



# Landpower Essay

No. 05-1  
January 2005



An Institute of Land Warfare Publication

## Combating Terrorism: A Joint Interagency Approach

by

Fred T. Krawchuk

### Introduction

The 11 September 2001 (9/11) terrorist attacks shocked the world, especially the United States and its allies. The United States is unused to the experience of terrorism on its own shores. U.S. citizens have become accustomed to relatively peaceful lives in this country and to the continued expectation of such lives. As a result, this tragedy continues to trigger many questions about security, both at home and abroad. More than three years after its attacks on the U.S. mainland, al Qaeda continues as a movement while America struggles with intelligence reform, interagency friction and an elusive threat. Recent terrorist attacks worldwide demonstrate that al Qaeda is adapting to its setbacks in Afghanistan and looking for new opportunities to strike at U.S. and international interests. Although progress has been made in homeland security and the Global War on Terrorism (GWOT), Americans should assume they will be attacked again.

Until the September 2001 attacks, terrorism was only a niche threat for the United States. Now it is at the forefront of the world's attention, and strategists need to better understand terrorist organizations, tactics, politics, communications, ideology and personalities. A cogent understanding of terrorist networks would help produce an appropriate strategy and organization to detect, deter and defeat them.

### Analytical Approach

To effectively combat terrorism, decisionmakers must have a clearer understanding of terrorism and its causes. Coupled with this understanding, a coherent strategy to find, fix (isolate) and finish terrorists is critical to ensuring that valuable U.S. resources are focused decisively to protect American interests. Specifically, this proposal will follow these analytical steps to formulate a counterterrorist (CT) framework:

- explain the uniqueness of the terrorist threat;
- based on the threat analysis, develop an appropriate CT strategy to detect, deter and defeat the threat;
- based on the strategy, recommend appropriate organizational structures that support implementation of the strategy.

*The Landpower Essay* series is published by AUSA's Institute of Land Warfare. The series is designed to provide an outlet for original essays on topics that will stimulate professional discussion and further public understanding of the landpower aspects of national security. The content represents the personal opinions of the author and not necessarily the position of the Association of the United States Army or its members. Candidate essays of 5,000 words or less may be submitted to: AUSA's Institute of Land Warfare, ATTN: Landpower Essay Series, 2425 Wilson Boulevard, Arlington, VA 22201. For more information about AUSA and the Institute of Land Warfare, visit our website at [www.USA.org](http://www.USA.org).

A comprehensive, systematic and relevant approach to counterterrorism necessarily includes several elements, among them shared strategy, structure and information systems across security agencies. Each element must be expertly designed and seamlessly work with the others to build an integrated means of dealing with threats at all levels. Though improved communications technology and better intelligence are significant and needed, they are not enough. An effects-based, systems approach to terrorism would be an excellent method for minimizing gaps in the fabric of U.S. national defense and for more successfully finding, fixing and finishing terrorists in the long term. The various components of the framework working in concert would help create synergy, make it more difficult for the enemy to penetrate U.S. defenses, and produce sharper and more focused offensive capabilities.

Protection of the United States and its interests requires an in-depth understanding of the multiple, complex threats it faces. As the nation realigns resources and focuses strategic assets and planning efforts, it must fully comprehend the nature of these threats and why they are so important to U.S. national security. Terrorism clearly presents an immediate threat to U.S. interests and those of its allies. The 11 September 2001 attacks concentrated on symbols of America's ideals and strengths. For a variety of reasons, the United States was caught off-guard. This tragic wake-up call demonstrated the threat terrorism presents to the U.S. view of itself as a nation, its strategic position among its allies and its relationships with many of the world's countries, especially Islamic nations. Protecting vital U.S. interests against a credible and capable threat is the primary reason the nation must expeditiously develop a more comprehensive approach to counterterrorism. In its role on the front lines of this effort, the U.S. military and other government agencies must develop and execute a systematic approach to detect, deter and defeat terrorist acts against the United States and its allies.

### **Terrorist Threat**

Understanding terrorists and terrorism will help the military and other elements of the U.S. government organize and focus resources to deal with emerging threats. To help frame the threat, CT strategists should look at al Qaeda as a global insurgency and fully appreciate the movement's compelling vision and sophisticated political strategy. Its members are mobile and elusive—distinct from the fixed and visible enemies of the Cold War era. This significant shift requires further transformation in the U.S. approach to dealing with a nimble enemy. Terrorists operate in flexible, networked organizations with a shared sense of values and beliefs. They are highly selective in their recruiting efforts, have an effective training program, and are skilled at managing and manipulating public perceptions and the media. Cellular structure facilitates compartmentalization and allows missions to continue when cells have been detected or disrupted. Current terrorist organizations do not generally utilize hierarchical structures; instead, they use decentralized, loosely structured networks. They adapt to local conditions and use creative means to achieve a shared end. These sophisticated networks also capitalize on up-to-date technology with off-the-shelf communications equipment and Internet access, turning e-mail, chat rooms and encryption into terrorist tools.

Leaders must understand that these small groups of dispersed terrorists patiently look for breaks in their targets' seams and methodically attack weak points. Terrorists take advantage of military, diplomatic, financial, physical, economic and informational vulnerabilities. This terrorist strategy is radically different from conventional threats. Terrorists do not offer traditional centers of gravity or large physical infrastructures to attack. Detecting, deterring and defeating a networked enemy presents new challenges to interagency planners, political leaders, policymakers and legislative bodies.

Given the ad hoc, dispersed nature of al Qaeda and similar terrorist organizations, security measures must be pursued within an international framework. Critical infrastructures that sustain American citizens are linked to global networks. Efforts to protect these structures will fail unless they are organized

regionally as well as domestically. Terrorist networks are spread too wide for the United States to combat without support from allies. The United States, to better provide homeland security, must more closely coordinate with its regional partners to detect, deter and defeat terrorist acts before they reach U.S. soil.

The enemy, current and imminent, will watch U.S. moves, adapt accordingly and attempt to surprise the United States in the future. As the United States improves its response to terrorism with preventive measures in airports and transportation systems and by bolstering the Department of Homeland Security (DHS), for example, it also must look ahead to and prepare for potential threats. Like the professional athlete who, to win the game, must always estimate where the ball will be rather than where it is at a given moment, the United States must know where the enemy is today, understand what he is doing and prepare for his future moves. If not, this nation will always be one step behind and is certain to suffer another tragic surprise.

## **Strategic Framework**

**A Flexible and Adaptable Approach.** Any counterterrorist or counterinsurgency (COIN) strategy must be comprehensive in its approach. The focus cannot solely be “kill or capture,” believing that only a physical center of gravity needs to be destroyed for the insurgency to end. Unfortunately, the terrorist threat worldwide is much more elusive and complicated. Terrorist recruiting, logistics, finances, ideology, propaganda and fear tactics have proved a formidable problem set for CT strategists and operators alike. COIN operations require an integrated, systems approach to a complex problem. Insurgency in Iraq, for example, makes clear that the U.S. government must adapt to a formidable opponent who is widely dispersed and decentralized, and whose many destructive parts are autonomous, mobile and highly adaptive.

With network-centric warfare in mind, counterinsurgency planners and operators have to better understand the political context and sociocultural environment in which they are operating. The vital connections among diplomacy, military power and other instruments of power in the war on terrorism require the U.S. military to be combat effective while creating and maintaining partners and allies in increasingly hostile regions. According to security expert Richard Heckler, author of *In Search of the Warrior Spirit*,<sup>1</sup> American power seen simply as a unilaterally wielded technological hammer will alienate cultural, ethnic and religious groups who will become increasingly hostile if America is not more sophisticated in its approach. At the same time, if the U.S. government does not maintain a security structure that can act quickly and forcefully it will be seen as weak, unprepared and easily exploited. Ancient Asian warrior traditions use a concept of “inward balance, outward preparation for action.” This capacity should be cultivated both in individual leaders and in counterinsurgency policy in Iraq and elsewhere in the GWOT. This means being extended and strong in working through, by and with coalition partners without being stiff and rigid—being flexible without being torpid.<sup>2</sup>

Understanding the local conditions of an insurgency and terrorism cannot be underestimated. Counterinsurgency planners must understand the needs of discontented groups. In addition to using military and federal agencies, counterinsurgency and counterterrorism planners should employ media specialists, finance and business experts, psychologists, social and organizational network analysts, cultural anthropologists, social scientists and religious leaders to develop a comprehensive picture. The more insight planners have into the causes of the insurgency, the better their capacity to effectively address those conditions. Insurgents require regional support. Understanding where and why they get their support, planners can help develop long-term strategies that will address the insurgents’ constituencies.

With this understanding in mind, counterinsurgency and counterterrorism planners and operators must take an interagency and multidisciplinary approach and produce an effects-based strategy that accomplishes the following:

- separate the insurgents and terrorists from the population by
  - denying insurgents sanctuary;
  - eliminating insurgent freedom of movement; and
  - denying insurgent resources and support;
- identify, kill, capture or detain the insurgents;
- create a secure environment;
- plan and execute long-term, comprehensive and integrated information operations and holistic civil affairs programs in harmony with the first three tasks that
  - address underlying causes of terrorism;
  - dissuade terrorists;
  - tarnish the terrorist image;
  - disrupt terrorist recruitment;
  - counter terrorist propaganda;
  - build support with the local populace;
  - help defeat threatening ideologies; and
  - coordinate U.S. government messages;
- develop and sustain host nation interagency capacities (military, law enforcement, intelligence, media, information operations, civil affairs, financial, diplomatic and economic) so a country or region with a terrorism threat can conduct the first four tasks successfully and unilaterally.

An effective counterinsurgency or counterterrorism campaign requires building bridges and creating incentives to more effectively blend diplomacy, justice, development, finance, intelligence, law enforcement and military capabilities. The U.S. government has to continue improving its ability to coordinate interagency and multinational operations in a timely and efficient manner. To do so, it must do a better job of integrating interagency capabilities and capitalizing on the assets and capabilities of its allies and partners. The 9/11 Commission Report states that long-term success in the war on terrorism “demands the use of all elements of national power: diplomacy, intelligence, covert action, law enforcement, economic policy, foreign aid, public diplomacy, and homeland defense. If we favor one tool while neglecting others, we leave ourselves vulnerable and weaken our national effort.”<sup>3</sup> Unity of effort in the interagency environment can be achieved only if all critical agencies are included in the counterinsurgency planning process. Leaders should provide incentives to improve integrated planning, train interagency personnel for working in complex and dangerous environments, and build mobile and expeditionary interagency teams. Equally important, the U.S. government needs to capture lessons learned and best practices to develop and institutionalize the civilian and military capabilities needed to be successful in counterinsurgencies.

By combating an insurgency in a more collaborative manner, planners could share critical information, track all parties involved in the insurgency network, coordinate themes and messages and develop a comprehensive picture of insurgents and their supporters, nodes, systems, processes, events and plans. With this information in hand, the U.S. government would be better prepared to systematically disrupt or defeat all of the critical nodes that support the entire insurgent network, thus rendering it ineffective.

With a more complete picture in hand, counterinsurgency planners can effectively use a networked organization to quickly take actionable intelligence and execute counterinsurgency operations in a

synchronized fashion. Much of the work in transforming future U.S. military capability focuses on command and control, i.e., on getting more and better information to the commander so that he or she can see and direct the battle. Although this is important, it also is challenging if the concept requires collecting and passing information to headquarters, where it is analyzed and then passed back to the battle. Effective and efficient network-centric warfare promotes collaborative sharing of information and planning, enhanced situational awareness, and rapid synchronization of joint, interagency and multinational operations.

Counterinsurgency experts who understand network-centric warfare know that battles against small, independent and mobile formations change too rapidly to allow rigid, centralized command and control. The U.S. military and other government agencies will have to continue to adjust and fight accordingly. Fast and fluid bottom-up planning and execution supported by top-down guidance, resources and support is an appropriate approach to counterinsurgency. Intelligence, logistics and communications must integrate horizontally and vertically with operations to support this innovative approach to fighting insurgents. Counterinsurgency forces, with clear guidance and appropriate technology, can be command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) nodes and execution nodes, greatly shortening the decisionmaking loop while still allowing the passing of information on actions and results to higher levels for strategic analysis.

**Joint Interagency Action Teams – Introduction.** The Department of Defense (DoD), Central Intelligence Agency (CIA), Department of State (DoS), Federal Bureau of Investigation (FBI) and DHS are working to untangle lines of authority, deconflict overlapping responsibilities and improve coordination of interagency counterterrorism operations in a timely and efficient manner. Continued worldwide attacks by elusive and deadly terrorists greatly increase the government’s responsibility to make additional changes that will further close the gap between detecting terrorist activity and rapidly defeating it.

The basic strategy, then, must look at how the U.S. government detects, deters and defeats this kind of enemy. The effectiveness of a CT strategy is, in part, based on the capacity of national and domestic agencies and the departments involved in defense and law enforcement to think like the enemy in anticipation of how they may act in a variety of situations and aided by different resources. Another form of deterrence is to correct the internal flaws of U.S. agencies. DHS, for example, is centralizing resources from various agencies to more effectively share information, thus hedging against the possibility of critical pieces of information falling through the cracks in U.S. national defense. This kind of initiative and others must take place at all levels of government. Effective detection and deterrence increase U.S. capacity to defeat a networked enemy. This goal requires that departments and agencies organize themselves for maximum efficiency and information sharing with the ability to function quickly under new operational definitions. New times make new behaviors necessary. Organizations must do what they have been reluctant to do in the past—they must reach across bureaucratic territorial schisms and share resources to defeat terrorism and other emerging threats.

New systems, procedures and programs must be built in a coordinated fashion to facilitate and institutionalize interagency coordination and deconfliction. CT organizations must be able to plug into a networked system in a manner that allows them to take a systematic and effective approach to beating terrorists at their own deadly game. Additionally, given limited resources and diverse interagency perspectives on terrorism, a more integrated interagency approach to CT operations can help provide a wealth of information and capabilities supporting complex CT contingencies.

To develop a more comprehensive and responsive CT capability, the CIA, FBI, DoD, DoS and DHS must systematically integrate interagency personnel and resources and set up a network of joint interagency action teams (JIANTs) in:

- a national CT fusion center that blends strategic offensive, defensive and informational (“hearts and minds”) CT efforts;
- joint military commands to help bridge civilian agencies and the military;
- key U.S. embassies and transnational regions to focus assets and coordinate with allies against non-state actors;
- key regions within the United States to develop a multi-jurisdictional CT approach.

Although different in scope depending on location, JIANTs would perform similar functions:

- paint a comprehensive picture of terrorist networks;
- plan, coordinate and monitor interagency CT operations (short-term and long-term);
- ensure connectivity and interoperability through networked CT centers that fuse domestic and foreign intelligence, operations, communications, logistical support and feedback mechanisms;
- integrate crisis and consequence management;
- plan and implement long-term public diplomacy, host nation capacity building, strategic communications, education, development projects and civil affairs programs.

The United States must blend short-term kill-or-capture operations with host nation capacity building and other long-term efforts to address root causes, dissuade future terrorists and reduce recruiting. The 9/11 Commission Report emphatically states that the United States must “help defeat an ideology, not just a group of people.”<sup>4</sup> Growing anti-American and anti-Western sentiment spelled out in numerous recent polls cannot be ignored. As JIANTs help conduct offensive and defensive CT operations, ways must also be found to prevent the spread of jihadist ideology and help promote the U.S. image abroad. This would include promoting rule of law, educational programs, cultural exchanges and development projects.

To win the war of ideas the United States must also confidently tell the truth, honor its words with its actions, counter propaganda and communicate its messages quickly and effectively. The 9/11 Commission Report warns, “If the United States does not act aggressively to define itself in the Islamic World, the extremists will gladly do the job for us.”<sup>5</sup> *Wall Street Journal* writer Robert D. Kaplan further states:

Because the battles in a counterinsurgency are small scale and often clandestine, the story line is rarely obvious. It becomes a matter of perceptions, and victory is awarded to those who weave the most compelling narrative. Truly, in the world of postmodern, 21st century conflict, civilian and military public-affairs officers must become war fighters by another name. They must control and anticipate a whole new storm system represented by a global media, which too often exposes embarrassing facts out of historical or philosophical context.<sup>6</sup>

The United States is in direct competition with radical fundamentalists on the battlefield and in the media. Any CT or COIN strategy must consider this and ensure that comprehensive information operations, civil affairs and host nation capacity building are integrated with the overall plan. Improving interagency systems and procedures would help the U.S. government implement necessary changes to the way it develops and communicates thoughtful and persuasive messages to the right audiences at the right time with the appropriate means.

Pooling interagency resources for CT operations would capitalize on the strengths of each organization and tighten the seams between different organizations. JIANTs would help bridge the gaps among media conduits, policymakers, intelligence agencies, law enforcement agencies, military commands and

crisis and consequence managers. They would improve interagency relationships and reduce redundancies and discontinuities. JIANT-linked eyes and ears throughout the entire chain of terrorist activities would produce a more complete picture of emerging threats. JIANTs located globally at strategic points would offer a faster and more wide-ranging response to these threats. By bringing together different capabilities and resources, JIANTs would create more opportunities to detect and defeat terrorists.

**JIANTs – Domestic Approach.** To be nimble and responsive against a methodical and networked enemy requires that leaders connect organizations horizontally and vertically to share resources and information that would lead to pursuing appropriate actions. In the United States and abroad, top performers from the military, diplomatic, economic, law enforcement, financial and informational sectors would make this happen by forming groups whose purpose is to develop a common picture at the local, regional and national levels. With a more complete sense of what is happening on the ground, JIANTs would then be able to help develop appropriate courses of action (short-term and long-term) to address specific emerging threats or opportunities.

Pooling resources horizontally would build synergy by capitalizing on the strengths of each organization while helping each better manage its respective weaknesses. By tying national, regional and local organizations together, JIANTs would help bridge the vertical gap between policymakers and those “at the pointy end of the spear” who put policy into action. Accurate and timely information from the front would also help national and regional decisionmakers make appropriate and opportune decisions. Enjoying full access to intelligence, planning resources and their respective decisionmakers, JIANTs would help leaders move quickly to detect threats, deter attacks, conduct preemptive strikes, coordinate themes and messages and counter anti-U.S. rhetoric and propaganda.

To help develop actionable intelligence against terrorists, JIANTs would work at a national CT center, assisting in linking DHS, the National Security Council and U.S. Northern Command, ensuring that these key national security entities share a common operating viewpoint and are able to take decisive action at the strategic level. The 9/11 Commission Report recommends the “establishment of a National Counterterrorism Center . . . a center for joint operational planning and joint intelligence, staffed by personnel from various agencies.”<sup>7</sup> Clearly, intelligence must be both physically and procedurally integrated within strategic operations. JIANTs would be the interagency action officers with a strategic focus at a national CT center, where they would help fuse intelligence and operations. This fusion would help national-level planners manage terrorism-related information and develop strategic CT plans. JIANTs would act as the glue between domestic and international counterterrorism efforts and serve as the focal point for JIANTs abroad.

**JIANTs – International Approach.** JIANTs would also work with combatant commands throughout the world to help build the bridge between national assets and joint commands and clarify the terrorist picture in a combatant commander’s theater. Using superior intelligence, JIANTs would enable combatant commanders to form more detailed ideas regarding the ways in which regional activities affect U.S. interests. They would be liaisons with allies in the theater and act as the regional commander’s interagency CT targeting cell. Pooling resources, information and interagency talents, JIANTs would be designed strategically to help strengthen relationships between different organizations and operational entities. Flexible, multifaceted interagency teams would help develop the operational picture, frame the CT problem and develop an appropriate response for the combatant commander.

At the local level abroad, JIANTs would fill a number of roles vital to fully countering terrorism. They would work with embassies and host nation authorities to help focus country team assets in the fight against terrorism. Depending on what the ambassador needed, JIANTs could provide liaison to host nation CT forces, support public diplomacy, coordinate civil-military relations and promote civic action

projects. Within an embassy, JIANTs could also act as the CT interagency intelligence and operations fusion cell. They would collect information from a variety of sources, paint a comprehensive picture of what is happening on the ground, offer appropriate courses of action, and support operations as necessary. JIANTs could also act as scouts, gathering information to help fill in gaps, working unilaterally or in conjunction with host nation forces. They would also be linked vertically with the regional and national JIANTs to help bridge the gap between policymaking at higher levels and the action needed at the grassroots level in the war on terrorism.

**JIANTs – Domestic/International Linkage.** Within the United States, the JIANT concept might also be used to help local and regional authorities develop a more integrated, multi-jurisdictional and networked capability to deal with terrorism. JIANTs could augment the FBI's Joint Terrorism Task Forces and help broaden and deepen links among the intelligence, law enforcement, military, and diplomatic communities. Linked internationally, they would help warn local officials of possible attacks, help prepare for emergencies and support domestic agencies as they thwart local attacks. This would enable law enforcement agencies, health authorities, fire departments and local governments to share resources and information, as well as to coordinate operations in detecting, deterring and defeating terrorist attacks. Linked together, these JIANTs would continually share information, building the terrorist situational picture. JIANTs would help network information, assets and operations throughout the world and be a key to detecting, deterring and defeating terrorism.

Domestic JIANTs would also look inward at U.S. security concerns. The most effective way to uncover and correct security weaknesses in any system is to simulate a determined attempt to penetrate the system in the manner likely to be used by a real attacker. JIANTs would methodically attempt to exploit all known and suspected security holes to discover vulnerabilities. This would greatly assist in the development of suitable defense measures and would serve to inhibit a terrorist's freedom of maneuver.

**JIANT as Part of a Strategic Plan.** The complete JIANT system would work concurrently at all levels:

- Information related to terrorism would come to the JIANT (or the JIANT would aggressively collect information) from any number of different sources. JIANTs would be proactive; they would not sit back and wait for a threat or opportunity to arise.
- Data would be analyzed and reviewed by trained analysts. When hard facts and vetted sources are not readily available, pattern recognition, predictive analysis and brainstorming using complexity science would be welcomed.
- JIANTs (having merged intelligence, analysis and operations) would assess their capacity, based on an evaluation of the assets on hand, to further monitor, deter or defeat a terrorist threat or exploit an opportunity.
- Working closely with ambassadors and local vetted authorities, JIANTs would quickly exploit an emerging threat or opportunity (U.S./unilateral, combined U.S./host nation or host nation/unilateral).
- Regional and domestic JIANTs, engaged in a similar assessment, would add to the picture and mobilize additional assets.
- If the combatant commander, host nation assets, or lead U.S. agency could not respond properly to a terrorist situation, the JIANT could depend on the national-level JIANTs for additional support.
- JIANTs would constantly assess results, adapt plans and programs accordingly, and ensure short-term and long-term CT goals and objectives remain consistent and mutually reinforcing.

All the while, the JIANTs would track terrorist movements, whether they are personnel, materials, components of weapons of mass destruction, radio communications, Internet traffic or other information

channels. In line with their long-term goals, the JIANTs would monitor this information, wait for the opportune moment to exploit the situation and avert a potential terrorist catastrophe. Alongside Northern Command and DHS, the stateside positioning of JIANTs would provide for the collective protection of the continental United States. JIANTs at forward positions would be global scouts, looking for indicators of potential terrorist operations abroad. This structure would provide worldwide coverage and linked mechanisms for quick and decisive action as necessary.

The JIANTs' approach would take advantage of a networked, distributed force of coordinated but independent interagency elements with a wide range of capabilities. Instead of using traditional sequential or linear planning, JIANTs would plan simultaneously and collaboratively. They would fuse C4ISR assets and focus them directly on a small, effective formation at the tip of the spear, allowing JIANTs to apply the right tool at the right time in the right place for the agreed-upon purpose.

Planners, information technology (IT) and security specialists, logisticians, financiers, operators and communicators from different agencies working together simultaneously would help build the terrorist link diagram. By looking at a terrorist organization in a collaborative manner, JIANTs could build an operational picture of critical terrorist nodes and take appropriate action. For example, many government agencies, to include DoS, FBI and the Treasury Department, look at how terrorists finance themselves and, based on their information, have taken important steps in concert with allies to freeze terrorist assets.

JIANTs would take this approach several critical steps further by working with a variety of intelligence, military, diplomatic, law enforcement and other interagency elements to track other parties involved in the entire terrorist chain and thus develop a more comprehensive organizational picture of people, events and plans. With this picture in hand, they would then systematically disrupt or defeat all of the critical nodes that support the entire terrorist network, rendering it ineffective.

Following operations against a terrorist target, JIANTs would closely monitor the situation, observe the consequences of actions taken and look for other emerging targets and opportunities. In all their operations, after actions are taken against a military, economic, diplomatic or informational target, JIANTs would follow the ripple of consequences. This could lead to other emerging targets and provide continued assistance in developing a comprehensive picture of what is happening on the ground. Just as the military conducts battle damage assessments of a target, the JIANT would do a post-operation interagency assessment to link diagrams and exploit new targets and opportunities. This assessment must include media analysis, polling and evaluation of the effectiveness of offensive, defensive, informational and "hearts and minds" plans and program.

**JIANT as a Critical Tool.** When one hits a bee's nest, bees scatter. Watching where the bees seek sanctuary; how other hives react; how and where they get new resources, seek new training and recruit replacement personnel; and how they identify and report to the queen bee is a crucial model for JIANTs to follow. By consistently applying pressure and staying ahead of terrorists, JIANTs could make them react, keep them off-balance and force them to show their hand. Additionally, by operating as a networked team at various levels, JIANTs could help conduct concurrent operations to fight terrorism at all levels. Instead of taking a traditional mass-and-maneuver approach, JIANTs would quickly converge on terrorist targets from multiple directions. The interagency targeting cycle would continuously seek emerging targets and opportunities. These proactive, prescriptive and preventive approaches would be highly preferable to the more passive tactic of responding defensively and reactively, which is what terrorists want the United States to do. Using the metaphor of terrorists as bees, JIANTs would understand that swarming the beehive would effectively paralyze significant components of a terrorist network. By bringing together different perspectives and types of information, JIANTs would build the CT puzzle and create more opportunities to detect, deter and defeat terrorists.

In Afghanistan, exploiting enemy locations and sharing captured information have helped improve U.S. knowledge of the ways terrorists train and operate. JIANTs would ensure that other agencies and allies have access to this exploited information so they would be better able to gather clues on other aspects of terrorist operations. From planning to execution, training JIANT-linked eyes and ears on as much of the chain of terrorist activities as possible would produce more complete nodal analysis for CT operational planning. This would directly help develop more complete link diagrams of terrorist organizations, which could only improve America's capability to detect, deter and defeat terrorist activities.

In addition to their inherent intelligence, operations and targeting advantages, JIANTs would also work with incident response teams that deploy into regions inside and outside the United States to help mobilize resources and information. Being close to hot spots, the JIANTs might also act as the initial crisis site command and control center until the appropriate agency took over. Since JIANTs would be deployed forward in theater, they could respond to crises in addition to monitoring local situations. Moreover, by closely monitoring emerging threats, the JIANTs would build regional expertise and local networks, which in turn would provide connectivity with various agencies and local authorities vertically and horizontally.

Yet another advantage of the JIANTs would be their contributions on diplomatic and policymaking fronts. They would be designed to help ambassadors, regional commanders and national decisionmakers manage their countless challenging national security tasks. At all levels—national, regional and local—many competing security interests intersect. JIANTs would help ensure that concerns about terrorism and other critical, emerging threats stay at the forefront of a leader's attention as necessary. As the interagency lead for CT, JIANTs would be a proactive and responsive focal point for decisionmakers regarding terrorist issues and concerns. This would also let ambassadors, combatant commanders, national decisionmakers and local officials focus on their other innumerable responsibilities in addition to emerging threats such as terrorism. Any time a crisis or terrorist incident occurred, a properly trained and equipped, fully functional mechanism would be in place to handle it, without having to create an ad hoc element out of hide.

An interlinked web of interagency coordination in the form of JIANTs would quickly assess situations, mobilize resources and take appropriate action on a variety of levels and for multiple disciplines. By vertically and horizontally aligning information and resources, JIANTs would develop a more complete picture, quickly provide the correct multiagency response and immediately mobilize needed resources. This networked integration would also mitigate the terrorists' own networked approach and minimize U.S. national security and informational seams. A tightly linked web of information and defined interagency capabilities would comprise a nimble and flexible entity to go after emerging threats, offering a more elusive and difficult target for terrorist organizations. Placing these JIANTs throughout strategic international locations would put them closer to potential launch points of CT operations, thus increasing the chance of deterring terrorist operations. JIANTs could also assist in coordinating the entry of appropriate means to defeat terrorists if a preemptive strike is deemed necessary. JIANTs would help provide unity of effort in CT planning and execution, in addition to their capacity to integrate limited resources and diverse viewpoints on the terrorist problem set. JIANTs, then, would act as enablers of networked information, operational coordination and logistical support that directly detect, deter and defeat terrorists.

**Implementation of Interagency Goals and Cooperation.** To support implementation of JIANTs and be more effective in CT/COIN operations, the military and other government agencies need to enhance interagency capabilities. DoD has made great strides in improving joint interoperability; it must now take the next logical step forward along with other government agencies to do the same within the interagency realm. These changes will not be easy. The 9/11 Commission Report states, "It is hard to break down stovepipes when there are so many stoves that are legally and politically entitled to have cast-iron pipes

of their own.”<sup>8</sup> Congress should produce legislation similar to that of the Goldwater-Nichols Act. This would help improve the interagency process by offering incentives and directives for interagency systems and procedures, new liaison positions, career assignments, training and education. Moreover, legislation would help create a more collaborative interagency culture that would nullify the stovepipes and rice-bowl mentalities that disrupt and inhibit interagency cooperation.

Legislative and executive-level directives are needed to substantially update and streamline interagency CT/COIN systems and procedures among DoS, DoD, FBI and the intelligence community. These agencies have very different perspectives, organizational cultures and overlapping responsibilities. Agencies must evolve strategically and operationally so that they can more effectively gather and exploit actionable intelligence, conduct operations, coordinate themes and messages, develop/execute long-term “hearts and minds” programs and truly become more integrated. To help make this happen, the National Security Council or the emerging National Counterterrorism Center should consider developing an “operational arm” with the authority of the President to deconflict, synchronize and task the various agencies of the government involved in CT/COIN operations.

This operational arm would also help ensure U.S. government agencies’ CT training programs and operations are thoroughly synchronized and deconflicted. Specifically, it must coordinate DoD Theater Security Cooperation Programs, DoS Antiterrorism Assistance Programs, and intelligence and law enforcement host nation capacity-building programs. Interagency leaders should align these initiatives with military and other government CT/COIN operations. Who and how the United States trains host nation counterparts and builds their capacities as an interagency community (military, intelligence, law enforcement, diplomatic, financial) should be consistent with who and how the United States conducts CT/COIN operations. Synchronizing these training programs among the different government agencies at the national, operational and tactical levels and then aligning them with CT/COIN operations would build synergy, avoid duplication of effort and ensure training leads to operational success.

Interagency challenges and unconventional threats will also require the selection and promotion of the right kinds of people to support JIANTs and other interagency positions. CT planners and operators have to be creative risk takers who appreciate a multidisciplinary and integral approach to complexity. They cannot be protectors of the status quo or risk-adverse careerists. Placing talented people in a collaborative work environment led by competent innovators would help instill the more adaptive organizational culture needed to engage ambiguous threats.

These talented interagency personnel will be needed in greater numbers as liaison officers between the different government agencies in order to better understand and complement one another’s strengths, share information and coordinate planning. To close interagency gaps, more resourceful and trained leaders must be placed with JIANTs and other critical interagency liaison positions, with expertise in the following responsibilities:

- educating the interagency community on capabilities and limitations;
- shaping and sharpening interagency plans and operations;
- providing timely information that would potentially accelerate the national decisionmaking process and improve the flow of critical information;
- helping establish systems and procedures to institutionalize CT/COIN planning and operations and tighten the seams between the military, law enforcement, intelligence and diplomatic communities (vertically and horizontally); and
- developing relationships and networks that will provide better support for policymakers and operators alike at all levels.

The government should place top performers in key interagency and JIANT positions. Joint assignments are highly sought and typically viewed as career enhancing by the military; the military and other government agencies will have to look at interagency positions in the same way. Duty on a joint interagency team should be another track that operationally- and strategically-oriented government personnel could successfully pursue and be rewarded accordingly. The military, as well as the rest of the government, must assign to JIANTs qualified personnel who would act as global scouts detecting, deterring and defeating terrorists. With unconventional threats in the forefront, changes in the interagency personnel and assignment process will be necessary to adapt to the new security environment.

## **Military Support**

Another way to improve our collective ability to fight terrorism and other emerging threats would include recognizing that CT and unconventional warfare (UW) are the bread and butter of the special operations forces (SOF). Additionally, information operations (IO) personnel are ideally suited for host nation relationship-building, strategic communications and hearts-and-minds programs. SOF and IO personnel are uniquely suited for networked, distributed warfare against terrorists and insurgents. While waiting for JIANTs to be created, SOF and IO personnel should be placed in key positions within the Joint Interagency Coordination Groups at the combatant commands, CT positions in the policymaking community, and abroad with embassies to apply their expertise to the complexities of terrorism.

In addition to placing more SOF personnel in key military and interagency CT-related positions, DoD should also consider exchanging additional personnel between its military commands. Given the nature of terrorist threats, exchanging liaison officers more widely between the combatant commands, U.S. Special Operations Command (USSOCOM) and U.S. Strategic Command (USSTRATCOM) would help fill seams and gaps and build a tighter worldwide network for the military to track terrorist networks as they move across geographical boundaries.

Establishing forward-based Joint Special Operations Task Forces (JSOTFs) in close consult with host nations and U.S. country teams would be an important step for the U.S. military. Linked with JIANTs, JSOTFs would provide an interoperable force with a broad range of skills and the maturity to execute mission orders without detailed oversight. Putting them forward in regional theaters would allow this expertise to be applied more decisively. They would be better able to take advantage of actionable intelligence, which requires a tighter decision loop between “sensor and shooter.” Forward-based joint/interagency organizations would promote regional orientation, closer proximity to potential targets and opportunities, and development of standard operating procedures needed for complex CT, UW and IO missions.

A JSOTF should operate as the supported command in a theater of operations where CT operations are being conducted. This would enable the military and other relevant government agencies to pursue a focused CT campaign with in-house experts, planners and operators on the ground and at the headquarters. The complexities of CT/COIN operations require sophisticated leadership with a keen understanding of CT, UW and IO and the resources required to fight effectively. USSOCOM would also provide needed guidance on conditions and standards for JSOTF training, systems, equipment and procedures. SOF integration with host nation and U.S. conventional units would be more efficient with USSOCOM and the Theater Special Operations Commands as the supported commander in CT-focused operations.

This forward-based approach demands diplomacy and respect for political sensitivities. Therefore, JSOTFs would focus on working in harmony and close coordination with their host nation counterparts and U.S. embassy officials. Although the military needs to kill or capture and detain terrorists, these direct-action missions should not be at the expense of the “advise and assist” approach that Foreign Internal

Defense (FID) and UW offer as their centerpiece. Working through, by and with host nation counterparts, to include training in human rights and respect for civil authorities, should be at the core of any successful counterterrorist or counterinsurgency strategy. Both FID and UW are essential to building capacity among friends, allies and coalition partners, which will help deter terrorism and insurgency.

SOF, especially U.S. Army Special Forces, are the only forces able to conduct sustained unconventional operations in the heart of areas in which terrorists freely operate. They are trained, equipped and educated for conducting unconventional warfare in an uncertain environment. SOF can do this with little external support and low overhead from higher headquarters in a low-visibility manner, which supports DoD's concept of small footprints throughout the world. This modus operandi respects local populaces and can actually help increase the legitimacy and improve the image of the United States among host nation populations.

To support implementation of JIANTs and forward-based JSOTFs, the military personnel departments must put skilled, experienced and interested people in these new organizations. DoD needs to improve the Joint Manning Document (JMD) development and sourcing processes to better support joint commanders. Selection criteria and specific standards must also be put in place. Applying joint manning lessons learned from recent JSOTF missions in Operations Enduring Freedom (OEF) and Iraqi Freedom (OIF), Joint Forces Command and the Joint Special Operations University would help build a strong foundation for creating standing JSOTFs.

For military personnel who enjoy and are successful in operational and strategic assignments, interagency duty would be satisfying work and would make a significant difference in U.S. national security. In the Army, for example, an officer or noncommissioned officer (NCO) could work in one of these interagency assignments following branch qualification, allowing the military personnel department to focus on putting its people in positions where they can best apply their skill sets. If the country's top priority is fighting terrorism, the military's personnel system must follow suit and put incentives in place to support interagency assignments. CT operations and interagency manning are much too complex and crucial for the all too common "fill spaces with faces" approach to assignments. Fortunately, the U.S. military currently has a strong pool of talent. To capitalize on this, the military should focus on putting skilled, experienced, qualified and interested NCOs and officers in key interagency CT positions.

The military must identify officers and NCOs with the right skill sets and attitudes for interagency work and ensure they have the necessary tools to keep their individual skills honed. Military personnel destined for a joint task force or key interagency position must take interagency and joint courses and become familiar with other agencies and joint headquarters. Military professional development courses should include an interagency-related focus and increase the number of exchange instructors from other government agencies. The military should also work collaboratively with other government departments engaged in the war on terrorism. Just as DoD prides itself on making its officers and NCOs "purple" (joint), the next step is to make a select group "gold," i.e., able to smoothly and efficiently operate in an interagency environment. The military will need to recognize this and ensure that promotions and school and assignment selections reflect the importance of personnel adequately trained for interagency assignments. Putting the best and brightest of military officers and NCOs in critical interagency liaison jobs is crucial to the next phase of preparing the U.S. military for future CT operations.

For a comprehensive CT strategy to be effective, JIANTs, JSOTFs and other joint and interagency teams would, on a regular basis, require a venue for training under realistic conditions. Establishing a joint interagency training center also would allow joint and interagency elements to plan, coordinate and rehearse together at all levels. The military has increased its lethality and combat effectiveness through years of training at combat training centers (CTCs). Building upon and linking these centers, joint and interagency elements would be able to integrate planning, procedures and C4ISR compatibility. Applying

a CTC-like model, joint and interagency headquarters could regularly train together to develop interoperability. In this manner, joint and interagency headquarters would be able to work out their systems and procedures and train with tactical-level elements, including JIANTs. This process would also produce stronger joint and interagency capabilities, serving as an excellent means of preparing these elements before they are deployed forward into their respective theaters and embassies.

### **Interagency Information and Communications Systems**

All activities of government agencies must focus on the most efficient and effective provision of resources that assist the CT effort. Improving the quality and quantity of intelligence analysts and language-trained personnel who can help develop a more comprehensive picture of threats and opportunities is a crucial step. Even with the right organizational structure and training venues in place, CT analysts and operators would be ineffective unless they had access to fast and uninhibited flows of information. Among the various agencies involved in fighting terrorism, the proper safeguarding and efficient sharing of information is imperative. Too often, compartmentalization and territorial interagency arguments regarding the need to know confuse the bigger picture and endanger the success of missions and operators on the ground. Of course, methods, personnel and procedures should be protected, and agencies must employ and deploy people with appropriate security clearances. To this end, it would be important to provide employees with the required clearances or to otherwise ensure that information is classified appropriately so that it could be reasonably and quickly shared. Bureaucratic stovepipes and informational seams do not contribute to the overall CT effort. In fact, they severely inhibit building a complete enemy picture. Jetliners were flown into buildings on 11 September 2001 because the enemy took advantage of seams in U.S. defenses and relied on the lack of shared information between agencies.

A national IT effort is needed to build an interagency, interactive communications system. The 9/11 Commission Report recommends that “agencies should still have their own databases, but those databases would be searchable across agency lines . . . an outstanding conceptual framework for a trusted information network has been developed by a task force of leading professionals in national security, IT, and law assembled by the Markle Foundation.”<sup>9</sup> Unfortunately, the recommendations in the report have not yet been implemented. Action in this area is imperative because interagency teams need management systems and processes to help gather, track and process information and requests. To help institutionalize information and resources sharing, the U.S. military must work with other governmental agencies on information management systems, information technology and compatible C4ISR. Given the array of information technology capabilities today, the U.S. government needs to build web-linked interagency databases and communication systems. A JIANT team member, for example, would access and feed information to the FBI, CIA, DoD, DoS, DHS, the National Security Agency (NSA) and other relevant departments and agencies. For interagency operations to be agile and relevant, an interoperable, multiagency information management system is imperative.

This interagency information management system should include links across relevant agencies and the lessons learned from previous CT operations, terrorist targets, terrorist profiles, link diagrams, data mining, media analysis and other integrated databases from a variety of sources. It should offer both interagency analysis and collaborative planning tools. This type of integrated information system would effectively break down the schisms that now exist between agencies and help put the pieces of the complex terrorist puzzle together. Moreover, a web-based, interactive system would allow teams on the ground to stay linked and better coordinate operations.

Having the means to quickly and securely coordinate across agencies is essential to impeding terrorism. Challenges in communications among law enforcement, firefighters and others in New York City in the aftermath of 11 September 2001 indicate how all parties involved in terrorist incidents would

benefit from shared, secure and durable multiagency information management and communications. These lessons need to be applied at all levels of interagency relationships to prevent similar mishaps in the future and to develop the capacity to quickly assess situations, share information and communicate appropriate action.

## **Conclusion**

Terrorism remains a dangerous threat for the United States and its allies. Recent terrorist attacks in Europe, Asia, the Middle East and Africa demonstrate that al Qaeda is adapting and reorganizing. Given al Qaeda's global reach, the United States must develop a more integrated CT strategy with its allies to detect, deter and defeat this threat at its many levels. To counter this menace, the nation must continue to develop flexible and efficient capabilities through innovative interagency organizations. Adaptive JIANTs would quickly assess dangerous situations, mobilize resources and take appropriate action at a variety of levels and across relevant disciplines. Directing department heads to institute interagency fusion centers worldwide would better protect Americans, both at home and abroad.

To successfully accomplish the devastation of 11 September 2001, terrorists looked at all elements of U.S. national power and crafted a simple, effective and surprising attack. Patiently looking for breaks in the national security fabric, they found an effective way to cause significant damage to U.S. interests. Their detailed target analysis included avoiding the strengths of U.S. national security and capitalizing on the weaknesses, including fault lines within immigration, transportation, law enforcement, financial, informational and intelligence systems, as well as with the likely military response.

Developing a comprehensive way of combating terrorism demands an effectively coordinated systems approach, using the best expertise of agencies at all levels of government and the private sector. To detect, deter and defeat a networked enemy requires observing, targeting and hitting the entire terrorist chain and the most critical nodes of a terrorist organization. Synchronizing offensive and defensive CT operations with public relations efforts, information operations, host nation capacity building and development projects would blunt terrorist recruiting, propaganda and radical ideology.

JIANTs would provide an effective, well-organized and easily implemented approach to combating terrorism at home and protecting U.S. interests abroad. Coordinating appropriate assets and resources would provide a nimble and adaptable means of combating terrorism. JIANTs, task organized to take advantage of the synergies of different departments, would be designed to help fuse intelligence and operations. Shortening the decisionmaking loop by providing on-hand access to appropriate assets, JIANTs would stay ahead of terrorists and keep them guessing, instead of the other way around. Crossing interagency boundaries and blending capabilities would help close the seams of U.S. national security and make the terrorists' task much more difficult. It would also increase the capacity of the U.S. government to find and disrupt terrorism by making a variety of different perspectives and capabilities available to leaders at local, regional and national levels.

To complement JIANTs, the military should deploy JSOTFs with IO assets forward in strategic locations around the world. Having an established joint footprint forward would provide an effective and interoperable military force available for preemptive action and host nation capacity building. As with JIANTs, in a systems approach to CT operations proper selection, training and development of personnel to staff these new organizations would be imperative. To support JSOTFs and regional combatant commanders, USSOCOM should be the supported command in appropriate circumstances. This would help coordinate CT expertise and resources.

For joint and interagency organizations to be successful, a deeper appreciation of the risks and potential for mistakes would be needed to better support decentralized operations against a murky enemy. Having a complete picture against a mobile target will not be the norm. Leaders on the ground will need the

confidence and trust of the U.S. government and the American people to act on a lack of perfect information. Waiting for a traditional hierarchy to send information up and down a lengthy chain of command could allow terrorists to escape, or worse. Attacking a networked enemy requires operating as a networked interagency community, with all the assets and authority on hand to act fast on available information.

Having the right strategy plus integrated, nimble counterinsurgency organizations—although extremely important—is not sufficient if leaders are unprepared to engage within ambiguous environments and reorient their organizational culture to deal with insurgencies. A successful counterinsurgency or counterterrorism campaign is not just about better intelligence or new organizations. It’s also about transforming the attitudes and mind-sets of leaders so they have the capacity to take decisive yet thoughtful action (based on a set of values) against insurgents in ambiguous situations. Ideally, the U.S. government would have in place law enforcement officers, intelligence analysts, economists, diplomats and military leaders who are sentient sensors and thoughtful decisionmakers capable of working seamlessly within military, civilian, media and international communities.

To develop this capacity, leaders must dedicate themselves to innovative training and education. In addition to traditional hard skills, soft skills in negotiations, psychology, social and cultural anthropology, languages, foreign area studies, integral studies, somatics, emotional intelligence, complexity theory and systems management will become increasingly important. Like the martial arts master who deftly handles multiple attacks, the counterinsurgency expert in a fast-moving and fluid environment, with multidisciplinary training and interagency experience, would learn to adapt to any given situation to serve selflessly. This new attitude is imperative. An integrated and comprehensive approach to counterinsurgency and counterterrorism requires a continued reorientation in the way the U.S. government plans, organizes, trains and thinks about complex and unconventional threats. Leaders engaged in the war on terrorism would become, through innovative training and adaptive organizations, “as hard as a diamond, flexible as a willow, smooth-flowing like water or as empty as space”<sup>10</sup> so they could make appropriate decisions that protect vital national interests. With such leadership, the United States would win with dignity and honor.

## Endnotes

- <sup>1</sup> Richard Strozzi-Heckler, *In Search of the Warrior Spirit: Teaching Awareness Disciplines to the Green Berets* (Berkeley, Calif.: North Atlantic Books, 2003).
- <sup>2</sup> E-mail from Dr. Richard Strozzi-Heckler, CEO, Strozzi Institute, March 3, 2004.
- <sup>3</sup> *The 9/11 Commission Report* (New York: W. W. Norton & Company, 2004), pp. 363–364.
- <sup>4</sup> *Ibid.*, p. 376.
- <sup>5</sup> *Ibid.*, p. 377.
- <sup>6</sup> Robert D. Kaplan, “The Real Story of Fallujah: Why Isn’t the Administration Getting It Out?” *Wall Street Journal*, May 31, 2004 (online at <http://www.opinionjournal.com/editorial/feature.html?id=110005147>).
- <sup>7</sup> *9/11 Commission Report*, p. 403.
- <sup>8</sup> *Ibid.*
- <sup>9</sup> *Ibid.*, p. 418.
- <sup>10</sup> Morihei Ueshiba, founder of Aikido.

Lieutenant Colonel Fred T. Krawchuk, a U.S. Army Special Forces officer currently assigned to the U.S. Pacific Command, has led soldiers in a variety of infantry and special operations assignments in the United States, Europe and Latin America. A General MacArthur Leadership Award Winner and a graduate of the U.S. Military Academy and Harvard University, he served as an Olmsted Scholar in Spain and as an Army Senior Fellow with the U.S. Department of State.