Information Operations: Strategy or Mission? Reflections on Allied Force

By Paul Bowman, Lieutenant Colonel, U.S. Air Force

Editorial Abstract: *Operation ALLIED FORCE has provided lessons learned impacting the full range of joint operations, particularly effects based operations. Having led the USEUCOM IO effort for the past two years, Colonel Bowman provides an interesting ground-zero perspective to the conduct of IO during Operation ALLIED FORCE and their place in the joint force commander's operational quiver.*

Immediately following the conclusion of Allied Force, there was an intense round of lessons learned efforts that produced a number of documents, briefings and publications. Headquarters European Command (EUCOM) produced its own Quick Look and Joint After Action Report, to which the EUCOM Information Operations (IO) division provided substantial input. Probably the most well known were the lessons learned produced by Admiral James O. Ellis, Jr., NATO Joint Force Commander for Operation ALLIED FORCE, and Commander, U.S. Joint Task Force NOBLE ANVIL. EUCOM has continued to experience a target-rich IO environment, with ongoing contingencies in Northern Iraq, the Balkans, and Africa. We have continued to refine our concept and employment of information operations, and many of the things we learned during Allied Force continue to surface. Now that nearly two years have passed since the conflict, it is worthwhile to revisit some of those lessons learned. Since this paper is being submitted at the unclassified level, the content will be somewhat constrained. However, there are significant issues of planning, resources and coordination that can be addressed at the macro level and are worth discussing.

The conventional wisdom about Allied Force in general, and IO in particular, is that "no one had a plan." This is not really true. There were many plans and much planning was accomplished prior to the conflict, but as is often the case, none of those plans were executed as originally envisioned.

IO planning for Kosovo began in the spring and early summer of 1998. There was the first Kosovo crisis, in which NATO and the U.S. put pressure on the FRY to withdraw its military forces from Kosovo and accept an international monitoring force. This initial conflict has largely faded from public awareness, but Information Operations planning for the Kosovo conflict began, and was more or less continuous from June of 1998. This first crisis was resolved over Columbus Day weekend in 1998, when Slobodan Milosevic agreed to withdraw the FRY armed forces (VJ) from Kosovo and accept the presence of the Kosovo Verification Mission (KVM) in Kosovo to monitor and verify the withdrawal. The U.S. and NATO conducted extensive planning during the summer of 1998 for potential strikes against the FRY and positioned forces to make this threat credible. Measures of effectiveness are difficult in IO, but the conventional wisdom is that the force movements which backed up diplomacy had a significant effect in persuading Milosevic to comply with Western demands.

The activity level of IO planning lessened during November and December of 1998. While it briefly appeared that the conflict was resolved, past experience with the cycle of violence in the Balkans made it prudent to conduct additional planning to prepare for the eventuality of renewed conflict. HQ EUCOM was preparing a U.S. supporting operations plan (OPLAN) to the NATO OPLAN for potential conflict with the FRY, and the newly created EUCOM IO division scheduled a planning conference to develop the IO portions of that plan in January 1999. This planning conference was scheduled to take place from the 25th of January to the 5th of February. By the time the conference convened, it had mutated from prudent contingency planning to actual crisis planning. The discovery by the KVM of 45 Kosovar Albanian bodies in a ditch outside the village of Racak, Kosovo, on 15 January had precipitated an international crisis and contingency planning was well under way. By the end of the first week of "deliberate" planning, Joint Task Force Noble Anvil (JTF-NA) was activated (on 30 January 1999), and the run-up to what became Operation Allied Force had begun.

The US European Command (USEUCOM) Information Operations Division (ECJ39), at that time totaling six personnel, produced an Appendix 3 to Annex C to U.S. Operations Plan (OPLAN) 4250 in accordance with joint doctrine. This OPLAN was largely finished by the end of the planning drill mentioned above. We also produced a EUCOM version of a synchronization matrix, which we called a "horseblanket." The EUCOM deputy IO chief and Special Technical Operations branch chief, LTC Mike Chesney, developed his horseblanket methodology while working some special projects for CINCEUR, then General Wesley Clark. Our horseblanket technique is basically a flowchart that lays out actions in the diplomatic, economic, military and informational spheres along a timeline, containing key decision points leading to alternate actions depending on events. The horseblanket attempts to lay out strategic, operational, and tactical actions and link them to recommended interagency and PSYOP tasks. Producing a detailed horseblanket is a labor-intensive exercise, but when complete, it provides an excellent blueprint for the conduct of information operations.

The horseblanket itself illustrates a key principle of information operations that needs to be highlighted. As information operations have continued to mature and develop, a debate has naturally begun over U.S. IO doctrine. One of the key events in the ongoing debate was the floating of a White Paper on Information Operations in July 2000, which recommended a number of changes to Joint Publication 3-13, Joint Doctrine for Information Operations. One element of current doctrine, which was singled out for criticism, was the concept of IO as an "integrating strategy." "As we normally understand the term "strategy," however, IO doesn't fit. It isn't "grand strategy," which integrates the policies and armaments of the nation. It isn't "military strategy," determining force structure, composition, readiness and posture. Nor is it "theater strategy," driving operations and operational art." In my experience, however, strategy involves more than the allocation of resources and force structure. In conflict, strategy also involves the national objectives of our and other nations, and the theater strategy for carrying out that national strategy. In this sense, IO is very much an integrating strategy and must be so.

Our national security strategy has encompassed the concept of instruments of power for some years now, and specified four elements of national power: military, diplomatic (or political), economic and information. Most of the elements of power have a clear lead agency within our governmental structure, such as the Department of Defense (DoD) for the military instrument and the Department of State (DOS) for the diplomatic instrument. But information cuts across all the elements of power and is used to carry out national interests by many actors within the U.S. government. To be effective, information efforts must be synchronized laterally among all the players at any given level (strategic, operational, tactical or interagency). In addition, information must be synchronized vertically within each agency or chain of command. In the information age, with media able to provide real-time coverage, tactical events can quickly have strategic consequences. Therefore, it is essential that information must be integrated vertically and horizontally within and across organizational structures if a unified information campaign is to be executed.

The horseblanket illustrates this principle by explicitly identifying information tasks at the strategic, operational, and tactical levels and by color-coding those recommended events that require interagency coordination. The DoD clearly does not "own" the information sphere; it does not have primary responsibility for U.S governmental information activities—and even more so, does not have lead responsibility or authority for NATO information activities. Other governmental institutions have primary responsibility for U.S. information activities aimed at foreign audiences, and to be effective DoD and State Department informational activities need to be synchronized (where possible) and, at a minimum, consistent. All governmental information efforts need to be consistent with national policy and objectives—that is, strategy—and information operations therefore needs to be an integrating "methodology" if strategy is not the proper term.

But—my experience is that IO does need to be a strategy. We have found over and over in deliberate and contingency

planning within the European theater that IO planning becomes strategic very quickly. When planners begin to lay out themes, messages, and statements and to determine how best to communicate those messages, whether by public affairs, psychological operations, or physical destruction, it becomes critical that the planners have strategic guidance on what the "message" is. When a planner tries to craft the message to be conveyed by a TLAM or aircraft strike mission, it is essential to know precisely what the theater and national command authorities intend to achieve and what they wish the adversary to do as a result of that strike. If IO is a means of influencing behavior, then a military planner who is laying out operations intended to influence adversary behavior needs to know what we are trying to get the adversary to do. What the concept of IO brings to the fight is a disciplined way of using all the elements at our disposal to focus on influencing the adversary to do what we wish the adversary to do. In the case of Allied Force, the strategic objective was to influence Slobodan Milosevic to accede to NATO's demands, but we did not necessarily synchronize all the elements at our disposal effectively throughout the conflict.

This illustrates another key aspect of IO. Often, the idea of IO generates skepticism and resistance among military and government professionals. People who have been competently conducting military operations for their entire careers are naturally skeptical of the newest buzzwords that come along. The comment is often made that "none of this IO stuff is really new—we've been doing PSYOP and targeting and public affairs forever." Anyone who has graduated from a command and staff college or war college, (whether the easy way in residence or the hard way by correspondence) has read at least the Cliff Notes of Sun Tzu's Art of War, and few military officers are unfamiliar with Clausewitz's characterization of war as the continuation of policy by other means. IO attempts, as all military attempt, to impose our will on the adversary. IO is simply a way of applying all the instruments at our disposal—information as well as force—and trying to focus them on a target to achieve our objective as effectively as possible.

What is new about IO is that these operations are taking place in the information age. We have abilities to collect, analyze, and disseminate information that are unparalleled in human history. If we use our information technology wisely, we can leverage it to achieve our objectives by operating faster and more effectively than an adversary can cope with. And, a new battlespace has come into being—cyberspace. As the premier information technology nation in the world, we need to be prepared to operate in this new realm and be able to achieve information superiority, as we are able to achieve air superiority.

Which brings me back to Allied Force. Although we developed a sound information campaign prior to the beginning of Allied Force, and advocated using all the information elements available to prevent conflict, the crisis developed very rapidly between late January and mid-March of 1999. In retrospect, there were a number of things the armed forces and European Command could have done to support the State Department and the Rambouillet negotiations, but the planning and coordinating structures to achieve the integration of military and diplomatic information efforts were not well developed at that time. It is possible that diplomacy could have been supported by visible force deployments that would have clearly communicated NATO and U.S. resolve and prevented the need for armed conflict. That is a topic for another paper and a serious study, and I will simply note that IO did not fulfill its promise at this stage of the crisis for a variety of reasons.

When the diplomatic negotiations failed and the unthinkable began to seem likely, crisis planning within NATO and USEUCOM reached a very high tempo. The diplomatic situation evolved very rapidly, and military and political planning by necessity evolved just as rapidly to adapt to the situation. As the onset of conflict approached, the campaign plans changed daily. A protracted campaign was not expected, and the forces in place reflected that planning. Many essential information operations that were deployed later in the conflict were not in place. European Command does not have organic Psychological Operations forces, for example, nor did we have Commando Solo aircraft in place to serve as a dissemination mechanism. The lesson here is that information operations take time. If we are to fully practice our doctrine, IO will be most effective in the "Shaping" or pre-conflict phase of an operation. But IO structures in most theaters are still rudimentary and undermanned, and many IO capabilities require long lead times. Units that are key to the conduct of information campaigns often must be deployed, and legal and political permission for employment of many capabilities requires a very lengthy review process. To begin planning and execution of Information Operations requires national-level commitment well in advance of the onset of hostilities. But the will to deploy forces and approve execution of capabilities often does not coalesce until late in a crisis. Information operators must solve this riddle of the early commitment of resources before a crisis if we are to be able to fully exploit our capabilities.

When Allied Force began and continued beyond its original expected duration, information operations were executed based on our pre-crisis planning and adapted as the situation changed. IO was very much a supporting effort to kinetic targeting. The Joint Psychological Operations Task Force (JPOTF), stood up prior to Allied Force, began getting support for expanded operations. Commando Solo was deployed and began broadcasting the JPOTF's products. OPSEC began to take on greater and greater implications as the holes in our posture became visible. The JTF IO cell we had stood up with six people at the inception of the JTF tried to cope with the deluge of actions that were necessary for them to coordinate and execute. All those who had a piece of the IO mission, particularly our air component at USAFE and those forward deployed to the JTF and Combined Air Operations Center at Vicenza, scrambled to catch up with the rapidly evolving tactical situation.

It is important to note here that this was a NATO operation and all information operations had to be coordinated through and executed by the NATO chain of command. This introduced a whole new layer of complexity, since NATO and U.S. IO policy and doctrine are not identical, and U.S. doctrine had reached a more complete state than NATO's. As the war began, the Supreme Headquarters, Allied Powers Europe (SHAPE),

had not established an IO structure per se. This shortly was remedied when General Clark directed that an information campaign be established and an officer was appointed the head, but the ad hoc nature of the NATO IO cell meant that we had to create channels for coordination during the conflict.

After several weeks of conflict, both the NATO and U.S. chains of command began considering options to expand the campaign in order to achieve NATO objectives. One area that was ripe for greater emphasis was information operations. The Joint Staff and USEUCOM, along with a host of supporting agencies, met and replanned the information operations campaign. This in-depth planning took advantage of what we had learned during the conflict and was a quantum leap in the breadth and depth of the original campaign. This plan achieved a fundamental shift in emphasis. Originally, IO was simply an adjunct to targeting. In the revised plan, for certain classes of significant targets, the IO campaign needed to lead the prosecution of kinetic targets for two reasons. First, in order to achieve the full effect of physical destruction on the adversary, all the information elements must be executed in the proper sequence. If a significant target is to be struck to pressure the adversary, the messages that support it must be delivered in the correct sequence. So the timing of attacking a particular target must be sequenced with the information/non-kinetic fires that support it—just as a C4I target set must often be struck in the correct sequence. In addition, the human factors analysis that provides the optimum influence target set often needs to lead target selection. Ideally, the human factors analysis of adversaries needs to be a key element in targeting board decisions, and kinetic and non-kinetic targets need to be integrated into a single target list.

Needless to say, adding the IO dimension to a well-established targeting process in the middle of a conflict is not a simple task. And the number of people dedicated to the IO aspect was far too small. We originally stood up only a six-person cell at JTF Noble Anvil, enough to cover each of the primary capabilities. This was not nearly enough. When we developed another Joint Manning Document for a subsequent JTF, we established a 20 person IO cell for a planning-only JTF. This is probably close to optimum for a one-shift operation. The need for close coordination with targeting and intelligence requires far more than a cell one-deep in each key capability, and we discovered the need for expertise in intelligence, comm./computer and targeting that also needs to be organic to the IO cell.

Information Operations are a targeting discipline. In trying to understand and help our leaders understand what IO is all about, we should focus on the concept of targeting, which is understood at least in a macro sense by nearly all military personnel. IO is the effects-based targeting that directly seeks to affect the mind and will of the adversary. Sometimes we use public affairs, sometimes we use PSYOP leaflets, sometimes we try to confuse the mind of the adversary with military deception, and sometimes we make our point by destroying things. We have found that some of the best IO officers have been not only PSYOP officers or EW officers, but field artillery officers. In the Army, field artillery officers are very familiar with the concept of deep operations and direct and indirect fires, and as my old Deputy J3 used to say, "IO is just another kind of fires. You have artillery fires, you have infantry fires, and you have IO fires." It is noteworthy that KFOR I , which first occupied Kosovo and established the KFOR mission, established IO as their Deep Operations Group. For KFOR, deep operations were not attack helicopters, SOF and long-range artillery behind the FLOT—their deep operations were Information Operations.

Which takes us back to the strategy or mission area argument. Information Operations are part of a long strand of operational strategy. IO comes out of Information Warfare, which in turn came out of Command and Control Warfare (C2W). C2W was the central strategy to the successful conduct of Operation DESERT STORM. C2W was not something thrown into the soup to season it at the end; C2W was the central strategy to the entire DESERT STORM campaign. Information Operations, as the successor to C2W, needs also to be at the center of military thinking. IO takes the idea of dismembering the adversary's command and control structure as a means of defeating his military forces, and expands it to use information to achieve our objectives in peace as well as in war. Rather than being an adjunct to kinetic targeting, a thorough Information Operations analysis needs to be the foundation of target selection, both kinetic and non-kinetic. IO is, therefore, an integrating strategy and one that we need to advocate, not as an interesting additional activity alongside traditional military operations, but as a central concept that focuses operations to achieve the desired effect.

Lt Col Bowman is currently assigned as Deputy Chief of the Information Operations Division at HQ US European Command. He has led the IO effort in EUCOM for the past two years, including ALLIED FORCE and number of other crisis operations. He is an Air Force Electronic Warfare Officer (EWO) with a secondary specialty in Intelligence. He is a Master Navigator with 3,900 flying hours in B-52 and RC-135 aircraft. He has served in a variety of flying and staff assignments as an instructor in the B-52G and RC-135, and staff assignments at RAF Chicksands, UK and HQ USEUCOM as an intelligence contingency planner, analyst, and briefer. His IO experience includes several assignments as an Air Force Tactical Deception Officer, an OPSEC Officer, and as a Wing Weapons and Tactics Officer. Lt Col Bowman's academic credentials include a BS in Business Administration from St Louis University, MS in Administration, Central Michigan University, and a MA in International Relations, University of Southern California, London Center for International Relations. Lt Col Bowman has completed Squadron Officer School, Air Command and Staff College and Air War College.