these operations, the traditional demands will neither be as time-consuming or time-urgent as might occur in a combat operation. For example, maintaining a constant track of heavy weapons placed in cantons does not require the same amount of resources as tracking an enemy tank battalion maneuvering for an attack. Even so, a key point is that intelligence staffs (at all levels) cannot abandon their "traditional" tasks to train and prepare for, and execute the "new" tasks that will emerge in complex emergencies.

Balancing 'traditional' requirements with emergent demands in a civil-military environment will remain a challenge. "Force protection" seems a mantra in the U.S. and other militaries. Intelligence staffs will focus on threats to the force, which are often defined in traditional ways (armed threats). Even here, however, the military intelligence staff will be working with new issues, concerning themselves with understanding terrorist or other "unconventional" threats to the force. The intelligence officer might even have to develop analysis of criminal threats to force personnel, an issue unlikely to have been the central concern in a NATO-Warsaw Pact battle in the Fulda Gap.

In the end, the intelligence staff will have no choice in a complex emergency or war-to-peace transition operation to shift at least some focus from "military" to "civilian" questions.

Implications?

The following are a few ideas that can be drawn from the challenges discussed in this article.[7]

Augmenting intelligence staffs

To deal with the new analytical challenges, countries should consider intelligence augmentation by civilian experts into lower intelligence staff levels. Relevant specialties could include regional experts, political scientists who study government systems, relief or development specialists, organized crime experts, and economists. If the operational environment is civil-military, is there any reason not to have combined civil-military intelligence teams at all levels?

It seems likely that few governments have enough, relevant specialists on the government payroll to meet all these requirements. Perhaps this is an arena to develop reservists with the requisite skills.

In terms of augmentation, do advances in information technology allow the command to rely on remote augmentation? The intelligence manager of future military operations might have to manage a "cell" of support analysts who meet via the Internet or video teleconferencing. These analysts would not necessarily come from the government, but might be university professors or businessmen willing to devote their expertise to support mission success.

Information technology

If the world is not in an "information revolution", it remains clear that how the world is in the midst of massive changes in the abilities to communicate and process information. This has had, and will continue to have, important implications for intelligence communities around the world. These effects should extend into civil-military operations as well.

---

[7] These are just a few of the implications that can be derived from the challenges raised in this paper.

To do their job right in a civil-military operation, for example, intelligence staffs cannot ignore the Internet—the potential sets of available data are too important. This means that the HQ must be wired for the Internet. This also means that the intelligence staff requires "unclassified" computers for searching the worldwide web.

As well, the intelligence community should create, maintain, and electronic databases with the material collected from all these new sources: press reports (both international and local), international community databases, and such. In an operation such as Bosnia, extended over several years, such databases might provide the only real continuity in an operation where the military staff rotates at least twice a year. Intelligence staffs might also exploit commercial databases to support information requirements.

Such databases again raise the issue of sharing with partners; if the intelligence staff is simply in a "receive" mode to fill its databases, other organizations might become reluctant to continue supplying the information. Thus, the staff might attempt to maintain a shared unclassified, not sensitive database for all players in the environment to use while reserving a separate, more comprehensive database for use within the HQ itself. In fact, the intelligence staff might support creation of a web site for sharing the non-sensitive material across all interested parties. Such openness would likely foster cooperative information sharing across organizations.

New staff relations

In complex emergencies, the intelligence staff should be working with different groups then occurs in war-fighting operations. The notion of this changed relationship does not, however, seem to have translated into the operational environment.

This will be an educative process, of both the intelligence staff and the other organizations (within the military and external to it). If the intelligence community accepts such relations as a requirement, the challenge then shifts to how to convince that working with intelligence is both required and valuable. In part, the intelligence professional will have to become "salesmen" to convince the other organizations to become more engaged in a relationship. In part, this will have to rely on emphasizing the difference between *information* and *intelligence*. Lawyers, doctors, civil affairs personnel, and public affairs officers (for example) should not be asked (or tasked) to provide "intelligence". This type of role could jeopardize their primary function and, potentially, cause serious damage to the operation. To suggest, however, that these specialists should be better linked into the overall staff to provide "information" gathered as a normal part of their duties should not jeopardize their primary responsibility. This type of tension increases exponentially when dealing with outside organizations, such as the Red Cross, which are already extremely wary of any ties to the military.

In addition, the intelligence staff might have to be prepared to educate other staff elements as to how intelligence can support them and how to ask intelligence personnel for assistance. For example, for a war-fighting mission the contracting officer is unlikely to be a provider of information for the intelligence process and even less likely to be a "client" for the intelligence community. In a complex contingency operation, however, the contracting officer could be both and not know how to do either. For example, if trying to understand whether to attempt to rent a specific building, the contracting officer might value knowing answers to the following questions: What is an appropriate rent for the area? Does the person offering the rental has real authority to do so? Is this person associated with some faction (such as a war criminal or drug cartel) for whom the force does not want association? And, is there some history of this particular building in the context of the conflict such that the force would not want that association (e.g.,

it was the site of torture or has political association)? It is possible for an intelligence staff to shed light on questions like these.

Fostering Intel Cooperation and Expertise

Nations restrict the flow of intelligence material. This is a fact. A question then emerges, in an operation with multiple national intelligence cells (NICs), are there means to foster more significant interactions between these NICs that would improve the overall intelligence posture without compromising individual national security concerns?

In extended operations, such as the NATO operation in Bosnia-Herzegovina, the multinational intelligence manager could establish "symposium" presenting analytic techniques to foster cooperation between the cells and to generally improve capacities to develop a richer understanding of the operational environment.

Conclusion

Military officers weaned on the concept of preparing for the battlefields of the "Third World War" between NATO and the Warsaw Pact have found it difficult to adapt to the realities of the civil-military operations of the 21st century. To support decision-making, these operations demand a different concept as to what information should be collected, how it should be analyzed, and what constitutes the intelligence from that analyzed information.

These challenges, however, are on multiple levels. The first challenge is to recognize that there are new challenges. After this comes a long educative process. The intelligence officer will have to educate not only themselves and their staff, but also other staff sections. There is even the challenge of educating the commander as to what "priority intelligence requirements" really deserve to have priority in a civil-military operation.

Building relations within the staff, however, might be simple compared to the challenge of dealing with the multitude of other organizations that will be involved alongside the military force that can provide critical information and will want some level of intelligence support in return.

On the ground, in the real world, intelligence and other officers have received an education in these new requirements. This knowledge has to be translated into training and education so that preparation does not fall to "on-the-job" training. In addition to such training requirements, military forces should examine what types of issues appropriately lie outside military expertise and preparation. Identifying such requirements will develop the structure for appropriate "outside" augmentation of the military force to provide more appropriate intelligence support.

Adam Siegel is a Senior Analyst in the Northrop Grumman Analysis Center. He has operational experience with US and allied forces in numerous operations over the past decade. The article represents the views of the author and are not necessarily those of the Northrop Grumman Corporation.