# Counterintelligence in the War Against Terrorism (U)

***Michael J. Sulick***

**"Closer integration could maximize the contributions of powerful counterintelligence tools in the fight against terrorism."**

US counterintelligence (CI) sometimes failed during the Cold War. Until unmasked, a number of Soviet spies inflicted serious damage on national security that could have shifted the balance in a war with the Soviet Union. The Soviets would have enjoyed significant military advantage armed with, among other secrets, the US Continuity of Government plan passed by Robert Hanssen, the volumes on US Navy capabilities from the Walker spy ring, and information on tactical nuclear weapons and military communications from retired Army Sgt. Clyde Conrad. Fortunately, the United States and the Soviet Union never went to war, and Moscow never had the opportunity to exploit the advantages gained from its Cold War spies. (U)

Now, however, the United States *is* at war. The enemy can immediately exploit information gained through espionage to launch attacks. Imagine a Hanssen or an Ames spying for a terrorist group, providing them data about US counterterrorist sources, analyses, and intelligence gaps—the damage could be catastrophic. Terrorist espionage inside the US Intelligence Community is no longer a remote possibility. Clandestine reporting has surfaced terrorist plans to infiltrate the community, and the number of government employees and applicants investigated on suspicion of terrorist connections is steadily increasing. Considering the potential speed of implementation and high-casualty focus of terrorist tactics, US counterintelligence cannot afford to fail to uncover enemy spies in this war. (U)

Neutralizing espionage is only one of the roles that counterintelligence plays. CI also compiles and analyzes information on the enemy's security services to disrupt their intelligence collection against the United States and facilitate our penetration of their ranks. It establishes mechanisms to protect sensitive intelligence through compartmentation, yet disseminate that intelligence to appropriate consumers. CI provides critical support to intelligence collection by vetting sources to ensure that information is comprehensive, accurate, and not designed to deceive—in the terrorist arena, disinformation from a single double agent could divert us from a real attack. The very nature of terrorist tactics, relying on surprise, clandestinity, and compartmentation, has thrust intelligence into a central role in the war against terrorism. (U)

The critical role of intelligence in this war argues for closer integration of counterintelligence and counterterrorist efforts than now exists. In a recent article in *The Economist*, six distinguished IC retirees emphasized the need for a new approach: ". . . the jobs

**Michael J. Sulick** served as the Associate Deputy Director for Operations at CIA.

(b)(3)(c)

> **Terrorists spy before they terrorize.**

of countering terrorism and countering hostile intelligence services are hardly distinguishable from the other. To separate them artificially, as the IC does now, is to make a difficult task even harder."[1] Along the same line, retired Gen. William Odom, a former director of NSA, noted the link between counterintelligence and counterterrorism in testimony before the US Senate: "CI is intelligence about the enemy's intelligence . . . because terrorists have much in common with spies, operating clandestinely, CI must also include counterterrorism intelligence, both domestically and abroad."[2] (S)

(b)(1)
(b)(3)(n)

This article examines the many ways in which closer integration of these similar missions could maximize the contributions of powerful counterintelligence tools in the fight against terrorism. (U)

### Terrorists as Intelligence Operatives (U)

Simply put, terrorist groups operate like intelligence services. Terrorists spy before they terrorize. They case and observe their targets. They collect intelligence about their enemy's vulnerabilities from elicitation and open sources. They vet potential recruits by rigorous screening procedures. Like intelligence officers, terrorists practice tradecraft. Materials found in al-Qa'ida safehouses in Afghanistan and other countries include training manuals on espionage tradecraft, such as the identification of clandestine meeting and deaddrop sites, techniques to recruit sources, covert communications, and tracking and reporting on targets. (U)

Terrorists also prepare their operatives to live cover with an intensity Soviet illegals would have envied. In an al-Qa'ida safehouse in Afghanistan, US forces discovered handwritten notes with guidance on operating under cover, including tips on traveling in alias, pocket litter to carry, and types of clothing to wear, down to details about the proper underwear to don in a foreign land.[3] (U)

For al-Qa'ida terrorists, living cover even has the sanction of Islamic doctrine. Some of the September 11 hijackers were believed to have been adherents of *takfiri wal Hijra*, an extremist offshoot of the Moslem Brotherhood spawned in the 1960s, whose adherents claim that the Koran advocates integration by Moslems into corrupt societies as a means of plotting attacks against them.[4] According to *takfiri* precepts, al-Qa'ida operatives can play the infidel to gain access to the enemy's targets and can even violate Islamic laws provided that the goal justifies the otherwise illicit behavior. The September 11 hijackers wore expensive jewelry and sprayed themselves with cologne at US airports, believing that these Western traits would shield them from the scrutiny given orthodox Moslems. The immersion of these 19 hijackers into American society tragically illustrates the effectiveness of living cover down to the smallest detail. (U)

If terrorist groups operate like intelligence services, counterintelligence can play the same role in combating them as it has and

[1] Bob Bryant, John Hamre, John Lawn, John MacGaffin, Howard Shapiro, Jeffrey Smith, "America Needs More Spies," *The Economist*, 10 July 2003: 3. (U)
[2] William Odom, Testimony to the US Senate Governmental Affairs Committee, 21 June 2002. (U)
[3] Susan B. Glasser, "A Terrorist's Guide to Infiltrating the West," *The Washington Post*, 9 December 2001: A1. (U)
[4] Jane Corbin, *The Base: Al Qaeda and the Changing Face of Global Terror* (London: Simon & Schuster, 2002), 131–32. (U)

> **"The best defense is recruitment of our own spies in their ranks."**

continues to do against the Russian SVR, the Chinese Ministry of State Security, and other intelligence services hostile to US interests. One of the primary tasks of CI is gaining a thorough knowledge of an adversary's intelligence service—its capabilities, organization, modus operandi, personalities, and use of cover. Such comprehensive knowledge can enable defensive measures to disrupt terrorist intelligence collection, but its primary goal is offensive counterintelligence: the recruitment of spies within the ranks of adversary intelligence-like organizations. The best defense against enemy spies, whether from foreign intelligence services or terrorist groups, has been and always will be the recruitment of our own spies in their ranks. (U)

**Exposing Terrorist Spies (U)**

(b)(1)
(b)(3)(n)

John Walker Lindh, however, was of a different mold. Dubbed the "American Taliban" after his capture in Afghanistan, Lindh, came from an affluent northern California suburb, had no criminal record,

[6] *Ibid.* (S)

"(b)(1)
(b)(3)(n)"

and carried decent academic credentials. He had studied Arabic and traveled extensively in the Middle East, experiences that might have made him an attractive candidate for US intelligence. If terrorists operate like intelligence services, intelligence officers should assume that they will attempt to infiltrate the security agencies of their main enemy by cultivating promising candidates for employment with backgrounds similar to Lindh's. (U)

(b)(1)
(b)(3)(n)

Terrorist spies within the Intelligence Community also would present more imminent risks than Cold War spies who passed information on US plans, intentions, and capabilities. Once the Cold War spies were discovered, the government had time to adopt and implement countermeasures to balance the losses. But time is not on our side in the war on terrorism. Terrorist spies within the Intelligence Community could acquire information on gaps and vulnerabilities that could be used to plan attacks in very short order, or could even launch attacks from within against the agencies themselves. Our current security system was designed in the Cold War to protect classified information, not personnel and physical infrastructure. Now, however, we must develop a system that can do both. (U)

**More Employees to Worry About (U)**

The problem of protection against spies from within is further complicated by the fact that personnel and facilities must also be defended from individuals with minimal or no clearance—custodial staff, cafeteria workers, maintenance and delivery personnel—who have no access to areas with classified information, but could still pose a threat. While some government employees still flinch at the rumble of jets from a nearby aircraft, the terrorist insider with minimal or no clearance could silently poison the food or water supply or plant a time bomb while cleaning an empty office. (FOUO)

(b)(1)
(b)(3)(n)

**"Terrorist D&D borrows from the Soviets and Islamic tradition."**

(b)(1)
(b)(3)(n)

**Terrorist D&D (U)**

Terrorist groups have proven their ability to adopt the sophisticated D&D techniques of our Cold War adversaries: double agents reporting on the same threat to validate each other's information, passing vague yet enticing tidbits without details, and engaging in intentionally misleading telephone conversations that they expect to be intercepted. (U)

Terrorist D&D not only borrows from the Soviet bloc services but also is deeply rooted in Islamic tradition. Shiite Muslims, for example, practiced the concepts of *taqiya*, precautionary deception and dissimulation, and *kitman*, the concealment of malevolent intentions, against their Sunni enemies in the 7th century, and they continue to do so against today's adversaries.[8] One of the common tactics of kitman and taqiya involves "deceptive triangulation,"—persuading one enemy that a jihad is directed against another enemy. Taqiya is regarded as a virtue and a religious duty, a "holy hypocrisy" that justified lies and subterfuge in defense of the faith. Current attempts by double agents to plant bogus information about planned attacks draw from this ancient practice. (U)

(b)(1)
(b)(3)(n)

[8] "Taqiya and Kitman: The Role of Deception in Islamic Terrorism," <www.CI-CE-CT.com>, 2 December 2002. (U)

(b)(1)
(b)(3)(n)

(b)(1)
(b)(3)(n)

**Caveats (U)**

> **"Intelligence is now vital to a host of non-traditional users."**

Counterterrorism entails rapid turnover of agents, fast-paced operations, quick reactions, and tactical moves to exploit actionable intelligence in order to counter imminent threats. Counterintelligence, on the other hand, inherently involves long and patient study, painstaking review, and correlation of details to gradually illuminate the shadows around its targets. It is the difference between a quick game on a pinball machine and an elaborate jigsaw puzzle. (U)

### Sharing Intelligence Down the Line (U)

One of the most dramatic developments after September 11 was the recognition that intelligence information needs to be shared among a vast number of consumers to prevent future terrorist attacks. Intelligence previously disseminated to a handful of top policymakers is now vital for a host of non-traditional users in the counterterrorist arena, particularly the Department of Homeland Security (DHS) agencies and state and local law enforcement that had never required such access in the past. (U)

The budding alliance between intelligence and law enforcement is still an uneasy one. As former CIA General Counsel Jeffrey Smith wryly noted, "It's like putting diplomacy in the War Department."[10] Intelligence collects secrets, informs policymakers, and warns of threats; law enforcement catches criminals and tries them in public. In the counterterrorist arena, these distinctions are now blurred by the need to share intelligence with law enforcement and the need for law enforcement to act on that intelligence. (U)

Expanding the number and type of recipients of intelligence inevitably increases the risk of leaks of classified information. Such compromises can be costly, jeopardizing the security of agents operating in the most unforgiving environments, shutting down technical collection operations, tipping off terrorists to our capabilities, and perhaps driving them toward new plans and targets. (U)

Leaks of counterterrorist intelligence can also damage one of our most critical assets in the counterterrorist campaign: cooperation with foreign liaison services. The transnational activities and compartmented nature of terrorist groups require in-depth knowledge of foreign environments and cross-border

---

[10] Jeffrey Smith, quoted by Ralph Blumenthal, "War of Secrets," *New York Times*, 8 September 2002: 16. (U)

cooperation that unilateral efforts alone cannot provide. The United States cannot promote liaison cooperation, however, without ensuring that counterintelligence concerns are addressed. (U)

Unfortunately, our record in protecting liaison information and sources has been flawed on occasion. As a result, some foreign governments and their intelligence services deliberately withhold information from us out of concern for leaks in the US media. Other governments cooperate with us only behind the scenes because of domestic political considerations and the absence of good counterintelligence in handling their information could abruptly halt this discreet flow of information. (U)

Counterintelligence alone will not eliminate the probability of some compromises of counterterrorist information. We have never avoided compromises in other areas, and we face a far more daunting challenge in counterterrorism considering the volumes of information and increased numbers of consumers. Nor will counterintelligence resolve the inherent contradiction between expanded intelligence sharing and compartmentation of sources and methods. CI can, however, help establish mechanisms to achieve some balance between the two. (U)

CIA and the FBI have developed special controls to disseminate

> **"Leaks can damage critical cooperation with foreign liaison services."**

sensitive counterespionage information to appropriate consumers without jeopardizing penetrations of our most hostile and vigilant adversaries. Counterintelligence can now assist other counterterrorist programs in developing similar controls balancing the "need-to-know" principle with the requirement for increased dissemination. Counterintelligence also develops strategies to mitigate the damage from intelligence compromises once they occur to enable crucial decisions on the continued use of particular sources and methods. Finally, counterintelligence conducts damage assessments after compromises and produces "lessons learned" studies to enable necessary adjustments that may prevent similar losses in the future. (U)

Counterintelligence training can also help to familiarize new consumers with the proper procedures for handling intelligence. The Department of Homeland Security has established a counterintelligence office of its own and set among its main tasks a counterintelligence awareness program for its constituent agencies and state and local law enforcement officials. CIC already manages an extensive CIA training program open to Intelligence Community members that focuses on counterintelligence awareness. To the extent resources permit, CIA as well as other agencies sponsoring similar training should collaborate with DHS to develop and implement tailored counterintelligence awareness training for state and local officials who are granted access to intelligence information. All efforts to ensure that the expanded pool of recipients handles sensitive material carefully are steps in the right direction. Any leak averted as a result may be a source protected or, perhaps, a terrorist attack prevented. (U)

### Next Steps (U)

While many of the comments above apply to CIA's two core missions of operations and analysis, the integration of counterintelligence practices throughout the Intelligence Community could enhance overall US intelligence collection and analysis on terrorism. Some have argued that Intelligence Community reorganization is required to integrate the two disciplines. Gen. Odom has advocated a new "National Counterintelligence Service" to manage counterterrorism and counterintelligence.[11] The retired intelligence professionals cited in *The Economist* article proposed a new organization within the FBI incorporating counterintelligence and

[11] William Odom, Testimony to the US Senate Governmental Affairs Committee, 21 June 2002. (U)

counter-terrorism and subordinate to the DCI—somewhat similar to the National Reconnaissance Office's joint relationship with the Department of Defense and the DCI.[12] (U)

Discussion of broad Intelligence Community reorganization goes beyond the scope of this article. While debate proceeds about reorganization, however, valuable time is lost as terrorists plan more attacks. Counterintelligence operational, analytic, and investigative capabilities already exist and are well-developed in key national security agencies. The issue is marrying these capabilities more closely with counterterrorist efforts and ensuring that counterintelligence professionals and their tools—their knowledge of intelligence service modi operandi, agent validation procedures, D&D analysis, and compartmentation mechanisms—are fully integrated into counterterrorist components of the IC. (U)

(b)(1)
(b)(3)(n)

[12] Bryant, *et. al.*, *The Economist*, 10 July 2003: 4. (U)

**"Counterintelligence must impose itself now."**

### In Conclusion (U)

CIA and other US intelligence agencies were established by law for the primary purpose of collecting intelligence to protect national security, not to catch spies and conduct counterintelligence activities. But we cannot ensure that our intelligence is complete, accurate, and protected unless it is supported by solid counterintelligence practices. Counterintelligence, sometimes described as the "skunk at the party," is often resisted by intelligence officers troubled by its innately mistrustful and skeptical approach. As former Chief of CIC Jim Olson has remarked: "There's a natural human tendency on the part of both case officers and senior operations managers to resist outside scrutiny . . . when necessary, a CI service has to impose itself on organizations and groups it is assigned to protect."[14] Considering the high stakes in the war on terrorism, it is time for counterintelligence to impose itself now. (U)

[14] James Olson, "The Ten Commandments of Counterintelligence," *Studies in Intelligence* 45, no. 3, 2001: 57–58. (U)