JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY

Intelligence in Denied Areas

New Concepts for a Changing Security Environment

Russell D. Howard

Joint Special Operations University
357 Tully Street
Alison Building
Hurlburt Field, FL 32544

http://jsoupublic.socom.mil
https://jsou.socom.mil/gateway/

JSOU Report 07-10
December 2007

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intelligence in Denied Areas: New Concepts for a Changing Security Environment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Special Operations University,357 Tully Street,Alison Building,Hurlburt Field,FL,32544**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**58**	

Joint Special Operations University and the Strategic Studies Department

The Joint Special Operations University (JSOU) provides its publications to contribute toward expanding the body of knowledge about joint special operations. JSOU publications advance the insights and recommendations of national security professionals and the Special Operations Forces (SOF) students and leaders for consideration by the SOF community and defense leadership.

JSOU is a subordinate organization of the United States Special Operations Command (USSOCOM), MacDill Air Force Base, Florida. The JSOU mission is to educate SOF executive, senior, and intermediate leaders and selected other national and international security decision makers, both military and civilian, through teaching, outreach, and research in the science and art of joint special operations. JSOU provides education to the men and women of SOF and to those who enable the SOF mission in a joint environment.

JSOU conducts research through its Strategic Studies Department where effort centers upon the USSOCOM mission and these operational priorities:

- Preempting global terrorist and chemical, biological, radiological, nuclear, and explosive threats
- Enhancing homeland security
- Performing unconventional warfare and serving as a conventional force multiplier in conflict against state adversaries
- Conducting proactive stability operations
- Executing small-scale contingencies.

The Strategic Studies Department also provides teaching and curriculum support to Professional Military Education institutions—the staff colleges and war colleges. It advances SOF strategic influence by its interaction in academic, interagency, and United States military communities.

The JSOU portal is http://jsoupublic.socom.mil.

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY

Intelligence in Denied Areas

New Concepts for a Changing Security Environment

Russell D. Howard

JSOU Report 07-10
The JSOU Press
Hurlburt Field, Florida
2007

Comments about this publication are invited and should be forwarded to Director, Strategic Studies Department, Joint Special Operations University, 357 Tully Street, Alison Building, Hurlburt Field, Florida 32544. Copies of this publication may be obtained by calling JSOU at 850-884-2765; FAX 850-884-4732. Electronic versions of this and all JSOU Press publications can be found at https://jsou.socom.mil/gateway/highlights.aspx.

****

The Strategic Studies Department, JSOU is currently accepting written works relevant to special operations for potential publication. For more information please contact Mr. Jim Anderson, JSOU Director of Research, at 850-884-1569, DSN 579-1569, james.d.anderson@hurlburt.af.mil. Thank you for your interest in the JSOU Press.

****

ISBN 1-933749-21-0

The views expressed in this publication are entirely those of the author and do not necessarily reflect the views, policy or position of the U.S. Government, Department of Defense, United States Special Operations Command, or the Joint Special Operations University.

Recent Publications of the JSOU Press

Dividing Our Enemies, November 2005, Thomas H. Henriksen

The War on Terrorism, December 2005, James A. Bates

Coast Guard SOF, February 2006, Gary R. Bowen

Implications for Network-Centric Warfare, March 2006, Jessica Glicken Turnley

Narcoterrorism in Latin America, April 2006, Alvaro de Souza Pinheiro

The Changing Nature of Warfare, the Factors Mediating Future Conflict, and Implications for SOF, April 2006, John B. Alexander

Civil-Military Operations and Professional Military Education, May 2006, James F. Powers, Jr.

Blogs and Military Information Strategy, June 2006, James Kinniburgh and Dorothy Denning

2006 JSOU/NDIA SO/LIC Chapter Essays, June 2006

One Valley at a Time, August 2006, Adrian T. Bogart III

Special Operations Aviation in NATO, September 2006, Richard D. Newton

Beyond Draining the Swamp: Urban Development and Counterterrorism in Morocco, October 2006, Stephen R. Dalzell

Filling Special Operations Gaps with Civilian Expertise, December 2006, James F. Powers, Jr.

Educating for Strategic Thinking in the SOF Community, January 2007, Harry R. Yarger

The Israeli Approach to Irregular Warfare and Implications for the U.S., February 2007, Thomas H. Henriksen

Psychological Operations: Learning Is Not a Defense Science Project, March 2007, Curtis D. Boyd

2007 JSOU and NDIA SO/LIC Division Essays, April 2007

Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations, June 2007, Graham H. Turbiville, Jr.

Executive Report, JSOU Second Annual Symposium (30 April–3 May 2007)

A Theory of Special Operations, October 2007, Robert G. Spulak, Jr.

Block by Block: Civic Action in the Battle of Baghdad, November 2007, Adrian T. Bogart III

Private Security Infrastructure Abroad, November 2007, Graham H. Turbiville, Jr.

Contents

Foreword

Russell Howard's paper focuses on intelligence operations within denied areas and how these operations today differ from those of the Cold War period. Today, the preeminent threat is transnational, violent terrorist groups that operate under the cover of failed or weak states, as well as under the civil protections afforded in western liberal democracies. Howard focuses on the operational environments in failed or weak states as he discusses ways to improve intelligence targeting and collection in these challenging areas.

The congressionally mandated 9/11 Commission highlighted shortcomings in United States intelligence capabilities. In particular, the commission emphasized the need to refocus the intelligence community to overcome institutional biases toward technical intelligence collection. Howard's paper agrees with this assessment and provides four areas for consideration to improve our ability to operate against transnational terror networks.

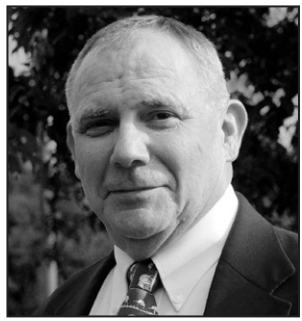
One area of consideration is using criminal networks to target terrorist networks. Howard makes a cogent argument that there is significant overlap between criminal and terrorist organizations. Targeting and manipulating criminals may significantly improve intelligence collection on terrorist activities. Traditionally, lawmakers have resisted using "tainted" intelligence sources, as evidenced by Congress' restrictions imposed in the 1990s on using sources with human rights violations. The reality is there is a nexus between criminal and terrorist networks and "wishing away" this linkage is not an appropriate policy—managing and taking advantage of the linkage is the right course of action.

Another theme that flows through this work is the importance of leveraging networks to target and collect on other networks. In the current conflict, the battle of the narrative is critical to winning and maintaining public support, and it is a pivotal element in the irregular warfare paradigm. Ethnic diasporas and nongovernment organizations (NGOs) are two powerful factors within the narrative battle and Howard is quite persuasive in his arguments for the need to better leverage these communities.

Intelligence targeting and operations may well be the decisive factor in winning the long war against radical terrorist networks. Most observers will readily agree that the United States intelligence community is not optimized for this fight and, although improvements have been made since 9/11, more needs to be done. Howard's treatise helps point the way, not only for the intelligence community, but for the SOF community in particular.

Michael C. McMahon, Lt Col, USAF
Director, JSOU Strategic Studies Department

About the Author



Brigadier General (Ret.) Howard is the founding director of the Jebsen Center for Counter Terrorism Studies at the Fletcher School and a JSOU senior fellow. Prior to assuming his current responsibilities, he was the Social Sciences Department chair and the founding director of the Combating Terrorism Center at West Point.

His previous Army positions include chief of staff fellow at the Center for International Affairs, Harvard University and commander of the 1st Special Forces Group (Airborne), Fort Lewis, Washington. Other recent assignments include assistant to the Special Representative to the Secretary General during United Nations Operations in Somalia (UNOSOM) II, deputy chief of staff for I Corps, and chief of staff and deputy commander for the Combined Joint Task Force, Haiti/Haitian Advisory Group. Previously, he was commander of 3d Battalion, 1st Special Warfare Training Group (Airborne) at Fort Bragg, North Carolina. He also served as the administrative assistant to Admiral Stansfield Turner and as a special assistant to the commander of SOUTHCOM.

As a newly commissioned officer, he served as an "A" team commander in the 7th Special Forces Group from 1970 to 1972. From 1972 to 1980, he served in the U.S. Army Reserve and was an overseas manager, American International Underwriters, Melbourne, Australia and China tour manager for Canadian Pacific Airlines. In 1980 he was recalled to active duty and served in Korea as an infantry company commander. Subsequent assignments included classified project officer, U.S. Army 1st Special Operations Command, at Fort Bragg, and operations officer and company commander, 1st Battalion, 1st Special Forces Group in Okinawa, Japan.

General Howard holds a B.S. in Industrial Management from San Jose State University and B.A. in Asian Studies from the University of Maryland. He also has two master's degrees: M.A. in International Management from the Monterey Institute of International Studies and MPA from Harvard University. He was an assistant professor of Social Sciences at the U.S. Military Academy and a senior service college fellow at the Fletcher School of Law and Diplomacy, Tufts University.

Introduction

The September 11, 2001 attacks and the ensuing American-led campaign against Al Qaeda and its affiliated movements marked the initial phase of what will no doubt be a long-term struggle against terrorism. The tasks facing the United States and other nations battling terrorism are extraordinarily difficult: future terrorist attacks must be prevented, terrorists must be denied the means to carry out attacks, and any plans to attack the U.S. and its allies must be preempted. None of these tasks can be achieved without accurate and timely intelligence—particularly human intelligence (HUMINT).

Unfortunately, and as outlined in a host of studies, panels, and committees, intelligence—and HUMINT in particular—was inadequate in predicting, preventing, or preempting the events of 9/11. This fact was clearly documented in the 9/11 Commission Report, which determined the U.S. intelligence community tried to solve the Al Qaeda problem with the capabilities it had used in the last stages of the Cold War and its immediate aftermath.[1] These capabilities, according to the Commission, were insufficient, yet little was done to expand or reform them. Finally, the 9/11 Commission concluded that the Central Intelligence Agency (CIA) and other intelligence organizations needed to wean themselves from an over-reliance on technical means of intelligence gathering and to markedly improve the quality of intelligence obtained from human agents.[2]

This paper agrees that technical intelligence methods that worked well in a Cold War environment, such as imagery intelligence (IMINT) or signal intelligence (SIGINT), have not proven effective against terrorists, and it posits that increased HUMINT capabilities will be crucial in waging an effective campaign against Al Qaeda and like-minded terrorist groups. More specifically, this paper addresses the difficulty in gleaning HUMINT from denied areas and offers unconventional alternatives that may better fit the post-Cold War security environment.

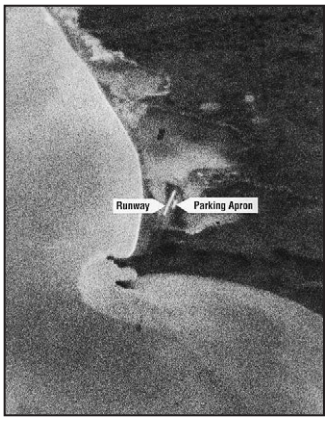
… increased HUMINT capabilities will be crucial in waging an effective campaign against al Qaeda and like-minded terrorist groups.

Background

Many in addition to those who prepared the 9/11 Commission Report have been critical of the CIA and other U.S. intelligence organizations for adhering to Cold War methodologies in the face of post-Cold War threats. Thorough examination of these intelligence shortcomings has been the topic of numerous reports, panels, and articles. However, missing from these critiques is much in the way of out-of-the-box thinking on ways to gather HUMINT in difficult-to-access or *denied areas*.

To "Cold Warrior" intelligence professionals, denied areas referred to the vast territories behind the Iron and Bamboo Curtains. In today's parlance, denied areas describe regions whose nations are characterized by weak state structures, including sub-Saharan and Eastern Africa, the former Soviet bloc (particularly the newly independent states in Central Asia), and several quasi-states such as Nagorno-Karabakh in Azerbaijan and Abkhazia and Ossetia in Georgia.[3]

During the Cold War, access to areas behind the "curtains" was difficult, particularly for HUMINT gatherers—known as spies in common language. To overcome these difficulties, U.S. intelligence organizations developed technical means that allowed collectors to look behind and inside denied areas. For example, more than forty-six years ago, a top-secret U.S. spy satellite code-named CORONA captured a series of grainy, black-and-white photographs of selected missile sites in the Soviet Union and became the first reliable *technical intelligence* system to penetrate the Iron Curtain. This "difficult, high-risk mission… brought back the world's first pictures from space and, according to the men who worked on it, helped preserve the peace between two Cold War superpowers."[4] In one day, "CORONA yielded more images of the Soviet Union than did the entire U-2 spy plane program," proving that the USSR's missile stockpile was much more meager than had been anticipated—somewhere between 25 and



First imagery taken by CORONA: Mys Shmidta Air Field, USSR (on the north coast of Siberia) 18 Aug 1960. Photo National Reconnaissance Office.

50 units, rather than hundreds.[5] The early CORONA systems ejected film canisters that parachuted to earth and were "snatched" by aircraft before the canisters landed. Later systems with intriguing names such as Argon, Lanyard, Gambit, Big Bird, Dorian, and Crystal had digital imaging systems and downloaded and forwarded images to operators and analysts via radio links giving both near real-time data.

Unfortunately, the intelligence community still relies mostly on the same collection paradigm created for denied areas during the Cold War. Clearly, remote technical collection was an appropriate means of obtaining critical intelligence from the Soviet Union, a bureaucratized, centralized, and rigid superpower adversary that exhibited strongly patterned behavior. However, the problem presented by many of the new threats—particularly transnational terrorist groups, which operate in the shadows of failed and failing states—is much more ambiguous and difficult to detect. Technical assets do little to overcome the difficulty of monitoring the activities of a dispersed network of multiple, secretive Al Qaeda-like terrorist organizations and operational cells that operate around the globe.[6] As one scholar states, terrorist cells "come and go, moving and morphing so rapidly as to render detection of their activities by hierarchically bound Western intelligence organizations highly problematic."[7] The diffuse, networked structure of Al Qaeda, unlike the hierarchical state structure of the Soviet Union, does not operate from large, easily identifiable bases and does not depend on extensive traditional communications techniques. Furthermore, unlike the Soviet and other conventional armies, Al Qaeda does not conduct large-scale repetitive exercises that are easily monitored with technical-intelligence assets. The visible signature of terrorists is much smaller than that of the former Soviet Union or any nation-state. Finally, technical collection assets do little to penetrate *denied minds*—not just those of a few recognized leaders, but of terrorist groups, social networks, and entire cultures for which there is little understanding in the West.[8]

Complicating the technical collection problem is the fact that Al Qaeda and its affiliated groups are transnational, non-state actors that often operate in ungoverned areas in failed and failing states. The CIA estimates that there are fifty ungoverned zones where terrorist groups take advantage of states that cannot control their "borders and boundaries."[9] Indeed, weakened central authority and state structure are common in many parts of the world, even in remote regions of

countries that are U.S. allies, such as Pakistan. As Daniel Byman notes, "Afghanistan, Mauritania, Pakistan, Somalia, Tajikistan, and Yemen are only a few of the countries where the government's writ is limited to the capital and other major cities."[10]

Clearly, technical intelligence is still an important capability in the campaign against terrorism and in confronting more traditional threats. For example, the worldwide network to intercept messages and to carry out other forms of signals intelligence (SIGINT) operated by the National Security Administration (NSA) is important, even though Al Qaeda operatives have become more sophisticated in avoiding listening and tracking capabilities. Also, unmanned aerial vehicles (UAVs) such as the Predator have been successful in identifying and attacking terrorist targets. Furthermore, despite being less successful in tracking non-state actors and terrorist groups, technical intelligence assets can be vitally important in monitoring rogue states such as North Korea and Iran. However, the technical assets used in tracking the activities of these two "axis of evil" countries, which still retain traditional state structures, are much less useful in monitoring the activities, capabilities and intentions of transnational non-state actors such as Al Qaeda. These terrorist organizations represent a new challenge to intelligence agencies: a small, well-trained, networked enemy that calculates, plans, and operates unchallenged from the ungoverned areas of failed and failing states.

Ungoverned Areas: Failed and Failing States

Prior to 9/11, U. S. security analysts viewed failed and failing states as humanitarian problems; they "piqued the moral conscience but possessed little strategic significance."[11] Al Qaeda's ability to act with impunity from Afghanistan changed this calculus, convincing the Bush administration that "America is now threatened less by conquering states than we are by failing ones."[12]

Failed states are characterized by a failed economic infrastructure, nonexistent or declining health and education systems, declining per capita GDP, soaring inflation, rampant corruption, and food and transportation shortages—the perfect breeding ground for Al Qaeda organizers and recruiters.[13] These so-called weak states appeal to Al Qaeda and other transnational, non-state terrorist groups for the many benefits they offer: safe havens, conflict (combat) experience,

settings for training and indoctrination, access to weapons and equipment, financial resources, staging grounds and transit zones, targets for operations, pools of recruits, and—perhaps most appealing to Al Qaeda—limited opportunities for the collection of technical intelligence and HUMINT by U.S. forces.[14] Failing states' problems mirror those of failed states, but at lesser levels of decline.

The threats posed by the ungoverned areas in failed and failing states have been exacerbated by the empowerment of non-state actors such as Al Qaeda and other terrorist groups who have access to modern technologies, including both highly destructive weapons and sophisticated communications and information systems.[15] This empowerment of individuals and small groups has combined with the inability of failed states to control such groups operating and recruiting disaffected elements to terrorist causes within their borders. "The ease of travel and communication in the closely integrated world enables terrorist groups to increasingly act globally."[16] The U.S. and other major powers are now vulnerable to attacks planned and executed from areas that are not only thousands of miles away from the target, but also from the terrorists' native countries, as was the case with Al Qaeda's 9/11 planning operations in Afghanistan.

This paper explores four different—and arguably controversial—means of gaining intelligence in ungoverned areas of failed and failing states—the post Cold-War denied areas. Presented in four sections, this paper elaborates on different groups that have the ability to gather intelligence on terrorists—particularly Al Qaeda—in areas where traditional intelligence collectors have difficulty operating.

1. The first section describes how criminals and criminal cartels could be used as intelligence gatherers—a controversial but historically not-unheard-of source.
2. The second section explains how ethnic diasporas could be leveraged to gain intelligence.
3. The third section evaluates the possibility of non-governmental organizations cooperating with intelligence services for mutually beneficial reasons.
4. Finally, the fourth section reexamines the *SOF for Life* program, a discarded concept that has unique intelligence collection possibilities.

1. The Enemy of My Enemy Is My Friend

This section advances the notion that criminals—particularly drug, arms, and human traffickers—could be a useful source of information and possibly actionable intelligence in the campaign against terrorism. This notion is timely because of a decision lifting restrictions imposed in 1995, which limited the opportunity for intelligence services to recruit informants who may have run afoul of human rights laws.[17] In theory, these guidelines were designed to protect U.S. intelligence services. However, in practice the guidelines discouraged the recruiting of potentially useful informants, thus hindering collection efforts.

It is unfortunate but necessary that intelligence operators must seek information from former terrorists and other criminals—people who most probably possess questionable human rights records. Such collaboration is all but inevitable in the process of obtaining specialized information, because these sources often operate in areas where U.S. intelligence professionals cannot easily establish a presence. As Cilluffo et al. state:

> The intelligence community must deal with individuals who are unsavory and dangerous. Interaction with them does not imply approbation of their previous actions, but recognizes that the potential knowledge—information that can save the lives of U.S. citizens—outweighs the disagreeable background of these sources.[18]

Seeking the cooperation of unsavory elements in time of war is nothing new.

Seeking the cooperation of unsavory elements in time of war is nothing new. Many credit Lucky Luciano, a Mafia kingpin, for aiding Naval Intelligence during World War II. In return for reduction in his prison sentence in 1942, it is often speculated that Luciano made a deal with the U.S. government to secure New York's docks from Nazi or Fascist sabotage and to provide human intelligence (HUMINT) that would be used during the invasion of Sicily. Interestingly, in July 1943, possibly because of Luciano's connections and influence, Italian troops did not fire a single shot at the invading Americans in Sicily.[19]

Just as the Mafia was used as an intelligence source because of its specialized knowledge and familiarity with the enemy, I argue that

criminals should be leveraged today for intelligence purposes in the fight against terrorism. Increasingly, and most certainly since the end of the Cold War, transnational terrorist and criminal organizations activities are linked through symbiotic activities and mutually beneficial arrangements. These linkages mean that it is possible for criminal syndicates and other illegal operators to provide valuable and actionable information about terrorist networks and operatives.

The Connection

International organized crime groups and terrorist networks such as Al Qaeda have much in common. They are both engaged in illicit activity and use many of the same methods and tactics in the pursuit of their goals: violence, fear, and corruption, are but a few. Also, the geographic scope of both transnational organized criminal syndicates and terrorist networks are global—a phenomenon resulting in the post-1990s security environment.[20]

There are also significant differences between organized criminals and terrorists. A terrorist is fundamentally an altruist: he believes he is serving a good cause designed to achieve a greater benefit for a wider constituency, whereas the criminal, by and large, serves no cause other than his own personal aggrandizement and wealth.[21] Also, the groups' main targets of violence are different. Criminals use violence against other organs of force, such as the police and competing criminal elements, while terrorists predominantly direct their violence against unarmed civilians.[22] Further, while the crimes committed by these two groups—drugs, human trafficking, arms sales, counterfeiting, corruption, and more—do not differ in substance, they differ in motive. For terrorists, revenue-generating criminal activity is a means to support larger political and ideological objectives. For criminals, criminal activity in itself is their business. Bruce Hoffman explains it best:

> Perhaps most fundamentally, the criminal is not concerned with influencing or affecting public opinion: he simply wants to abscond with his money or accomplish his mercenary task in the quickest and easiest way possible so that he may reap his reward and enjoy the fruits of his labors. By contrast, the fundamental aim of the terrorist's violence is ultimately

> to change "the system"—about which the ordinary criminal, of course, couldn't care less.[23]

Terrorist groups and organized criminal elements maintain various relationships for a number of mostly self-serving reasons. Drug trafficking, the smuggling of consumer goods, and extortion are important sources of income for both types of groups.[24] Also, organized crime plays a central role in terrorists' arms supply—from traditional small arms to weapons of mass destruction. For example, the Al Qaeda network has sought fissile materials through criminal elements and has explored the possibility of buying an intact nuclear weapon.[25] In order to gain access to "strategic nuclear goods," terrorists must link up with a subset of people who are willing to commit illegal or disloyal acts. The obvious candidates are members of criminal organizations—specifically those which have connections inside nuclear enterprises and cross-border smuggling experience.[26] In several known cases, "Al Qaeda reportedly negotiated with the Chechen 'mafiya' [sic] to buy tactical nukes and with Russian crime figures in Europe to obtain the makings of a radiological (dirty) bomb."[27]

The relationships between terrorists and criminal cartels vary, but they are most often marriages of convenience, used to gain expert knowledge (such as tactics or networks for activities such as money-laundering, counterfeiting, or bomb-making) or operational support (access to smuggling and transit routes, for example). Such a mutually beneficial arrangement is embodied in the relationships between criminal groups specializing in drug trafficking and terrorist groups. Since drug traffickers and terrorists operate in a clandestine environment, both groups utilize similar methodologies to function, says a 2005 Drug Enforcement Agency (DEA) report. Interestingly, drug trafficking is now the major source of profits for both international organized crime groups and terrorist networks.[28] Furthermore, both groups, says the DEA report, "…lend themselves to facilitation and are among the essential elements that may contribute to the successful conclusion of a catastrophic event by terrorists."[29] Drug traffickers and terrorists also use the same transit routes in pursuit of their activities. For example, the 2005 DEA report outlines an ongoing operation in which multiple Middle Eastern drug-trafficking and terrorist cells operating in the U.S. fund terror networks overseas, aided by established Mexican cartels with highly sophisticated trafficking routes.[30]

Human traffickers also serve terrorist interests. Trafficking in persons can mask the movement of members of terrorist groups. For example, the movement of Afghans and Pakistanis has been used as a cover for the transit of at least one Al Qaeda operative.[31] Also, profits from the trade in human beings are used to fund terrorist activities.[32] Terrorists and human and drug traffickers often use the same document forgers, particularly in Qatar and Bangkok.[33] Fake travel documents are easily obtained—albeit often for a steep price—at several shops in Bangkok's gritty Lard Prao district, which according to trafficking experts is a regional hub for forging passports and visas.[34] In fact, while doing research in Bangkok for a project linking human traffickers with terrorists, this author was told that for $4,000 he could change his identity in the Nara District of Bangkok—an offer that is surely also extended to terrorist groups and other nefarious individuals who use this busy city as a transit hub.[35]

The connections between terrorist networks and organized criminal syndicates are many and varied. Their operations are similar even if their motives differ. Hard-core terrorists who are ideologically driven are difficult to "break," as reports from Guantanamo and other detention centers indicate. By contrast, criminals with special knowledge of terrorist activity may not be as hard to break. Their interests are not ideological or focused on a higher calling; rather, they are personal, self-serving, based on survival, and should be exploited for the benefit of intelligence and counterterrorism operations.

Supporting Factors

The U.S. State Department's Bureau of Diplomatic Security runs a *Rewards for Justice Program* for the Department of Justice. The program, which offers rewards for tips leading to the capture of terrorists, was originally promulgated in 1986 and enhanced after 9/11.[36] For their efforts, informants, whose identities are kept secret, can receive up to $5 million for tips that lead to the capture—or death—of most-wanted terrorists. Indeed, the State Department has paid out nearly $48 million to nineteen different people since September 11, 2001, with payments between $300,000 and $1 million being the norm.[37] Although its success with Al Qaeda targets has been limited, the reward program has helped to net some key fugitives, particularly in Iraq. According to U.S. officials, five of Saddam Hussein's henchmen

were nabbed with the help of informants motivated by the promise of cash.[38] In fact, Hussein's sons, Uday and Qusay, were found and killed nineteen days after rewards of $15 million were offered for their capture. Rumored to be a cousin of the slain brothers, the informant was paid $30 million and has left Iraq, his identity never revealed.[39]

In recent months, three terrorist plots in the U.S. have been foiled by informants. In June 2006, an informant posing as an Al Qaeda operative helped bring down a plot to blow up the Sears Tower in Chicago, and in May 2007 an informant infiltrated a group of Muslim extremists plotting to attack soldiers at Fort Dix, New Jersey. And, most recently, an informant helped stop a plot by Muslim extremists to bomb the jet fuel pipeline that supplies the JFK Airport. The informant, a twice-convicted drug dealer who found himself in the midst of what investigators called a terrorist plot "conceived as more devastating than the Sept. 11 attacks" was so convincing that the suspects gave him unfettered access to their operation.[40]

In recent months, three terrorist plots in the U.S. have been foiled by informants.

Despite their often selfish and perhaps insidious reasons for cooperating, it seems that a policy of using informants—even criminals—works and should be exploited to its fullest extent. Criminals who have worked either with or in close proximity to terrorists should be priority informant candidates.

Case Study

International arms dealer Monzer Kassar of Marbella, Spain was arrested on June 9, 2007 in Madrid for conspiring to sell millions of dollars worth of weapons to the Fuerzas Armadas Revolucionarias de Colombia (FARC)—a designated foreign terrorist organization—to be used to kill Americans in Colombia.[41] Between February 2006 and May 2007, Kassar and two associates agreed to sell to the FARC millions of dollars worth of weapons, including thousands of machine guns, millions of rounds of ammunition, rocket-propelled grenade launchers (RPGs), and surface-to-air missile systems (SAMs). During a series of recorded telephone calls, emails, and in-person meetings, Kassar and his associates (who were also charged) agreed to sell the weapons to two men who claimed they were acquiring these weapons for the FARC with the specific purpose of using them to attack U.S. helicopters in

Colombia.[42] The buyers were actually confidential sources working with the Drug Enforcement Agency (DEA).

Also known as Abu Munawar and *El Taous*, Kassar has been accused of a variety of crimes, including drug trafficking, illegal arms deals, and terrorism.[43] Recently, he was named by the Iraqi government as one of its most wanted men.[44] A United Nations report called him an "international embargo buster." John Kerry, the Democratic presidential candidate in 2004, has called him a "vile terrorist."[45]

Since the early 1970s, Kassar has been a ready source of weapons and military equipment for armed factions engaged in violent conflicts around the world. He has provided weapons and military equipment to factions in Nicaragua, Brazil, Cyprus, Bosnia, Croatia, Somalia, Iran, and Iraq, among other hot spots. Some of these factions have included known terrorist organizations, such as the Palestinian Liberation Front (PLF), the goals of which included attacking United States interests and U.S. nationals. In 1992, Kassar was arrested in Spain on charges of piracy and providing the arms to the Abu Abbas-led PLF terrorists who hijacked the Achille Lauro cruise ship and murdered American Leon Klinghoffer. Western intelligence agencies determined that Kassar flew Abbas to safety aboard one of his private planes after the hijackers surrendered.[46] Kassar was acquitted of all charges related to the Achille Lauro ordeal when tried in a Spanish court because most of those who agreed to testify against him either died mysteriously or failed to show up in court.[47] In addition to Abu Abbas, Kasser has been connected to known terrorists Abu Nidal, Georges Habbash, and Farah and Hassan Aideed.[48]

Syrian-born arms dealer Monzer Al Kassar (L) escorted by Spanish police at his house in Marbella, southern Spain, June 8, 2007. REUTERS/Jon Nazca, used by permission from Newscom.

To carry out his weapons trafficking and other illegal businesses, Kassar developed an international network of criminal associates as

well as front companies and bank accounts in various countries, including the United Kingdom, Spain, Syria, Iraq, Poland, Bulgaria, and Romania. Additionally, Kassar has engaged in money-laundering transactions in bank accounts throughout the world to disguise the illicit nature of his criminal proceeds.[49]

The indictment against Kassar and two accomplices, Tareq Mousa Ghazi and Luis Felipe Moreno Gody, charges them with four separate terrorism offenses: "… conspiracy to kill U.S. nationals, conspiracy to kill U.S. officers or employees, conspiracy to provide material support or resources to designated foreign terrorist organization, and conspiracy to acquired and use an antiaircraft missile."[50] Additionally, Kassar and Moreno were charged with money-laundering. If convicted of all counts, the men face a sentence of life in prison without parole.[51]

Given Kassar's history and lavish lifestyle (a fifteen-suite residence designed like a Renaissance palazzo, where there is a swimming pool built in the shape of a four-leaf clover), one might surmise that Kassar would be good informant material. If half of the allegations about his associations are true, one can imagine the intelligence "treasure trove" that might develop from information given by Kassar in exchange for a reduced sentence. For his help during World War II, Luciano's thirty-to-fifty year sentence (for which he served ten years) was commuted, and he was deported to Italy. At the age of sixty-one, Kassar still has some time left to live a normal life; my guess is that he would prefer to live it somewhere other than prison.

Recommendation

My recommendation is that Kassar and those criminals like him who have special knowledge because of the nexus between transnational terrorist and criminal organizations, be leveraged for intelligence information in the global war on terror. Kassar's case is at least the fifth time in two years in which the U.S. government has relied on paid informants to bring terrorism related charges against U.S.-based Muslims.[52] These charges have resulted in four convictions and I believe more terrorist plots could be uncovered and convictions rendered by increasing efforts to co-opt criminal elements knowledgeable of terrorist activities.[53] Despite the various issues that might be raised by collaborating with established criminals, the potential to obtain actionable intelligence from them is an opportunity too great to pass

up. The developing nexus between criminal and terrorist activity—and the subsequent increased access to terrorist networks by criminal groups—make members of organized criminal syndicates ideal targets for intelligence-gathering operations.

2. Leveraging Diasporas

According to the Merriam-Webster Dictionary, a diaspora refers to "the movement, migration, or scattering of a people away from an established or ancestral homeland."[54] Originally, the term was exclusively applied to the Jewish Diaspora,[55] but it is now used to describe the global distribution of various ethnic and cultural groups, including the African, Chinese, and Irish expatriate communities.

For the purpose of this study, I define diaspora as a people dispersed from their original homeland who possess a collective memory and myth about a sentimental and/or material link to that homeland, and who also have a sense of sympathy and solidarity with those in their ancestral homeland. My definition implies that a member of a diaspora who has never lived in the ancestral homeland can have as great a sense of obligation to support the homeland as someone who was born there.

Ethnic diasporas are not a new phenomenon. According to Robin Cohen, "Diasporas as a social form have pre-dated the nation state, lived uneasily within it, and now, in specific respects, transcend and exceed it."[56] While diasporas have likely existed before the Westphalian state system was established in the mid-seventeenth century, in recent decades, advances in transportation and communications have increased the size, visibility, and impact of diasporas. As one scholar notes, "Diaspora networks have become important facilitators of internal, inter-state, and worldwide political, cultural and economic connections and may be the precursors of post-modern, trans-state social and political systems."[57]

Leveraging Diasporas: The Traditional View

Since the tragic terrorist attacks on September 11, 2001, scholars and policy makers have increasingly observed the ability of terrorist groups to leverage diasporas. Indeed, there has been a "veritable explosion" in the number of public, media, and policy statements about the potential links between expatriate ethnic groups and national security challenges—with good reason.[58]

Terrorist organizations such as Hezbollah and Al Qaeda use diasporas to provide a cover for their operations. Sometimes members of

these diasporas overtly sympathize with the terrorists or are economic beneficiaries of their illicit activities. Other times, the diaspora community is not complicit in terrorist operations; its members merely provide shelter or support, perhaps unwittingly, to members of a terrorist network.[59] Although most of the September 11 terrorists were Saudi citizens who entered the U.S. legally and were recruited and trained in Afghanistan, they were supported by Arab expatriate communities in Germany, the United Kingdom, France, and elsewhere. Other failed Al Qaeda operations took advantage of locally-recruited sympathizers and were supported by expatriate cells in such places as Canada and the Philippines.[60]

Certainly many diasporas in the U.S. and Europe "require watching"—particularly those that might fall victim to Al Qaeda's theoretical indoctrination and ideology.[61] Says John Sullivan of the Los Angeles Sheriff's Department, "… diaspora communities can provide extremists with a permissive environment that can favor conditions that enable the emergence of extremist cells."[62] Radical enclaves can emerge within diasporas and serve as catalysts for further radicalization. When communities are linked through social networks and online media to lawless zones in failed states, radical enclaves, and denied areas, a powerful *networked diaspora* can result.[63]

An example of this type of networked diaspora can be observed in the United Kingdom. According to Sullivan, the UK is currently the vanguard of violent jihadism in Western Europe. Extreme Islamist sects are active in British cities, and their members—separate and in concert—concoct viable rationales that legitimize extremist narratives and threatening actions.[64] Sullivan believes the threat is certain to continue beyond the attempted and successful bombings of central London cars and public transportation in recent years. As reflected in the statements of British Islamist extremist Anjem Choudary, "There is no doubt whatsoever that there will continue to be attacks against the British government … there are many in Britain who take their ideology from Osama bin Laden and Al Qaeda and are ready to carry out many more attacks."[65] Ultimately, says Sullivan, this threat, if unchecked, will mature in the United States and elsewhere.[66]

The notion that a diaspora might be used for intelligence gathering purposes is not new or novel. However, most of the existing research has been focused on diasporas working for terrorists—not counterterrorists. For example, terrorist organizations such as Hezbollah

and the Liberation Tigers of Tamil Elam (LTTE) understand how to leverage diasporas.

Hezbollah has used the Lebanese Shi'a diaspora to gather intelligence abroad, including information that has helped the terrorist organization launch attacks on overseas Israeli targets.[67] Hezbollah has expanded its operations from Lebanon to the wider Middle East and other regions. According to James Phillips, Hezhollah "… now is truly a global terrorist threat that draws financial and logistical support from the Lebanese Shiite Diaspora in the Middle East, Europe, Africa, Southeast Asia, North America, and South America."[68]

Another case study is the Tamil diaspora, which has played an important role in supporting the Tamil insurgency in Sri Lanka in its struggle to carve out an independent Tamil homeland. The Tamil diaspora numbers between 700,000 and 800,000, and its members are settled across North America and Europe.[69] This community has provided crucial support to the LTTE, the most active Tamil terrorist organization—in particular, by providing its primary financial backing. LTTE funds come from countries hosting large Tamil diaspora communities, including Switzerland, Canada, Australia, the UK, the U.S., and Scandinavian countries.[70] Additionally, apart from the utility of the Tamil diaspora in raising funds and producing intelligence, its members also generate political and diplomatic support and help in weapons procurement.[71]

Leveraging Diasporas: A Proactive View

Sullivan's findings about the danger of diasporas supporting Al Qaeda and other terrorists in the UK and U.S. are most certainly true, and the Hezbollah and LTTE case studies are only two of many examples describing how terrorists are supported by diasporas. However, this paper advocates that diasporas can be positively leveraged in the fight against terrorism. I argue that diasporas, both in the United States and abroad, can be sources of intelligence in the campaign against terrorism. The growing use of the Internet and modern communications, the ease of international travel, and other globalization functionalities increase opportunities for globally distributed ethnic diasporas to play key intelligence roles in counterterrorism campaigns involving their home state or adopted territory.[72]

To clarify my arguments, diasporas will be viewed in two different contexts (locations). First, diasporas originating from failed states and denied areas—primarily Muslim diasporas (for example, Somalia)—will be viewed as sources of intelligence about activity both within the diaspora's ancestral land and within the expatriate diaspora community within resettlement countries such as the U.S. Second, diasporas composed primarily of economic immigrants, such as the varied Chinese communities, will be discussed as a possible domestic source of intelligence for U.S. agencies. Diasporas are commonly used as sources of information by the governments of their adopted or native countries. However, it is rarer and therefore more innovative for a third-party government to leverage global diasporas.

Leveraging Diasporas Resident in the United States

According to migration scholar Rex Brynen, "Many of the chief tools of effective counterterrorism and counterintelligence are remarkably similar to those of good community policing."[73] Diaspora networks in the U.S. are particularly well equipped to detect within their neighborhoods potential terrorist activities that are detrimental to their adopted country. However, this information is useless if it remains locked inside a close-knit community.[74] Therefore, it is imperative that security and intelligence agencies work to develop relations of trust and transparency with diaspora communities.

Recruitment from all diasporas—but particularly from various ethnic Muslim diasporas—into U.S. military, intelligence, and law enforcement agencies should be a major policy goal for two important reasons. First, those with diaspora ties who are recruited into domestic law enforcement agencies are well equipped to identify Islamist jihadi infiltrators within diaspora communities. Second, recruitment of Americans with various ethnic backgrounds into the military—particularly the Army, Marines, and Special Operations Forces—could be great value-added in the campaign against terrorism, particularly when these recruits are deployed. Organizations charged with domestic and external security need to take advantage of the ethnic diversity in diaspora populations and leverage diasporas for the linguistic and cultural skills they make readily available.

In addition to the contributions previously mentioned, diaspora recruitment has the potential to be particularly useful to intelligence

services trying to glean information from denied areas. For example, one important benefit of diaspora recruitment is member knowledge of and contacts in the country of ethnic origin. If recruits hail from failed states and denied areas where normal sources of intelligence are not readily available, this information can be invaluable.[75] Many individuals residing outside of their country of origin, regardless if they left voluntarily or involuntarily, are able to answer questions about the geography, culture, and social infrastructure of their former homeland. According to Brian Auten, "They can interpret the nuances, infighting and splintering of their home country's political landscape."[76]

Furthermore, it is unusual for communications to completely sever even for those from so-called denied areas such as Somalia. For example, even though Somalia has no formal banking system, Somali diasporas in the U.S. and United Kingdom repatriate more than $700 million a year to their homeland through the hawala banking system.[77] In fact, it is estimated that nearly twenty-three percent of Somalia's total income is sent there by Somalis living abroad.[78]

In addition to financial information, when communication is possible, personal ties can be used as a conduit for continued information gathering among diaspora networks. It is a communication medium, says Auten, "…that can double as a conduit for receiving information on current (and possibly future) happenings within the home country."[79] Important for intelligence organizations, this conduit can also be used for recruiting and running agent networks back in the home country, particularly where the diaspora's country of origin is so ethnically or culturally dissimilar to preclude the use of the U.S. government's normal intelligence assets.[80]

Again, the United Kingdom serves as an interesting case study of diaspora activity, this time in the recruitment of Muslims from various ethnic diasporas into law enforcement and military service. After the July 2005 London subway bombings, recruitment of police officers from within the Muslim diaspora increased dramatically. Presently, there are 300 Muslims in the London Metropolitan Police Constabulary and 3,000 nationally, with another 6,000 community officers to be added.[81] Interestingly, this recruitment of the Muslim community does not extend to the UK military services, where, according to one member of Parliament, "there is a particular problem relating to the Muslim community, because the levels of recruitment of members of

that community to the three services are almost statistically insignificant."[82]

In the U.S., several security and military service organizations are recruiting aggressively in diaspora communities (particularly those with predominantly Muslim backgrounds), also with mixed results. Faced with a shortage of "personnel who speak Arabic and understand Islam, the U.S. military is quietly courting American Muslims."[83] The Marines are perhaps the most proactive and far-sighted. Recognizing that deployed forces often serve as the main face of the U.S. abroad, the Marines have established an outreach and recruiting program for Muslim communities within the United States. The program is a mechanism for increasing the diversity of the force in order to better represent the backgrounds and skills of the U.S. population to foreign audiences.[84] However, members of most Muslim diasporas show little enthusiasm for joining these organizations that many say are prejudiced against them.[85] Says Ibrahim Hooper of the Council of American-Islamic Relations (CAIR), "The military have the same problem as civilian government agencies, such as the FBI. There is a general reluctance to join because Muslims think there is bias against them and career prospects are limited."[86]

This perception is unfortunate, because many benefits could accrue from diaspora recruiting within the U.S. military, intelligence, and law enforcement communities. The superior cultural and contextual knowledge possessed by diasporas is an untapped resource that the U.S. and other countries have not yet fully leveraged.

Leveraging Third-Party Diasporas

To my knowledge, leveraging the diasporas living in countries not of their native homeland for U.S. intelligence purposes is a relatively new and perhaps novel concept. For my example, I use the Chinese diaspora (though the Indian diaspora would also be a good example to study). Notionally, one could expect that Chinese living overseas would pass intelligence on to their home country, and as we have learned from bad experiences in the U.S., they sometimes do. However, one might not expect that the Chinese diaspora might be useful for U.S. intelligence collection.

I have chosen to highlight the Chinese diaspora for four reasons. First, Chinese diasporas are located worldwide, and resident in virtu-

ally every country. Second, Chinese have lived outside their homeland for generations. Third, I speak Chinese and have experience with intelligence operations in the region. Fourth, and most important, members of the overseas Chinese community are entrepreneurs. They make their living through business and commerce. The notion of a Caliphate—a Muslim state governed by Sharia Law, which is the goal of Al Qaeda and unfriendly to business—goes against everything most Chinese diasporas live for. Therefore, there is no interest in Al Qaeda or its ideology within the Chinese diaspora community which could be a beneficial circumstance for the U.S. intelligence community.

Generally referred to as *overseas Chinese*, the Chinese diaspora is an instructive case study in capitalism and entrepreneurship. Overseas Chinese number between thirty five and fifty million people and are resident in 150 countries worldwide.[87] As an economic bloc, overseas Chinese constitute the third largest economy in the world— thought to possess $1.5 to $2 trillion in liquid assets—and has been the main investment engine in China's massive and continuous growth for the past three decades.[88]

The Chinese people have a long history of migrating overseas. The earliest migration dates from the Ming Dynasty (1368-1644), when Chinese were sent to the South China Sea and Indian Ocean to develop commerce. Several waves of migration have occurred since, most notably in the nineteenth century, when surplus Chinese laborers filled the labor shortage gap in colonial empires and the industrializing West. A third major migration wave was the result of twentieth century political turmoil and later the competition between the mainland (Communist China) and Taiwan (Nationalist China).[89] A fourth and much smaller wave began after the so-called Cultural Revolution in China at the end of the 1970s and continues today. In the late 1970s, when Deng Xiaoping ("to get rich is glorious") ruled the People's Republic of China (PRC), political and military intelligence services received special funding to start hundreds of so-called "private" firms and companies in Third World countries. By a special decree of the Politburo, the Chinese intelligence services organized trading companies, manufacturing industries, banks, and other enterprises designed to look like very attractive business partners without any real connections to the Communist regime. In the mid-1980s, hundreds of these companies were created, usually headed by persons with strong family connections with the Communist Party and the PRC government.[90]

American intelligence organizations should not bother to look for assistance among first-generation immigrants who were sent by the PRC to engage in mercantile and espionage activities. Even if they might cooperate, they generally have fewer connections, and less access to information. Rather, U.S. intelligence services should try to develop contacts among second-, third-, and fourth-generation immigrants who have largely become part of the local and historical fabric of the area in which they and their families have settled. They have had a chance to do business, to take part in political and social life, and to work inside the system, and they possibly have access to valuable domestic information. Importantly, the vast majority of these Overseas Chinese descendants of immigrants are not susceptible to working with the Chinese intelligence services. More than likely, these long-term residents would be more responsive to monetary compensation.[91]

Conclusion

American diplomatic, intelligence, and defense policy makers will to have to consider the potential impact ethnic diasporas can have on regional conflict in the next ten to twenty years as they become more involved in supporting the security postures and campaigns of their home territories and adopted states.[92]

This paper has presented two of ways of leveraging diasporas in the campaign against terrorism. The first example was a traditional approach of leveraging diasporas in the U.S. who have special knowledge of the language, culture, religion, and personalities of foreign lands which may be harboring those who might want to harm us. Domestically, they know the "street" and can sense when homegrown terrorists might be in their midst, in ways that most law enforcement and intelligence officials will not. The challenge with these diasporas is gaining their confidence to the degree that they will report untoward behavior. Getting them to join the ranks of law enforcement, intelligence agencies, and the military is another challenge worth pursuing. Their special knowledge would be useful to these organizations in the U.S. and in far-off places such as the Horn of Africa, Afghanistan, Somalia, Iraq, and other deployment spots where the U.S engages the forces of terror.

The second, not-so-traditional example focused on leveraging third-country diasporas living abroad, the hypothesis being that they would

rather help the U.S. intelligence apparatus than watch an Al Qaeda-inspired Caliphate undermine their entrepreneurial endeavors. The Chinese diaspora was case study used for the second example, but it could have just as easily been the Indian, Korean, or Philippine diasporas, which are also entrepreneurial and live and work in failed states and denied areas at risk. Early knowledge of Al Qaeda and other terrorist activities in these areas could enable the U.S. to prevent a future Afghanistan or, worse yet, an Al Qaeda-led state.

3. A Marriage of Convenience

NGOs and U.S. Intelligence Agency Cooperation

Special Forces Field Manual (FM) 3-05.102 (formerly FM 34-36, Army Special Operations Forces and Intelligence) stipulates in Annex A that there may be situations where intelligence should be shared with non-governmental organizations (NGOs) "outside usual political military channels," but does not clarify or elaborate on the statement.[93] This lack of further detail is regrettable, because NGOs could be an important partner in securing vital intelligence information, particularly in denied areas. These organizations and their staff would be especially useful as information sources in areas where technical intelligence gathering is not effective and it is difficult for traditional intelligence organizations responsible for human intelligence (HUMINT) collection.

Interestingly, since 9/11 the potential for positive information-sharing dynamics between intelligence operatives and NGOs has expanded dramatically for four reasons:

a. The availability and diffusion of information technology
b. The increasingly visible role of NGOs as important players in international affairs
c. The demand for international engagement in failed or failing states, many vulnerable to penetration by terrorists
d. The recognition of NGOs as important international economic players that account for over five percent of the gross domestic product and over four percent of the employment in thirty-six of the most impoverished countries in the world.[94]

In denied areas where U. S. military operations are not being conducted, no U.S. diplomatic presence exists, and intelligence assets are scarce or non-existent, it is my view that non-traditional HUMINT sources—including NGOs—should be developed. In many cases, NGOs will have been in the area long before any intelligence or military deployment. As such, NGO staff—particularly those of development, humanitarian assistance, and disaster relief organizations—will have a grasp of the overall situation "on the ground" in their particular area of expertise and operational area, making them excellent intelligence sources.[95]

Cumulatively, hundreds of international NGOs comprise a "global network of information" and capacity for information gathering, "even if the information flow is unpredictable and action is rarely coordinated."[96] Concurrently, the U.S. intelligence community and the national security apparatus in which it is embedded comprise another global information gathering network. In a perfect world, the information gathering capabilities of both networks should create opportunities to pool information and coordinate information requirements. However, several structural, cultural, and operational factors inhibit closer coordination and more positive working relationships.[97]

NGO and U.S. intelligence networks retain significant differences of mission and structure that militate against collaboration. The missions and motivations of NGOs and intelligence organizations stand almost in direct opposition. NGOs respond to the needs of their clients and the desires of their primary financial donors—the lifeblood of their existence. Intelligence organizations, on the other hand, respond to the desires of the current administration and to departments and agencies responsible for U.S. security.

In structure and organization, too, NGOs and intelligence agencies dramatically differ. As William E. DeMars notes, "The U.S. security apparatus is organized in a hierarchical structure under the President and the executive branch. Intelligence organizations are bureaucratic and respond to a definite chain of command. Conversely, international NGOs interact as a fluid and decentralized mix of thousands of independent organizations."[98] In stark contrast to U.S. military and security operations, NGOs operate independently, with no central control and no centralized chain of command. They rely on decentralized authority (especially in field operations) and value independence.[99] In recent years the NGO sector has seen a movement toward setting operating standards and best practices, but they are still often criticized for lacking standard procedures and adequate training.[100] Conversely, intelligence agencies—particularly military intelligence organizations—rely on established doctrine, regulations, and set procedures, expect discipline and conformity and are well trained.

Different cultural approaches to information requirements also affect the priority given to information-sharing relationships. NGO professionals are action-oriented and develop highly pragmatic information strategies intended to support immediate requirements. They don't do deep analysis. In contrast, U.S. intelligence analysts are

information specialists and place value on deep expertise: "For them, trading information is an end in itself, not a means to an end."[101]

Operationally, U.S. military and intelligence organizations differ greatly from their NGO counterparts. Access to operational funding is a good example. U.S. intelligence assets have what many argue are unlimited (and poorly regulated) funds. Comparatively, while they strive to remain neutral, few NGOs are able to fund their activities entirely out of private donations. For example, World Vision—now the largest U.S.-based NGO—secures 70 percent of its $869 million annual budget from private donors (individuals, corporations, and foundations), with the difference funded by government grants.[102] According to one specialist, the sheer magnitude of resources of the military and security agencies dwarf the programs of humanitarian NGOs, not only in Iraq and Afghanistan but in other low-income countries as well.[103]

Working with NGOs is complicated. Many are suspicious of the military and intelligence types and of Special Forces in particular. To me this is somewhat surprising, given the common contexts in which NGO staff and military or intelligence operatives often work. Years ago I articulated (albeit in a bit of tongue-in-cheek analysis) why Special Forces operators and NGO workers—particularly those who work for development, disaster relief, and humanitarian assistance NGOs—actually have much in common:

a. We tend to want to serve in interesting, far-off, and usually dangerous places
b. Most of us have foreign language qualifications
c. We work for low pay
d. We actually like mystery meat or can get by with no meat at all
e. We can get along without hot water for long periods of time. And, often—more often than not—smell peculiarly the same
f. We wear the same kinds of clothes
g. We hang out in the same bars
h. We don't like to be over-supervised … or supervised at all
i. We enjoy taking risks
j. And, in our own ways, both train hard to help mankind.[104]

Fundamentally, mutual mistrust mars the relationship between NGOs and most government agencies: NGOs "see any collaboration

as compromising their reputation for independence and impartiality," while government agencies "tend to view NGO workers as unpredictable and overly idealistic."[105] Most humanitarian, development, and disaster relief NGOs base their operations on three principles: impartiality ("that assistance is distributed solely on the basis of need regardless of race, religion, or political affiliation"), neutrality ("that organizations do not take sides in a conflict"), and independence ("that their actions are free of any political or military interests").[106] NGOs with a long history of independence tend to be more sensitive about following these principles, and often conclude that associating with any military or intelligence organization reduces their "neutral" status and increases their security vulnerability.

Some NGOs, such as the International Committee of the Red Cross (ICRC), pride themselves on serving a completely apolitical set of objectives and feel no need to share information with government-associated groups operating in the same area. The ICRC in particular "has maintained the clearest position of classic neutrality—that humanitarian action can and should be completely insulated from politics."[107] In fact, "Not only does the ICRC base its actions on its interpretation of established humanitarian law but in order to maintain neutrality has often adopted a position of silence in order to avoid being perceived as partisan."[108] Not all NGOs agree. Rather, some seek an association with the U.S. military in crisis zones, believing that a cooperative relationship will serve to protect their workers.[109]

In my view, complex counterterrorism challenges pose major problems for NGOs to remain truthful to the three principles of neutrality, impartiality, and independence, even when their contact with the military or intelligence services is limited. One important question in the context of any conflict is, "Who determines and defines neutrality and impartiality?"[110] Certainly, most terrorist groups—particularly Al Qaeda and its surrogates—do not recognize these three principles, as the ICRC found out in Baghdad in October 2003 when a car bomb aimed at Red Cross headquarters killed ten people.[111] It is primarily for this reason—the refusal of Al Qaeda to recognize the neutrality and impartiality of NGOs—that I believe NGOs should be willing collectors of information for intelligence purposes where Al Qaeda is presently recruiting, training, and operating or will be likely to do so in the future.

Advantages and Disadvantages of NGOs as Information Collectors

NGOs have several comparative advantages over traditional intelligence collectors engaged in early warning activities. As mentioned previously—and most importantly—NGOs often operate in locations where there is no military and/or intelligence presence.[112] Disaster relief, development assistance, and human rights NGO personnel are normally involved in on-the-ground operations and are therefore attuned to the local real-time security situation. Also, because NGOs are often present in an area over many years, they understand the sensitivities of the local culture and the immediate needs and vulnerabilities of the populace.[113] Finally, NGOs often have access to individuals who for any number of reasons would not speak with military or intelligence personnel.[114]

NGOs have several disadvantages too. The capabilities that most NGOs lack include ways to disseminate the information they may be able to gather. There are no protocols or systems for information sharing or analysis among the myriad of disparate NGOs. There is also a general lack of cooperation among NGOs. Differing agendas and mandates often divide groups. In addition, the competition for donor dollars often makes NGOs reluctant to share information with potential competitors in the battle to attract donors' largesse. Due to these factors, "…an NGO, in fulfilling its normal humanitarian functions, may collect important data for effective early warning, but this information rarely finds its way to governmental policy-making bodies."[115] Finally, one persistent obstacle to institutionalizing the collaboration between the intelligence community and NGOs is the unspoken norm of reciprocity that pervades the decentralized networks of NGOs. In other words, the "intelligence community is hard pressed to offer anything to NGOs in return for the information they provide to the U.S. government."[116]

Cooperation Does Work

There have been positive cases of successful information-sharing between intelligence collectors and NGOs. The "Great Lakes Crisis" in Central Africa in the mid-1990s is one example; the 2004-2005 tsunami relief effort is another. During the Great Lakes Crisis, which was prompted by the genocide in Rwanda, Washington wanted to act but

had few assets on the ground. Several NGOs were also eager to help, but had trouble identifying the most acute areas of crisis in Rwanda, Burundi, and the Democratic Republic of the Congo. Because U.S. national security sensitivity around the issues was low, "the government was willing to share satellite imagery (although it was of dubious value in heavily forested areas) and other intelligence derived information."[117] For their part, NGOs on the ground using modern means of communication were able to send back *ground truth* to U.S. agencies that had an interest in the operational area.[118] Southeast Asian tsunami relief operations in 2004-2005 were also a largely positive story. The U.S. government and its forces responded to NGO requests for transportation, while NGOs shared information.[119]

Much of the ability for NGOs and military or intelligence agencies to cooperate is based on personal contacts and relationships honed during times of crises. From personal experience—mine in Somalia and others from a number of hot spots—NGO workers and U.S. military and intelligence personnel deployed to crisis areas have often developed ad hoc collaborative arrangements for information-sharing based on mutual respect and, at least at a personal level, a capacity and commitment to work together.

Conclusion and Recommendations

Entities, like people, most generally cooperate when it is in their common interests to do so. In regions with the weakest state structures, Al Qaeda and other terrorist organizations often respond to citizens' basic requirements when state institutions cannot. For these regions, understanding Al Qaeda's presence, strategies, tactics, and operational procedures advances both counterterrorist operations and the ability of many NGOs—particularly development, disaster relief, and humanitarian assistance NGOs—to fulfill their charters. For such environments, NGOs and U.S. intelligence operators can hardly avoid dealing with each other, and at a minimum should value the information the other has to offer.[120] U.S. operatives must recognize that "NGOs, individually

… NGOs and U.S. intelligence operators can hardly avoid dealing with each other, and at a minimum should value the information the other has to offer.

and cumulatively, know some things that the intelligence community does not know from other sources."[121]

Typically, a variety of NGOs are on the ground in failed states and regions at risk, their staffs working in remote areas and interacting with diverse populations where traditional HUMINT operatives have difficulty maneuvering. In counterterrorism terms, the value-added in NGO-provided information lies in the opportunity to analyze the likelihood of terrorist activity resulting from the political, economic, and humanitarian consequences on the ground. The value-added by intelligence agencies is their ability to analyze a large volume of complex data, which NGOs cannot accomplish on their own.[122]

So what to do? Five observations and recommendations come to mind. First, the potential for compromise on the "three principles" outlined previously in this chapter should be addressed within the NGO community. Retaining neutrality and impartiality when an enemy such as Al Qaeda does not respect those principles is impossible for NGOs to achieve and counterproductive to their interests and mandate.

Second, complex terrorist security challenges require both NGOs and intelligence organizations (particularly those of Special Operations) to acknowledge, understand, and respect each others' mandates, capacities, and contributions.[123] Intelligence and NGO players should be involved in consultation at the strategic, operational, and tactical levels, and appropriate ways of communication need to be established.

Third, education is an important mechanism for creating understanding and long-term relationships. Increased knowledge about each other's need for information, coupled with increased knowledge about which information can be exchanged between different functions and players would contribute greatly to more effective information sharing and operations among the NGO and intelligence sectors. A specialized course—perhaps taught at the Joint Special Operations University or the National Defense University—could be the venue for increasing knowledge. The goals of such a course would be to develop and improve cooperation and sharing of information and intelligence in denied areas by giving operators, analysts, and NGO professionals who are involved in, or designated to work in areas at risk the ability to build—at least notionally—functioning networks and systems for collection, analysis, and dissemination of information.[124]

Fourth, consider using intermediaries to facilitate collaboration between NGOs and the intelligence community. A successful example of intermediary use occurred during the African "Great Lakes Crisis" in 1994. During that crisis, the National Security Council's Africa Director acted as the intermediary between Washington-based NGO Refugees International and the intelligence community. Due to his involvement, "The compatibility between the terms of the humanitarian issue as framed by the NGO and the terms of U.S. interests as framed by the NSC allowed the exchange to proceed with reciprocity and semi-transparency."[125] In contrast to traditional exchanges between U.S. intelligence agencies and NGOs, this reciprocity was based on trading information for information, rather than NGOs providing information for the possibility of influence.[126]

Finally, reciprocity is important. When dealing with intelligence agencies, a common complaint among NGOs is that the information flow is one-way: NGOs give, but do not receive. Also, there is little or no feedback on the reliability or effectiveness of the information NGOs feed. To alleviate this problem, my suggestion is for both sides to deal primarily in the exchange of non-classified, open-source information. Interestingly, intelligence analysts are finding it more important to keep up with this non-classified material published in full public view—like newspapers, jihadist blogs, and discussion boards in foreign countries—than some of the more secretive sources of intelligence.[127]

In my view, the major obstacle to good intelligence is the obsession with secrecy. According to some observers, 75 to 90 percent of classification is used to protect "turf" and reputations, not sources. Only a small minority of the information actually needs to be classified to protect sources, agents, or to prevent potential damage to the interest of the state.[128] According to a source with which I agree, the products produced by classified agencies are also frequently beaten out by non-classified sources when they compete head-to-head. Various past examples have embarrassed the classified intelligence communities badly. Colin Powell probably said it best when he commented on his information opportunities while Secretary of State: "I preferred the Early Bird with its compendium of newspaper stories to the President's Daily Brief, the CIA's capstone daily product."[129]

4. SOF For Life

A Potential Intelligence Force Multiplier

Special Operations Forces (SOF) For Life was a concept that had some traction at USSOCOM from 2001 through 2003. It was a program to "produce and sustain force of SOF Warriors capable of meeting the national security demands of today and tomorrow."[130] It was to be a "highly specialized and focused personnel program" that was intended to produce a SOF Warrior with a level of proficiency that would guarantee SOF relevance in the future. As envisioned, the concept would have placed emphasis and had impact on all the personnel phases of a SOF Warrior: recruitment, accession, development, and retention.[131]

Post-retirement utilization (or Continuous Reserve) was a main feature of the program. Despite the implications of the name, this feature applied to personnel separating from active duty, not formally retiring. Conceptually, the Continuous Reserve program would have selected "voluntary separating personnel" with eight to fourteen years of SOF experience to belong to a Joint SOF Reserve Organization (JSOF-R). Those who became members of JSOF-R would have been available for call-up as individual augmentees for periods of ninety days, or longer in special cases.[132]

The SOF For Life program was a novel, eclectic, all-encompassing concept that died in 2004 for unknown reasons. It is probable that the program was too difficult to comprehend in its entirety and too expensive to implement. Still, the Post-Retirement Utilization (Continuous Reserve) idea, perhaps in a modified format, could have great utility for intelligence gathering.

My suggestion is this: recruit retired Special Forces personnel who live or work overseas in at-risk areas as a force multiplier. While no statistics exist categorizing where retired Special Forces work or live, anecdotal evidence exists that suggests that the numbers are substantial for those who work, and frequently reside, in areas where current or potential terrorist, criminal cartel, and other security-threatening activities are taking place. One such anecdotal case was the September 2007 reunion and fifty-year anniversary of the First Special Forces Group. Among the attendees, six presently work in Nigeria, Sierra Leone, and Liberia. Two others work in Sudan. I know

of another who just sold a bar in Southern Thailand—an area rife with extremist Islamic terrorist activity. My guess is that there are many more, perhaps in the hundreds, who are working overseas in areas at risk and whose previous training makes them excellent information and intelligence assets. I recommend retaining their capabilities and skills in some organized form.

How This Might Work

You are a retired Special Forces NCO or officer and are working for an oil company or NGO in an at-risk area. With your employer's concurrence, you belong to a *retired reserve pool* whose members are on a small retainer for basically keeping their eyes and ears open and reporting once a month to a central facility. These reports might contain observations, thoughts, impressions, and gut instincts about the area you are in. To help you do this, you are "re-blued" in a short course before you deploy and given a standard template for reporting purposes—nothing fancy, but easy to use and to consolidate electronically. What you report is all *open source*.

If the area you are in heats up, you can (and this is tricky) be directed to get specific information. This is still all open source, but you are being asked to provide more detailed information that increases your exposure and the understanding of your employer. For this, your retainer is increased.

Then, if the area you are in really heats up, you might be in a position to do a lot of advanced party preliminary work: intelligence, logistics, LZ and DZ surveys, and similar tasks. For this level of work and exposure, you are brought back on active duty in your retirement grade, which does a number of things: protects you legally, compensates you for the increased risks, and provides for your family if things don't work out so well. All retirees can be recalled to active duty in an emergency until age sixty (in certain cases age seventy), so this is—or could be—a fairly pro forma procedure if all the advanced paperwork was front-loaded and held in your file.

Interested? My guess is that most Special Forces retirees would be. Expensive? Not really; the financial retainers for the first levels of exposure would be fairly minimal, and for the last level of exposure the government would be saving a lot of money in deployment and training costs.

How This Could Be Realized

First, a database needs to be developed to catalogue and categorize all of those Special Forces retirees who would like to voluntarily participate and are in a position and location to do so. Regardless of whether the plan is eventually adopted, this database should be developed as a minimum measure.

Second, a small control center would have to be established to run the program. This does not need to be (nor should it be) a large organization and it should not be in some headquarters intelligence shop. It needs to be at the War College or in the basement in the Department of Social Sciences at West Point and titled a "Research Officer" or "Research Directorate" or some such term. Retirees in the program would be listed as researchers until or unless they were activated, and then they would be handled, controlled, directed, and protected by normal military command and control or "country team" channels and procedures.

Far-fetched? I think not. Doable? Most certainly. This program could be the most substantive force multiplier for intelligence collection to exist in several decades.

Concluding Remarks

The main premise of this research paper is that the present international security environment requires new and perhaps controversial intelligence collection alternatives. The technical remedies that satisfied Cold War intelligence requirements are not adequate for the collection challenges faced by the U.S. and its Western allies. Our common enemy today—Islamist extremists, the most dangerous being Al Qaeda—are not vulnerable to the same intelligence-gathering mechanisms that helped to bring down our past common enemy, the Soviet Union.

Unlike the Soviet Union, Al Qaeda is not a centralized, hierarchical state that exercises its military arm in full view of satellite technology and or communicates in ways that make eaves dropping relatively simple. Al Qaeda and its extremist compatriots are networks of relatively autonomous cells, held together by a perverse ideology and inspired and directed—though not controlled—by charismatic leaders.[133] Also, unlike the Soviet Union, Al Qaeda holds no territory and possesses no capital. Al Qaeda operates in the shadows and seeks sanctuary in failed and failing states, where the organization can plan terrorist attacks and recruit and train operators undetected by sophisticated technical intelligence assets.

Offered in this paper were four ideas for leveraging diverse groups—criminals, diasporas, NGOs, and SOF retirees—to help intelligence organizations collect intelligence-producing information from denied areas where technical assets have limited success and regular HUMINT assets have difficulty operating. None of these ideas are entirely new. All have been used in the past, and are used now in some fashion—albeit not very often and, in the case of diasporas, are used mostly by our adversaries. Individually or collectively—at least in my view—these four *intelligence force multipliers* could help win the global war on terrorism.

The benefit to SOF in leveraging criminals, diasporas, NGOs, and retirees for intelligence purposes is mixed. National-level agencies would most likely take the lead and benefit most from leveraging criminals and diasporas. However, disseminated intelligence information from these sources would eventually find its way to SOF consumers. Information from NGOs could have immediate benefit for national

intelligence organizations and SOF, depending on the type and location of the NGO and at what level in the organization the information is processed. One could assume connectivity between Washington and the headquarters of major NGO organizations. One would hope that forward deployed NGO and SOF teams would share information and develop symbiotic partnerships in denied areas. Finally, retirees in the proposed SOF for Life concept would be the easiest and my guess the most beneficial intelligence force multiplier for SOF to leverage. Many SOF retirees—particularly Special Forces retirees—have the requisite knowledge base, could be easily re-trained and are out there now. All they need is a bit of direction and support to become important intelligence force multipliers in denied areas.

Endnotes

1. The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Executive Summary* (Washington, DC: U.S. Government Printing Office, 2004). Available at <www.9-11commission.gov/report/911Report_Exec.pdf>. Accessed September 11, 2007.
2. Ibid.
3. Lawrence E. Cline, "Operational Intelligence in Peace Enforcement and Stability Operations," *International Journal of Intelligence and Counter-Intelligence*, Vol. 15, No. 2 (Summer 2002): 179-194; William E. DeMars, "Hazardous Partnership: NGOs and United States Intelligence in Small Wars," *International Journal of Intelligence and Counter-Intelligence*, Vol. 14, No. 2 (Summer 2001): 193-222, 200.
4. Paul Hoversten, "Forty Years Ago a Top Secret Satellite (CORONA) Snapped Photographs of Selected Missile Sites in the USSR," Space.com, September 26, 2000. Available at <www.space.com/news/space-history/nro_at_forty_00926.html>. Accessed September 11, 2007.
5. Ibid.
6. See Daniel Benjamin and Steven Simon, *The Age of Sacred Terror* (New York: Random House, 2002).
7. Dennis M. Gormley, "The Limits of Intelligence: Iraq's Lessons," *Survival*, Vol.46, No.3 (Autumn 2004), 8.
8. Found at <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/curing-analytic-pathologies-pathways-to-improved-intelligence-analysis-1/summary.htm>.
9. Gormley, 8.
10. Daniel Byman, "U.S. Counter-Terrorism Operations: A Taxonomy," *Survival*, Vol. 49, No. 3 (Autumn 2007), 127.
11. Stewart Patrick, "Weak States and Global Threats: Fact or Fiction," *The Washington Quarterly*, Vol. 29, No. 2 (Spring 2006): 27-53; 27.
12. Ibid, 27.
13. John Robb, *Brave New War* (New York: Wiley, 2007), ii.
14. Ibid.
15. Banning N. Garrett and Dennis M. Sherman, "Why Non-Globalized States Pose a Threat: Increasing Interdependence is Key Concern," *Update: For Alumni and Friends of the UW-Madison School of Business* (Fall/Winter 2003). Available at <www.bus.wisc.edu/update/winter03/globalization.asp>. Accessed September 11, 2007.
16. Ibid.
17. Frank J. Cilluffo, Ronald A. Marks, and George C. Salmoiraghi, "The Use and Limits of U.S. Intelligence," *Strategic Intelligence: Windows Into a Secret World*, (Roxbury Publishing: Los Angeles, 2004), 36. See also *Counterterrorism Intelligence Capabilities and Performance Prior to*

9/11, House Permanent Select Committee on Intelligence, July 2002, available at <www.fas.org/irp/congress/2002_rpt/hpsci_ths0702.html>; and William C. Banks and Peter Raven-Hansen, "Targeted Killing and Assassination: The U.S. Legal Framework," *University of Richmond Law Review* (March 2003), available at <http://insct.syr.edu/Research/Publications/ProfessorsPublications/Banks/Targeted%20Killing%20and%20Assassination.pdf>.

18. Cilluffo et. al., 37.
19. Tim Newark, "Pact With the Devil," *Britannica Online*, April 2001. Avail. able at <www.britannica.com/magazine/article?query=Mafia&id=2>.
20. Stefan Mair, "The New World of Privatized Violence," *International Politics and Society*, Vol. 2 (2003), 12.
21. Bruce Hoffman, *Inside Terrorism* (New York: Columbia Press, 1998), 43. See also Svante E. Cornell, "The Interaction of Narcotics and Conflict," *The Journal of Peace Research,* Vol. 42, No. 6 (2005), 753.
22. Mair, 12.
23. Hoffman, 42.
24. Mair, 19.
25. Rensselaer Lee, "Nuclear Smuggling, Rogue States and Terrorists," *China and Eurasia Forum Quarterly*, Vol. 4, No. 2, (2006), 26.
26. Ibid.
27. Ibid.
28. Louise I. Shelley and John T. Picarelli, "Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism," *Police Practice and Research*, Vol. 3, No. 4 (January 2002), 312.
29. Sara A. Carter, "Terrorists Teaming with Drug Cartels," *Washington Times*, August 8, 2007, 1.
30. Ibid.
31. Shelly and Picarelli, 312.
32. Ibid.
33. "Crackdown on Thai Visa Train to Canada," *The Southern Post*, August 8, 2002. Available at <www.southasianpost.com/portal2/ff8080810ebfa5d9010ebfcfaea200b0.do.html>.
34. Ibid.
35. Interestingly, the Grace Hotel is located in the Nana District. During the Vietnam era, the Grace was a popular spot for U.S. Special Forces soldiers. Today it caters to Arabs and others of the Muslim faith. See also, Bertil Lentnir, "A How-To-Guide for Fleeing China," *Asia Times Online*, April 19, 2007, available at <www.atimes.com/atimes/China/ID19Ad01.html>.
36. Douglas A. Kash, "Hunting Terrorists Using Confidential Informant Reward Programs," *FBI Law Enforcement Bulletin*, April, 2002, 26.
37. Kevin Whitelaw, "Just a Phone Call Away," *U.S. News and World Report*, January 23, 2005.

38. Ibid.
39. Gethin Chamberlin, "Uday and Qusay Die in Gun Battle," *The Scotsman,* July 23, 2003, 1. Available at <http://64.233.169.104/search?q=cache:_DElNHehDnYJ:www.mercurynews.com/ci_6055622+former+drug+dealer+turned+informant+helps+stop+jfk+airport+plot&hl=en&ct=clnk&cd=1&gl=us>.
40. JFK Terror Plot Informant Crucial to Case," *CBS News*, June 4, 2007. Available at <www.cbsnews.com/stories/2007/06/04/terror/main2880870.shtml>.
41. Josh Meyer, "Three Arrested on U.S. Arms, Terrorism Charges," *Los Angeles Times*, June 9, 2007, A7.
42. "International Arms Dealer Charged with Trying to Kill Americans," *P. R. Newswire*, June 8, 2007. Available at <http://news.findlaw.com/prnewswire/20070608/08jun20071233.html>.
43. Meyer, A7.
44. Aram Rosten, "Meet the Prince of Marbella," *The Observer*, October 1, 2006, 1.
45. Ibid.
46. Matthew Brunwasser, "The Prince of Marbella: Arms to All Sides," *PBS Frontline*, May 2002.Available at <www.pbs.org/frontlineworld/stories/sierraleone/alkassar.html>.
47. Ibid.
48. Chris Thompson, "Busting the Merchant War," *The Village Voice*, July 24, 2007. Available at <www.villagevoice.com/news/0730,thompson,77325,6.html>.
49. "International Arms Dealer Charged with Trying to Kill Americans."
50. Meyer, A7.
51. Rosten.
52. Richard Willing, "Papers: Con Was Key in Foiling JFK Plot," *USA Today*, June 4, 2007, 3A.
53. Ibid.
54. "Diaspora," Merriam-Webster Online Dictionary. Available at <www.m-w.com/dictionary/diaspora>. Accessed October 1, 2007.
55. "Diaspora," *Oxford English Dictionary* Online. Available at <http://dictionary.oed.com/cgi/entry/50063322?single=1&query_type=word&queryword=diaspora&first=1&max_to_show=10>. Accessed October 1, 2007.
56. Robin Cohen, *Global Diasporas, an Introduction* (London: University College London Press, 1997), 520.
57. Gregory Kent, "Diaspora Power: Network Contributions to Peacebuilding and the Transformation of War Economies," paper presented at the "Transforming War Economies" Seminar, Plymouth, UK, June 16-18, 2005. Page 7. See also Gabriel Sheffer, *Diaspora Politics at Home and Abroad* (Cambridge: Cambridge University Press, 2003), 245

58. Rex Brynen, "Diaspora Populations and Security Issues in Host Countries," paper presented at the Metropolis Interconference Seminar, "Immigrants and Homeland," Dubrovnik, Croatia, May 11, 2002, 4. Full text of paper available at <http://international.metropolis.net/events/croatia/brynen.pdf>. Accessed October 1, 2007.
59. Louise I. Shelley and John T. Picarelli, "Methods not Motives: Implications of the convergence of International Organized Crime and Terrorism," *Police Practice and Research*, Vol. 3, No. 4 (September 2006), 308.
60. Brynen, 4.
61. John P. Sullivan, "Policing Networked Diasporas," *Small Wars JournalBlog,* July 9, 2007. Available at <http://smallwarsjournal.com/blog/2007/07/print/policing-networked-diasporas>. Accessed October 1, 2007.
62. Ibid.
63. Ibid.
64. Ibid.
65. Ibid.
66. Ibid.
67. Daniel Byman, Peter Chalk, and Bruce Hoffman, "The New Face of Insurgency," *Rand Research Brief,* RB-7049-OTI, 2001. Available at <http://rand.org/pubs/research_briefs/RB7409/index1.html>. Accessed October 1, 2007.
68. James Phillips, "Hezbollah's Terrorist Threat to the European Union," Testimony Before the House Committee on Foreign Affairs, European Sub-Committee, June 20, 2007. Available at <www.heritage.org/Research/MiddleEast/tst062007a.cfm>. Accessed October 1, 2007.
69. C. Christine Fair, "Diaspora Involvement in Insurgencies: Insights from the Khalistan and Tamil Eelam Movements," *Nationalism and Ethnic Politics*, Vol. 11, No. 1 (Spring 2005), 139.
70. Ibid, 140.
71. Dominic Whitman, "LTTE Tamil Tigers and its UK-Wide Network," *Global Politician*, October 18, 2006. Available at <www.globalpolitician.com/articledes.asp?ID=2235&cid=3&sid=74>. Accessed October 1, 2007.
72. Brian Nichiporuk, "The Security Dynamics of Demographic Factors," *Rand Monograph Report,* 2000. Available at <www.rand.org/pubs/monograph_reports/MR1088>. Accessed October 1, 2007.
73. Brynen, 14.
74. Ibid.
75. Brian J. Auten, "Political Diasporas and Exiles as Instruments of Statecraft," *Comparative Strategy,* Vol. 25, No. 4 (Otober-November 2006):329-341; 329.
76. Ibid, 332.

77. Joseph Winter, Somalia's Diaspora offers Financial Lifeline," BBC News, November 24, 2004. Available at <http://news.bbc.co.uk/2/hi/africa/4038799.stm>. Accessed October 1, 2007.
78. Ibid.
79. Auten, 332.
80. Ibid.
81. Jytte Klausen, "British Counter-Terrorism After the July 2005 Attacks, Adapting Community Policing to Fight Against Domestic Terrorism," *USIPeace Briefing*, U.S. Institute for Peace, February 2007. Available at <www.usip.org/pubs/usipeace_briefings/2007/0205_terrorism.html>. Accessed October 1, 2007.
82. House of Commons Hansard Debates, March 20, 2007. Available at <www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070320/halltext/70320h0002.htm>. Accessed October 1, 2007.
83. "U.S. Military Courting American Muslims," *NewsMax.com*, February 7, 2007. Available at <http://archive.newsmax.com/archives/ic/2007/2/7/154749.shtml>. Accessed October 1, 2007.
84. Tim Kilbride, "Shared Understanding Provides Key to Defeating Extremism," *American Forces Press Service,* April 26, 2007. Available at <www.defenselink.mil/news/newsarticle.aspx?id=32955>. Accessed October 1, 2007.
85. There is no such thing as a "Muslim Diaspora" in the United States. There are many predominantly Muslim diasporas that are mostly structured along ethnic rather than religious lines. Underscoring the lack of information about Muslim diasporas is the fact that no one knows how many Muslims there are in the United States. Estimates vary from three to eleven million people.
86. "U.S. Military Courting American Muslims."
87. The World Bank Group, *Entering the 21st Century: World Development Report 1999/2000* (Washington, DC: International Bank for Reconstruction and Development, 2000), 40. See also Min Zhou, "The Chinese Diaspora and International Migration," forthcoming in *Social Transformations in Chinese Societies*. Paper available at <www.sscnet.ucla.edu/soc/faculty/zhou/pubs/Zhou_Chinese_Diaspora.pdf>. Accessed October 1, 2007.
88. Kent, 1. Professor Kent's article specifies the last two decades, but this author was in China in 1979 and maintains that the growth really started when Deng Xiaoping assumed power.
89. I taught Chinese Politics and Government at the U.S. Military Academy, West Point for a number of years, went to graduate school in Taiwan, and have made more than thirty trips to China. This is my best recollection of Chinese migration periods as I have studied and taught them.
90. Stanislav Lunev, "Chinese Intelligence Activities," *Insight on the News,* November 17, 1997, 1.
91. Ibid.

92. Nichiporuk, 23.
93. *FM 3-05.102, Army Special Operations Forces Intelligence*, July 2001, Appendix 1.
94. For an in-depth discussion of the potential for information sharing between intelligence agencies and NGOs, see Ellen B. Laipson, "Can the USG and NGOs Do More? Information Sharing in Conflict Zones," *Studies in Intelligence: Journal of the American Intelligence Professional*, Vol. 49, No. 4 (2005). Available at <www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no4/USG_NGOs_5.htm>. Accessed October 1, 2007.
95. Lawrence E. Cline, "Operational Intelligence in Peace Enforcement and Stability Operations," *International Journal of Intelligence and Counterintelligence,* Vol. 15, No. 2 (Summer 2002): 179-194; 184.
96. William E. DeMars, "Hazardous Partnership: NGOs and United States Intelligence in Small Wars," *International Journal of Intelligence and Counterintelligence,* Vol. 14, No. 2 (Summer 2001): 193-222; 196.
97. Ibid.
98. Ibid.
99. Laipson, 2.
100. See, for example, "The Sphere Project: Humanitarian Charter and Minimum Standards in Disaster Response," available at <www.sphereproject.org >, accessed October 1, 2007; and "The HAP Principles of Accountability," The Humanitarian Accountability Partnership-International, available at <www.hapinternational.org/en/page.php?IDpage=3&IDcat=10>, accessed October 1, 2007.
101. Laipson, 4.
102. "Frequently Asked Questions: World Vision at a Glance," World Vision website. Available at <www.worldvision.org/worldvision/pr.nsf/stable/press_FAQs?Open&lid=press_FAQs&lpos=main>. Accessed October 1, 2007.
103. Barbara Brubacher, "Moral and Practical Challenges to NGO Neutrality," *Global Policy Forum*, September 28, 2004. Available at <http://globalpolicy.org/ngos/aid/2004/0928neutrality.htm>. Accessed October 1, 2007.
104. First articulated by the author of this piece at a "Ground Operations Workshop" in Washington, DC sponsored by the Carr Center for Human Rights at the John F. Kennedy School of Government, Harvard University, October 17-18, 2002. Sara Sewell, the director of the Carr Center, often comments on the "reliability" of the list: "General Howard captures a central truth that many would prefer to deny: the Special Forces and humanitarian assistance communities have much in common. Their values-driven professions appear at odds, but they have striking similarities from which mutual respect can grow. Understanding and respecting both the differences and the similarities is critical for planning and executing field missions that affect foreign civilians." For more

information about the "Ground Operations Workshop," see <www.ksg.harvard.edu/cchrp/programareas/conferences/october2002.php>, accessed October 1, 2007.

105. "Does Early Warning Work?" *Forced Migration Monitor*, May 1997. Monthly newsletter of the Forced Migration Projects (1994-1999), a past initiative of the Open Society Institute. Available at <www.osi.hu/fmp/html/fmm_may_97.1.html>. Accessed October 1, 2007.
106. Djenana Jalovcic, "Who Leads, Who Follows and Who is Able? The Operational and Strategic Relations between International Organizations, the Military and NGOs," unpublished paper presented at the Weak States and Sudden Disasters and Conflicts: The Challenge for Military-NGO Relations Conference, Ottawa, Canada, June 7, 2005, 3. Available at <www.irpp.org/events/archive/jun05NGO/jalovcic.pdf>. Accessed October 1, 2007.
107. Brubacher.
108. Ibid.
109. Ibid.
110. Jalovicic, 3.
111. Charles Hanley, "Baghdad Bomb Kills 34," *The Age* (Australia), October 28, 2003, 1.
112. Daniel Byman, "Uncertain Parners: NGOs and the Military," *Survival*, Vol. 43, No. 2 (January 2001), 100.
113. Ibid.
114. Ibid.
115. "Does Early Warning Work?"
116. DeMars, 199.
117. Laipson, 2.
118. Ibid.
119. Ibid.
120. DeMars, 200.
121. Ibid, 201.
122. Ibid, 204.
123. Adapted from Jalovicic's "Who Leads, Who Follows and Who is Able?," 7.
124. A possible model for such a course might be the "Information and Intelligence Cooperation in Multifunctional Operations" Course, taught at the Folke Bernadotte Academy in Sweden. Course description available at <www.oss.net/dynamaster/file_archive/060531/f340b4a8c09b9b825a1969f07cb4b812/Swedish%20PKI%20Course%20description.doc>. Accessed October 1, 2007.
125. DeMars, 208.
126. Ibid.

127. Clive Thompson, "Open Source Spying," *New York Times Magazine*, December 3, 2006. Available at <www.nytimes.com/2006/12/03/magazine/03intelligence.html>. Accessed October 1, 2007.
128. Tom Quiggen," "Open Source Intelligence for National Security," International Relations and Security Network website, September 28, 2006. Available at <www.isn.ethz.ch/news/sw/details.cfm?ID=16727>. Accessed October 1, 2007.
129. Ibid.
130. *USSOCOM Concept: Special Operations Forces (SOF) For Life*, concept paper prepared by the Future Concepts Development Branch (SORR-STC), U.S. Special Operations Command, April 18, 2003 (Version I), 12.
131. Ibid.
132. Ibid, 27-28.
133. Mair, 17.