Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control

Gaetano Joe Ilardi
Published online: 12 Mar 2009.

PLEASE SCROLL DOWN FOR ARTICLE

Routledge
Taylor & Francis Group

GAETANO JOE ILARDI

Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control

It is up to the leadership and individuals to make continuous effort to reach a perfect security image that could achieve the required target. It is up to each group to keep developing and innovating security measures that suit the development of the enemy's abilities to benefit from previous trials and renewed experiences and to be familiar with whatever is new with regards to the opposing security of the group's movement.[1]

Among the reasons for success as well as the reasons for failure at the same time is the security factor. The more care and importance Islamic groups...give to this aspect, the more successful and powerful they will be, and conversely, the less care they give to this aspect...the more it will bring about failure and loss to the group and its people.[2]

The challenges facing intelligence collection against al-Qaeda, and the raft of other groups it has spawned or inspired, are formidable. Functioning as a social or cultural network, al-Qaeda, like most other *jihadi* groups, has an integrated vetting mechanism which ensures that recruitment, promotion, and the assignment of tasks are based on displays of religious devotion, loyalty, and trust. These measures are in turn complemented by a series of counterintelligence practices that emphasize deception, concealment, and camouflage.

From the earliest stages of an al-Qaeda operative's association with the organization, he is constantly reminded of the dangers inherent in his operating environment. This is often emphasized within the context of

Dr. Gaetano Joe Ilardi, a serving police officer with Victoria Police, Australia, is also a Postdoctoral Research Fellow with the Global Terrorism Research Centre, Monash University, Melbourne, Australia.

counterintelligence, where lax security procedures are equated with threats of the highest order.[3] Operational success and organizational survival, it is stressed, can come only through strict observance of the organization's rules of security and deception, based on a thorough and detailed knowledge of the enemy's methods of operation.

Al-Qaeda's extensive use of counterintelligence tradecraft is intended to create an impenetrable security umbrella around every aspect of its activities, regardless of their apparent triviality. The construction of a security plan is, therefore, meant to disguise each element of an operation, ranging from the acquisition of weapons to the collection of intelligence. This methodical approach to counterintelligence is revealed in al-Qaeda's operational manual, *Declaration of Jihad Against the Country's Tyrants* (hereinafter, *The Declaration*), which explains that planning for an operation requires "...a careful, systematic, and solid security plan to hide the operation from the enemy until the time of its execution...".[4] Other al-Qaeda instructional guides reiterate this edict, emphasizing the importance of implementing thorough security measures before conducting an operation.[5]

At the heart of al-Qaeda's counterintelligence effort lies the simple yet effective principle: activity should proceed only with the knowledge that it is safe to do so. In other words, defense should always precede offense to ensure that plans can be made with complete confidence that events will unfold as planned. Secrecy and surprise are understood to be vital assets if the terrorist group is to redress the problem of successfully challenging a power asymmetry.

ORGANIZATIONAL VIEWS ON COUNTERINTELLIGENCE

The perils inherent in al-Qaeda's operating environment form the basis of its commitment to the principles of counterintelligence. The world's ongoing counterterrorism effort against al-Qaeda is unparalleled in its magnitude, allocation of resources, and level of international cooperation.[6] The hazards for al-Qaeda are exacerbated by the nature of its operations, which have proven both ambitious and complex. Extensive planning and logistical preparations have been required, along with the direct involvement of a large number of operatives. Al-Qaeda's efforts contrast sharply with those groups such as the Irish Republican Army (IRA), where the number of men involved in an operation was usually less than five. For these reasons, the potential to manifest indicators of an impending operation are significantly greater for al-Qaeda than they are for most other terrorist groups. Additionally, al-Qaeda conducts its operations in exceptionally hostile environments, isolated from a secure base where it exerts strong control or commands the respect and sympathy of a large part

of the population. Surrounded by enemies rather than sympathizers, lapses in counterintelligence protocols are more likely to end in operational failure.

These organizational and operational traits, along with the asymmetric nature of the conflict in which it is engaged, have, therefore, made secrecy intrinsic to al-Qaeda's method of operations. In his 1996 *fatwa*, Osama bin Laden acknowledged the relationship between this type of conflict and the need for operational security, observing, "[d]ue to the imbalance of power between our armed forces and the enemy forces, a suitable means of fighting must be adopted, i.e., using fast-moving light forces that work under complete secrecy."[7]

The Impact of Lapses

Moreover, exposure, frequently stemming from minor lapses in operational security, can have wide-reaching consequences for the organization. For instance, the frequent capture of al-Qaeda operatives has taken a significant toll on the organization, revealing the existence and identity of other operatives, including highly-valued support structures. The arrest of an operative in one country has frequently led to the arrest of operatives and the disruption of cells in other parts of the world. For example, the arrest of Qari Saifullah Akhtar in the United Arab Emirates in August 2004 led to various raids in Great Britain, and subsequently uncovered al-Qaeda surveillance material of targets in the United States. Similarly, the arrest in Pakistan of Ahmed Khalfan Ghailani and Mohammed Naeem Noor Khan at approximately the same time resulted in the arrest of a dozen suspects in Britain and intelligence that led to a terror warning in the United States. Security forces have also extracted high-grade intelligence from captured senior al-Qaeda operatives such as Khalid Sheikh Mohammed, Abu Zubaydah, and Ramzi Binalshibh, which has been used to identify previously unknown suspects, the location of known suspects, the role of operatives in past operations, pending operations, and al-Qaeda's methods of operation. Similarly, the confessions in 2002 of Omar al-Faruq, al-Qaeda's senior representative in Southeast Asia, revealed details of the organization's internal functioning and its relationship with terror groups in that region.[8] Successes of this sort can also be used for counterterrorist propaganda, which al-Qaeda admits can disrupt its capacity to attract new followers.[9]

Al-Qaeda, therefore, understands the unforgiving nature of terrorist activity and the potential for even the slightest lapse in security to have catastrophic effects. Its Chief of Security, Sayf Al-Adl, acknowledged this potential, when he said,

> There is a type of error described as the first and last error because once it occurs, there is no remedy. Anyone who handles explosives, for example,

> must be an expert and aware of the safety procedures necessary for handling. We often hear that an explosive device blew up while a brother was assembling it. . . . In the sphere of security there are errors that are considered as the first and last and are, in fact, more dangerous than handling explosives without knowledge.[10]

This concern was reflected in a 1997 al-Qaeda security report which observed that ". . . anyone who studies security matters seriously will never handle anything carelessly, regardless of how small or great it is, but will take all matters seriously."[11]

For al-Qaeda, counterintelligence is thus the foundation upon which all other matters and activities rest. Detailed and robust security measures, meant to precede and underpin each activity, are the key elements in determining operational success. *The Declaration* thus defines a "Security Plan" as

> . . . a set of coordinated, cohesive, and integrated measures that are related to a certain activity and designed to confuse and surprise the enemy, and if uncovered, to minimize the work loss as much as possible

> The more solid is the security plan, the more successful [the work] and the fewer the losses. The less solid the security plan, the less successful [the work] and the greater the losses.

This section of *The Declaration* concludes with the observation that "[t]here should be a security plan for each activity that is subject to being uncovered by the enemy."[12] The practical and psychological benefits of a robust security plan are elaborated upon by Al-Adl, who observes that its advantages include the following:

a. It achieves the principle of surprising the enemy, which is one of the principles of war to achieve victory.
b. It is by itself one of the principles of war.
c. It makes the *Jemaah* [group] fully alert to what is being planned against it and this leads the *Jemaah* to prepare to repel the enemies' strikes against it.
d. It protects the *Jemaah* from attempts to infiltrate its ranks by the enemy.
e. It lessens the losses amongst the ranks and capabilities of the *Jemaah*.
f. The absence of security leads to frustration as a result of recurrent failure of the actions that the *Jemaah* carries out.[13]

The importance of operational security has ensured that it remains among the most frequently discussed issues in al-Qaeda–related military and training literature, including its periodicals, manuals, and encyclopedias. Regular features on security and intelligence in biweeklies such as *Al-Battar Training Camp* provide advice on how to protect intelligence, how to remain anonymous during the planning and execution of operations, and techniques in the use of disguises, codes, and ciphers.

Instruction manuals address very specific aspects of security and counterintelligence. For instance, the Pakistani apartment in which Ramzi Binalshibh was arrested on 11 September 2002 contained a manual on how to avoid detection by police and intelligence services while boarding aircraft or crossing borders.[14] Al-Qaeda also encourages counterintelligence tradecraft of a more sophisticated nature, including the use of deception, disinformation, double agents, the recruitment of informers, and countersurveillance techniques.[15] These aggressive methods equip al-Qaeda with the knowledge required to devise effective defensive countermeasures and employ innovative offensive techniques of its own.

Anonymity and Secrecy

Al-Qaeda's repeated references to operational security is intended to instill a strong awareness among its members and supporters that anonymity is the most important barrier between the operative and the security services. Furthermore, it is considered an organizational responsibility, regardless of an individual's position or seniority.[16] Al-Qaeda manuals are supplemented by an extraordinary number of security-focused documents and manuals published by other groups and appearing on a range of *jihadi* Websites and chat forums.[17] Referred to by some as a "virtual Afghanistan" because of its capacity to compensate for the loss of that country as a training area,[18] Web-based forums are a highly effective means by which al-Qaeda can propagate new counterintelligence methodologies in response to the latest counterterrorist tactics employed by the world's security services. Indeed, the nonhierarchical nature of these networks is conducive to al-Qaeda's rapid dissemination of information and its ability to improve decisionmaking.[19]

Al-Qaeda has thereby developed a culture of secrecy that permeates the organization and virtually every aspect of its operations. In an environment where al-Qaeda sees enemies everywhere, everything is subordinate to security. But, this does not mean that al-Qaeda's security is impenetrable or faultless. Al-Qaeda members of all ranks and positions have been killed or apprehended because their errors violated the most basic rules of counterintelligence, notably in the reckless use of communications equipment, especially telephones. Despite repeated instructions to the contrary, al-Qaeda operatives have compromised operations either through the use of telephones, particularly cell phones, which have revealed their locations, or communicated sensitive information subsequently intercepted by technical means. For instance, Ramzi Binalshibh was located and arrested after making excessive use of his satellite phone and email.[20] Similarly, transcripts of law enforcement telephone intercepts on *jihadists* operating in Western Europe reveal their habit of communicating telephone numbers of associates during these

conversations.[21] This serious lapse in operational security provides law enforcement the opportunity to link telephones to certain individuals, intercept further conversations, and, in the case of mobile phones, pinpoint the location of the handset.

These failures are a reminder of the importance of counterintelligence, and the perils involved in not taking appropriate security precautions. Security failures can occur even when operatives are convinced that their counterintelligence protocols are robust and conform to the organization's standards.

AL-QAEDA'S COUNTERINTELLIGENCE DOCTRINE

The essence of al-Qaeda's counterintelligence doctrine reflects its broader organizational philosophy, which dictates that chance has no place in the conduct of operations. By providing the most detailed and comprehensive understanding of the operating environment, and the nature of the threats likely to be encountered therein, this doctrine is intended to minimize situations in which the al-Qaeda operative is unprepared or ill-informed. This principle can be found in the organization's dual approach to counterintelligence.

Attention to Detail

Implicit in al-Qaeda's approach to counterintelligence is the acknowledgment that almost every act performed by the organization and its operatives involves some risk. Every act has the potential to betray indicators that could expose the group and its intentions. Each telephone call, meeting, attempt to acquire materials, and interaction with individuals outside the group is fraught with danger. Al-Qaeda also understands that a lapse in only one of these areas may be sufficient to expose an entire operation and all those involved. An eye for detail has, therefore, become one of the hallmarks of al-Qaeda's counterintelligence strategy, reinforcing the attitude among members which dictates that nothing should be left to chance.

Indeed, al-Qaeda's security philosophy encourages an almost mechanistic approach among operatives. The delivery of instructions and information, through a process characterized by rote repetition, is designed to instill in operatives something akin to an instinctive response to circumstances that require the implementation of security measures. Detailed step-by-step security instructions, designed to carefully guide operatives through an array of situations, ensure a methodical and conditioned response. This detail reinforces the need to exert a strong measure of control over the operative's environment, especially on all matters pertaining to security.

Indeed, the operative is provided advice on virtually every form of behavior that might draw unwanted attention. For instance, al-Qaeda's is known to have issued instructions even on the type of underwear that should be worn, on which wrist to wear a watch, and the type of antiperspirant to be used.[22] Instructions revealing similar attention to detail are evident in *The Declaration*, *Al-Battar Training Camp*, and a range of other instructional documents. Al-Qaeda's operational philosophy of establishing a robust and meticulous counterintelligence regime from the inception of an operation, and for each subsequent activity associated with it, creates a protective cloak that is difficult to penetrate.[23]

''Know Thy Enemy''

The essence of al-Qaeda's counterintelligence doctrine is encapsulated in the notion of "know thy enemy," which has been extended to include the maxim "study thy enemy." Al-Qaeda understands that its own approach to security is inextricably linked to, and determined by, the activities of those forces waged against it. The *Encyclopedia of the Afghan Jihad* (hereinafter *The Encyclopedia*) demonstrates the essence of this encounter by observing that "...the struggle between us and our enemy is a struggle of beliefs first and foremost, and then a struggle of security and intelligence."[24]

To this extent, much of al-Qaeda's counterintelligence effort is determined from its study of opposing intelligence forces and its ability to disseminate this intelligence globally. On this basis, al-Qaeda and its followers can devise suitable countermeasures that form the core of its own counterintelligence paradigm. Former U.S. Deputy Secretary of Defense Paul Wolfowitz acknowledged the importance of this doctrine in diminishing the effectiveness of the U.S. intelligence effort against al-Qaeda when he said,

> ...we should not underestimate the skill of our enemies and their determination to conceal their activities and deceive us. They understand how we collect intelligence, how we are organized, and how we analyze information. Just like them, our intelligence services must constantly adapt and innovate. Thus, we have aggressive efforts underway to find new ways to discern terrorist "signals" from the background "noise" of society, but we must also recognize that enemies will deliberately create "noise" in the system in order to conceal the real signals.[25]

Al-Qaeda's counterintelligence paradigm dictates that the detailed study of the enemy, including its methods, tactics, and assumptions, is critical for the development and maintenance of the *jihadists*' security umbrella. Counterintelligence, thus intimately linked to its intelligence function, reflects an organizational philosophy which dictates that knowledge must

be the precursor to action. This nexus between intelligence and counterintelligence is evident in the *jihadi* literature. For instance, *The Encyclopedia* observes: "He who succeeds is he who is able to obtain more information, so that their intelligence is stronger and their security tighter."[26] By carefully studying the methods of its enemies, al-Qaeda is able to identify and exploit weaknesses which improve the likelihood of operational success. Indeed, it allows al-Qaeda's planners and operatives to form expectations of the likelihood of operational success, and, therefore, whether or how to proceed in attacking a target.

Al-Qaeda's counterintelligence doctrine thus fulfills a major role through its ability to inform operatives and supporters of events in advance. By anticipating and describing circumstances likely to be encountered, operatives can adopt the necessary countermeasures. This doctrine fulfills a purpose similar to that of al-Qaeda's detailed intelligence collection on targets and its practice of conducting dry runs.[27] The following example drawn from *The Declaration* is illustrative of this approach. Provided for the benefit of *jihadists* wanting to travel to Afghanistan for training, it prepares them for the type of questions likely to be asked at each stage of their journey, thereby allowing them to formulate credible responses in advance. The elimination of surprise and uncertainty in all its forms is a key consideration in al-Qaeda's decisionmaking process (Figure 1).

This same philosophy is apparent in most *jihadi* instructional documents, regardless of their source. For instance, one Islamist forum posted a series of letters from a terror suspect who escaped from a U.S. prison in Afghanistan in July 2005. These letters describe in considerable detail U.S. arrest and interrogation methods, along with the type of information interrogators are seeking. Similarly, another *jihadist* site released a detailed manual on interrogation entitled, *How to Confront and Cope with Intelligence Agency Interrogation*. It, too, provides a description of interrogation methods the *mujahidin* are likely to confront, along with suggested counter-interrogation techniques. The manual observes that a greater understanding of these methods brings more likelihood of defeating them.[28]

Moreover, the psychological dimension of this analysis provides a demonstration that al-Qaeda's enemy, despite its size and strength, can be defeated. More recently, this intention was demonstrated in such documents as Muhammad Khalil al-Hakaymah's *The Myth of Delusion*.[29] First appearing on Islamist Internet forums in 2006, this thoroughly researched document provides insightful analysis identifying the vulnerabilities and strengths of the U.S. Intelligence Community. Devoid of doctrinal or rhetorical language, the 150-page document presents a lucid and rational discussion, based on extensive use of open source intelligence, to provide sufficient information to encourage caution, while

Example of a security plan for an individual mission
(training in Afghanistan):

Prior to Departure: Traveling through an airport, the brother might be subjected to
interrogation. It is essential that he be taught the answers to the following anticipated
questions:

    A.   What are the reasons for your travel?
    B.   How did you get the money for travel?
    C.   How long is the travel period?
    D.   Who will meet you in the arrival country?
    E.   What will you be doing in the arrival country?

(There are different degrees of interrogation)

During Travel (transit country): The brother should be taught the answers to the
following questions:

    A.   Why are you going to Pakistan?
    B.   Do you belong to any religious organizations?
    C.   How did you get the travel money?
    D.   Who got you the visa to Pakistan?
    E.   What will you be doing in Pakistan?
    F.   With whom will you be staying in Pakistan?

Arrival Country (Pakistan): The brother should be taught the answers the following
questions:

    A.   Why did you come to Pakistan?
    B.   How long will you be spending in Pakistan?
    C.   With whom will you be staying?

Transit Country (Return): The brother should be taught the answers to the following
questions:

    A.   What were you doing in Pakistan?
    B.   Are you a *Jihad* fighter?
    C.   Do you belong to religious organizations in your country?
    D.   Why did you come to our country in particular?
    E.   Whom will you be staying with now?
    F.   How long will you spend here?

Return Country (Returning to your Country):

    A.   What were you doing in the transit country?
    B.   Addresses and telephone numbers of those who hosted you during your
          stay?
    C.   Whom did you visit in your group, and for how long?

When Your Travel to Pakistan Is Discovered:

    A.   What were you doing in Pakistan or Afghanistan?
    B.   In which camp were you trained?
    C.   Who trained you? On what weapons were you trained?
    D.   Who assigned you to go to Afghanistan?
    E.   Whom will you contact in your country?
    F.   What are the tasks and missions that you intend to execute in your
          country?
    G.   Who else trained with you in Afghanistan?
    H.   How many of your countrymen are in that camp and in Afghanistan?
    I.   What are their names?
    J.   Who are the group commanders there [in Pakistan]? Where do they live
          and what do they do?
    K.   What things do the commanders talk about?

Source: al–Qaeda, *The Declaration*, pp. 58-59

Figure 1. Sample Al-Qaeda Security Plan.

simultaneously dispelling perceptions of U.S. intelligence as an omnipotent and ubiquitous force incapable of being defeated. A similar rationale is evident in the magazine *Technical Mujahid (Al-Mujahid al-Taqni)*. A bimonthly released for the first time in late 2006 by the al-Fajr Information Center, its editor-in-chief, Abu al-Mothanna al-Najdi, describes the magazine's objectives as eradicating "the phobia and anxiety suffered by those who refrain from participating in jihad because they erroneously believe that intelligence services are monitoring their every move."[30]

Learning and Teaching

In its pursuit of intelligence capable of offering new insights into the methods of its enemies, al-Qaeda has adopted the characteristics of a learning organization.[31] Al-Qaeda's adaptive and generative learning styles are particularly relevant to, and apparent in, its approach to counterintelligence. In this regard, the organization has shown itself adept at learning from the experiences of others, regardless of their political or religious orientation. For example, its followers are encouraged to tap into the experiences of *jihadists* throughout the world, in particular those who may have come into contact with foreign security services. Such individuals will be able to impart knowledge on the methods of their captors, while also revealing their own operational mistakes. In an issue of *Al-Battar Training Camp*, Al-Adl captured the essence of this approach, saying,

> [a] Muslim should be constantly alert and vigilant to deprive the enemy of the element of surprise.... For security alertness to be of the highest degrees the Muslim should continuously acquire the information which would be useful for his work, particularly that which pertains to the actions of the Muslims and their news in all of the Muslim countries. He should also read useful books and develop his education in this field. We affirm ... the necessity of exchanging information with your brothers everywhere; they ask you and you ask them: How were they arrested and what were their mistakes? What were the hiding places that the enemy discovered? What information do you have about the enemy.... Also, with the brothers who recently got out of prison, what did they say and what did they do? For all these issues polish the experience and expand the horizons and make you alert and vigilant.[32]

Learning from the past is a strong theme evident in the *jihadists'* military doctrine, reflecting an evolutionary process designed to prolong the survival of the movement and enhance its efficiency. In addition to lessons provided by historic Islamic figures, lengthy documents on the experiences of past *jihads* continue to appear on *jihadi* forums. Among the most comprehensive and well-known of these comes from al-Qaeda's senior

ideologue, Abu Mus àb al-Suri,[33] in his sixteen-hundred-page, *Call of the Global Islamic Resistance—Guide to the Jihad Way* . Similar studies have surfaced which attempt to catalogue the lessons learned from U.S. operations in Afghanistan and how this knowledge might be applied by those involved in the Iraq insurgency.[34]

Studying the methods of its enemies not only instructs the organization on the type of countermeasures it needs to deploy, but also provides experiences considered worthy of emulation. For example, *The Declaration* points out that Israel's Mossad was able to defeat a Palestinian plan to assassinate the then–Israeli Prime Minister, Golda Meir. The example was intended to demonstrate the importance of observation and analysis in identifying and neutralizing threats.[35] Drawing on the experiences of others, including another previous Israeli leader, Menachem Begin, himself a revolutionary, is evident in other al-Qaeda manuals.[36]

Al-Qaeda's counterintelligence doctrine, therefore, provides strong evidence of its ability to act rationally. It demonstrates a desire to acquire a sufficiently detailed knowledge of its adversaries so as to identify and exploit their vulnerabilities and maximize the likelihood of operational success. This doctrine also has a symbolic utility. With its strong emphasis on defining the enemy, it helps to reinforce images of a dichotomy based on notions of good and evil. By defining and describing the enemy in minute detail, along with the seriousness of the threat it presents, al-Qaeda's counterintelligence doctrine reinforces notions of a cosmic struggle between good and evil, belief and unbelief. The ability to construct such images is fundamental to al-Qaeda's grand design.[37] Moreover, the potential for such images to strengthen group cohesion can, in turn, further reinforce what Mark Juergensmeyer has described as a ''dichotomous opposition on an absolute scale.''[38] Indeed, studies on terrorism provide strong evidence that the dangers inherent in the terrorists' operating environment, and the resulting need for them to become more secretive, can significantly strengthen group cohesion and perceptions of good and evil, based on a rhetoric of "us versus them."[39]

But while these studies show how such conditions can lead to increased group cohesion, they also contend that they distort reality.[40] Yet, my previous analysis demonstrates that the opposite may be true. While such cohesion can lead to a more insular existence, in which group and individual perceptions of the larger struggle and its rationale are rarely challenged, and are presented in a highly dichotomous form, the terrorists can ill afford to allow such distortions to extend to their operational environment. Al-Qaeda's counterintelligence doctrine provides compelling evidence of its response to perceptions of risk characterized by a strong need to acquire a highly detailed and accurate image of its adversaries. Through a desire to attain empathy-like knowledge, this doctrine reveals a

commitment to learning and understanding which contrasts sharply with arguments of risk and danger leading to distortions of reality.[41] Indeed, this understanding is a critical function in al-Qaeda's various counterintelligence strategies.

AL-QAEDA'S COUNTERINTELLIGENCE STRATEGIES

Each of al-Qaeda's security strategies is underpinned by its counterintelligence doctrine. These strategies of deception and both passive and aggressive counterintelligence practices combine to provide a high level of operational resilience and certainty.

Deception

As noted earlier, al-Qaeda has acquired, and sought to impart to its operatives, a level of understanding of the West akin to empathy.[42] In its attempts to refine its own counterintelligence tradecraft and allow its operatives to pass unnoticed in the West, al–Qaeda has developed an insight into what it considers to be the Western mindset. This includes developing an understanding of ''Occidental'' beliefs and values, behavior patterns, culture, and historical development. For al-Qaeda, this has distinct operational advantages, allowing its operatives to exploit vulnerabilities and manipulate Western perceptions of reality. For instance, al-Qaeda strategists and trainers have relied upon the West's stereotypical view of the Islamic extremist to avoid detection. Indeed, within counterintelligence circles, the most successful form of deception is that which amplifies its target's own preconceptions.[43] By encouraging its members not to engage in behavior normally expected of Muslims, al-Qaeda hopes to exploit the West's preconceived notion of how an Islamic extremist is meant to look and behave.

These methods of deception are sanctioned according to the Islamic principle of *taqiyya*, originally a practice peculiar to the Shi'a, but whose use is now widespread among Islamists of various persuasions.[44] In Islamic law, *taqiyya*, or dissimulation, not only sanctions deception, but even makes it a religious obligation in defense of the faith.[45] Fundamental to this principle is the notion of not appearing to be religious in order to avoid persecution or imminent harm.[46] This principle, therefore, emphasizes the concealment rather than the abandonment of a *jihadist*'s religious beliefs through deception and lies. Al-Qaeda has, therefore, found in *taqiyya* a counterintelligence tool that allows it to jettison those aspects of Islam that might endanger its activities or its operatives. The permissibility of lying and deception during times of war is reinforced through training manuals such as *The Encyclopedia*, which observes that ''. . . war is deception, and as soon as it is declared, then there is no truth between militants.''[47]

Al-Qaeda's use of deception, especially when it involves the suspension of an operative's religious belief, and includes a call for behavior contrary to deep ideological views, suggests a grasp of reality at odds with notions of the metaphysical. Placing the organization's operational needs ahead of ideological zeal, albeit temporarily and deceptively, indicates an ability to order priorities and postpone hostilities in the interest of whatever security requirements are deemed fundamental to operational success. It also demonstrates a level of instrumental aggression, characterized by a deliberate and calculating approach to operations, rather than mere hostile aggression involving impulsive and emotional outbursts of violence.[48]

Maintaining this deception is a central component of al-Qaeda's counterintelligence strategy, as evidenced in an array of activities. For instance, *The Declaration* instructs undercover members to "have a general appearance that does not indicate Islamic orientation (beard, toothpick … small Koran)."[49] Furthermore, it directs members to avoid places frequented by Muslims, including mosques and Islamic fairs, while also recommending a non-Muslim appearance when renting apartments. Manuals found on the computer of Ayman al-Zawahiri, al-Qaeda's second-highest official, also demonstrate the importance the organization attaches to this notion of personnel assimilation, providing detailed guidelines on Western behavior and appearance.[50] Al-Qaeda members were advised, when traveling through airports, to pack cologne and packets of cigarettes, believing that these items would divert customs suspicion due to their being considered *haram*.[51] Mohamed Sadeek Odeh, who was linked with the al-Qaeda East Africa cell responsible for the U.S. Embassy bombings in 1998, explained that its members often shaved before traveling to avoid the attention of customs officials. He admitted that he shaved off his beard as he was making preparations to leave Kenya several days before the bombing.[52]

Learning to imitate the behavior of Westerners has even been part of the training delivered in al-Qaeda camps in Afghanistan. A recruit described how "[t]hey train us here on how to mix with the Christians and how to emulate their life style. We have to learn how to drink alcohol and to shave off our beards."[53] Islamists have even been known to dye their hair and wear blue contact lenses in order to appear "European."[54] Disinformation is also encouraged in order to support cover stories, with one al-Qaeda–prepared encyclopedia suggesting the adoption of counterintelligence techniques similar to those used by the former Soviet Union's KGB. In this instance, operatives are instructed to plant false evidence for the enemy to find that corroborates their cover story.[55] An Al-Qaeda–trained operative, Ahmed Ressam, also provided evidence that he was instructed by one of his co-offenders to leave misleading evidence at crime scenes to confound and delay police investigations. For instance, with regard to armed robberies

used to raise funds for terrorist activities, Ressam was advised to leave the syringe of a drug addict at the scene, so that the user's fingerprints would impede subsequent investigations.[56]

For similar reasons, al-Qaeda has demonstrated a keen interest in recruiting members who do not conform to the Occidental stereotypes of the Islamic extremist. The recruitment of citizens from Western countries has, therefore, been a high priority for al-Qaeda for some years. Indeed, al-Qaeda's former operational commander, Mohammed Atef, in reference to utilizing Caucasian operatives, informed Australian terrorist Jack Roche[57] that it was better "to make use of material that's available in the country rather than try and send people in because everyone was looking for people of Middle Eastern appearance."[58] Al-Qaeda is also known to have sent dark-skinned operatives into African countries such as Somalia for similar reasons.[59]

Deception and subterfuge have other operational applications. The use of props to provide a cover for its operations is quite common. For instance, al-Qaeda has, on numerous occasions, impersonated security personnel in order to facilitate access to targets. Specialty vehicles, such as ambulances and police vehicles, have also been used to great effect. In the November 2003 attack on a housing compound in Riyadh, access to the compound was facilitated after the attackers posed as security personnel driving a vehicle that resembled a police car.[60] Similarly, al-Qaeda has used police vehicles to mount security checkpoints in Saudi Arabia to abduct and kill Westerners. U.S. engineer Paul Johnson was abducted and subsequently executed under these circumstances in June 2004.[61]

Passive Counterintelligence

Al-Qaeda's ability to achieve surprise and operate under conditions of its own choosing is directly dependent upon its concealment of indicators that might reveal the existence of some activity. This, of course, does not have to relate exclusively to activity in preparation for an impending operation. Al-Qaeda, like other terrorist organizations, must engage in behavior that supports a range of goals, and this may include fund-raising, publicity, recruitment, and training. But these activities must also be concealed because they have the potential to reveal the identity of members, methods of operation, and locations and sources of assets. Importantly, they may also act as reliable indicators of impending operational activity. For this reason, al-Qaeda's counterintelligence strategy aims to construct a detailed and thorough security plan relating to each activity undertaken by itself and its operatives. In addition to deception, al-Qaeda's use of passive counterintelligence is designed to suppress these indicators by creating a barrier that either conceals or camouflages its activities.

Detailing all the passive counterintelligence methods used by al-Qaeda, would require a volume of its own. Nevertheless, some of the most important can shed light on the organizational thinking behind them.

(a) *Recruitment and training.* As a clandestine organization, al-Qaeda's most fundamental obligation is to conceal the identity of its members and supporters, thereby providing a strong foundation upon which its future security measures can rest. Thus, from the moment new al-Qaeda recruits enter training camps, including the process by which they are recruited, to the time they engage in actual operations, a priority of the highest order is the need to conceal their identities through the use of passive counterintelligence measures.

For instance, upon entering training camps, recruits are immediately assigned an alias, and all forms of personal identification are removed.[62] From this point on, trainees know each other only through the use of aliases; real names are never used. A common method is to refer to a person on the basis of his country of origin—pseudonyms such as Abu Bakr Sudani (Sudan), Saif al Liby (Libya), and Abu Fadhl al Makkee (Mecca, Saudi Arabia) are typical for those entering the training camps. Similarly, recruits receive their training as members of smaller groups, the composition of which is frequently determined by nationality. The expectation is that these groups will subsequently form the basis of cells. In this way, the integrity of cell membership can be guaranteed at the most critical stage of an operation.[63]

Techniques of deception and disinformation have also been employed within the camps to conceal the identities of high value recruits. For instance, Jack Roche informed me that Sayf Al-Adl had instructed him that, while training at an al-Qaeda camp outside Kandahar, Pakistan, in 2000, he was to inform other recruits that he was from England, not Australia. Furthermore, Roche was accommodated separately from the other trainees to protect his identity. Roche's potential value and distinctiveness served as the rationale for these additional security measures.[64] The use of deception and the adoption of aliases, nicknames, and *kunyahs* offers al-Qaeda's operatives an additional layer of protection from law enforcement and security service surveillance and penetration. The use of fraudulent documents, such as passports and drivers licenses for "backstopping," adds a dimension of legitimacy to the assumed names.

These camps also place considerable emphasis on operational security. The preservation of secrecy and the concealment of members' identities and operational details were given the highest priority.[65] The "need to know" principle was emphasized throughout. Ahmed Ressam recalls being told "...when you work in a group, each person knows only what he is supposed to do, not more, to preserve your secrets." Furthermore, he recounts how he received lectures on counterintelligence, although these

appeared to be fairly elementary and designed to instill a security consciousness consistent with their clandestine existence.[66] In this environment, recruits also receive instructions on the practical aspects of operational security, including how to create a cell, and to not engage in sensitive conversation within the confines of a building.[67]

The camps themselves have also become an effective way of vetting new recruits. Consistent with the practices of the world's intelligence services, al-Qaeda's counterintelligence function was frequently performed by its intelligence apparatus. The intelligence office sometimes carries out the vetting of new or unfamiliar members. This can consist of an interview in which various aspects of the person's background are tested, including geographic areas in which he may have fought while in the military, and those camps in which he may have trained.[68]

(b) *Communications*. Ensuring secrecy in communications is a major operational priority for al-Qaeda. The global nature of its activities, whether as an organization heading an international network of like-minded groups or not, requires it to communicate over great distances and with considerable frequency. The extent of its communication needs has been well documented.[69] But it must balance this operational need with the risks inherent in communications. *The Declaration* specifically expresses this predicament for the operative: "It is well known that in undercover operations, communication is the mainstay of the movement for rapid accomplishment. However, it is a double-edged sword: It can be to our advantage if we use it well and it can be a knife dug into our back if we do not consider and take the necessary security measures."[70] Security in communications represents a second line of defense, and is indicative of al-Qaeda's layered approach to counterintelligence.

Al-Qaeda's strategy to ensure secure communications rests on its ability to provide accurate and timely information to its members and supporters about their own vulnerabilities. By examining the methods most commonly used by various security services to detect enemy communications, it is able to devise countermeasures. The use of training documents with titles such as "How does the state monitor telephone lines?" provides its operatives with comprehensive insights into police and intelligence methods.[71] For example, the al-Qaeda operative is provided details on the type of information typically captured each time a telephone call is made, including the receiving number, duration, and, in the case of mobile telephones, the location. The document includes case studies that provide a step-by-step description of the methods used by the security services to identify and locate suspects through the analysis of telephone traffic.

Where or when avoiding the use of communications methods discouraged by al-Qaeda's tacticians and strategists is not possible, its operatives have developed measures capable of negating the monitoring capabilities of the

security services. For instance, al-Qaeda's extensive use of codes in its communications has become a standard method of operation among *jihadists*, including those that operate in small, self-contained units acting independently of larger groups or organizations. In addition to concealing the true nature of *jihadists* activities, code words make more difficult security attempts to secure prosecutions against those apprehended and charged for plotting acts of terror. The burden of proving intent is complicated by the ambiguity inherent in the use of code words, which, by and large, are designed to convey innocuous meaning and intent. Cognizant of the possibility that the security forces can decipher codes over time, al-Qaeda has also been known to change its code words at regular intervals, especially at critical junctures of an operation's development. Ramzi Binalshibh, the coordinator for the 9/11 attacks, observed, "[E]ach phase has a language of communication that differs from the following one; and before each phase, a meeting takes place and an agreement is reached over this language."[72]

Some of the communication protocols employed by al-Qaeda, especially those involving its senior leadership, have been revealed by Jack Roche who was convicted in 2004 of conspiring to bomb the Israeli embassy in Canberra, Australia, in 2000. These protocols ensured that, by the time Roche returned to Australia in mid-2000, his movements were not known to the security services of a number of countries, despite the fact that he was in contact with some of the world's leading terrorists (Figure 2).

(c) *Cover*. A key element to al-Qaeda's counterintelligence protocol, and one common to most *jihadi* groups, is to avoid suspicion by acting inconspicuously in public and avoiding behavior commonly noticed in counterterrorism profiling. Considerable effort is invested in this attempt to achieve assimilation because of its capacity to provide a cover that lends the organization and the operative both legitimacy and anonymity. *The Encyclopedia* defines "cover" as "...the external appearance used by an individual or a group to conceal the true nature of the secret mission, and to hide their activities from the enemy's security forces. The cover is the public story that hides the actual secret mission."[73] In addition to deception to assist with cover, al-Qaeda employs a range of passive counterintelligence methods for this purpose.

The establishment of business and charitable fronts, the creation of falsified documents to support assumed identities, and the adoption of innocuous physical and behavioral characteristics are common techniques used by al-Qaeda. Constructing credible and convincing cover allows an operative to function in an otherwise hostile environment in safety and with confidence. For instance, the 9/11 hijackers assumed a temporary American identity before they embarked on the more risky elements of

The decision to send Roche to an al-Qaeda training camp came in early 2000 after the al-Qaeda leadership wished to explore the possibility of forming a cell in Australia that could attack Israeli targets in that country. It was specifically requested that this person be Caucasian. This desire was communicated to al-Qaeda's South East Asian representative, and senior JI member, Hambali, by some unknown means, but likely involved the use of a human courier. Hambali, in turn, passed this request onto the JI leadership in Australia, the Ayub brothers, who were expected to nominate a suitable candidate. After being nominated by the Ayubs, Roche telephoned Hambali from Australia on a number provided to him by the Australian JI leadership. He was then dispatched to Malaysia, where he met with Hambali, who provided Roche further instructions to travel to Pakistan where he was expected to meet Khalid Sheikh Mohammed. He was also given a letter of introduction for this purpose. Roche then traveled to Pakistan where, at Karachi Airport, he was met by two men associated with Khalid. Taken to a safe house, Roche was met there the following day by Khalid, who questioned Roche about Israeli targets in Australia. After providing Roche another letter of introduction, this one apparently intended for Osama bin Laden, Khalid instructed Roche to travel to Quetta. Roche subsequently traveled to Quetta by bus with several other males. Upon his arrival in Quetta, one of Roche's traveling companions reported to the Taliban, which had a safe house in the city. Several days later, a Taliban representative collected Roche and conveyed him over the Afghan border. From there, he was taken to an al-Qaeda camp outside Karachi, where his letter from Khalid was provided to an unknown person within the camp. Shortly thereafter, Roche met with senior members of al-Qaeda, including Abu Hafs and Sayf al-Adl, who instructed him to conduct surveillance of Israeli targets in Australia and to form a small cell. On the day of his departure from the camp, Abu Hafs provided Roche with another letter intended for Khalid. This letter contained instructions for Khalid to provide Roche with US$8,000 to enable him to undertake the duties assigned to him. After traveling back to Karachi, Roche contacted Khalid at a mobile telephone number provided to him during their first meeting. After handing him Abu Hafs's note, Khalid provided Roche with approximately half the US$8,000. Khalid provided Roche another note that he was to give to Hambali in Malaysia. On receipt of this note, Hambali eventually provided Roche the remainder of the US$8,000. At this point, Roche returned to Australia where he commenced his surveillance of Israeli targets as instructed.

Source: Jack Roche, interview with author, 25 and 26 August 2005

Figure 2. Sample of al-Qaeda's Communications Methodology.

their operation, such as searching for aviation schools and learning to fly.[74] Similarly, al-Qaeda had an entrenched presence in Kenya in the years leading to the 1998 embassy bombings. This provided the operational and support cells the cover they needed to conduct their clandestine activities. For example, Mohamed Sadeek Odeh established an al-Qaeda–funded fishing business in Kenya as early as 1994 that was ultimately used to provide a

cover for various operational activities undertaken in support of the East Africa cells,[75] while Wadih al Hage established a charity organization to provide al-Qaeda members with identity documents.[76]

Aggressive Counterintelligence

In the area of aggressive counterintelligence, al-Qaeda has demonstrated a level of sophistication and tradecraft reminiscent of the counterintelligence techniques traditionally utilized by the world's top intelligence services. Al-Qaeda's capacity to penetrate security and intelligence services is a significant measure of its aptitude for, and dedication to, intelligence collection. For al-Qaeda strategists, the infiltration of hostile security and military services is an issue of vital importance. Since counterintelligence efforts are directed against other intelligence threats, these successes amount to major intelligence coups for al-Qaeda, while representing intelligence failures of the highest order for the targeted services. Furthermore, the insertion of intelligence assets within enemy ranks, or their recruitment as agents, is a strong indication of al-Qaeda's need for intelligence capable of minimizing operational risk by determining the intentions, capabilities, and methods of those organizations intent on its destruction.[77] Al-Qaeda's preference for recruiting or inserting moles and agents into hostile military and intelligence services is indicative of the tremendous value the organization places on intelligence that strengthens its counterintelligence protocols. Consistent with an ideological outlook that emphasizes the long-term nature of their struggle,[78] *jihadists* understand the importance of patience and the need for a strategic view on matters relating to aggressive counterintelligence. While the effort required for such penetrations can be considerable, and is unlikely to produce immediate results, the benefits can ultimately be immense. Abu Bakr Naji, considered one of the *jihadi* movement's most important strategists in the post 9/11 period,[79] observed in his work, *The Management of Savagery*, that the infiltration of organizations capable of enhancing the movement's security position should remain a major priority. According to Naji,

> Our battle is long and still in its beginning....Its length provides an opportunity for infiltrating the adversaries and their fellow travelers and establishing a strong security apparatus that is more supportive of the security of the movement now, and later the state. We should infiltrate the police forces, the armies, the different political parties, the newspapers, the Islamic groups, the petroleum companies (as an employee or as an engineer), private security companies, sensitive civil institutions, etc. That actually began several decades ago, but we need to increase it in light of recent developments.[80]

In Naji's view, the value of infiltration is such that *jihadis* chosen to perform this duty should be told that its importance is equal to that of a martyrdom operation.[81]

The aggressive counterintelligence activities of al-Qaeda and other *jihadists* are well-documented. The following cases provide some indication of the nature and scope of these penetrations.

Late 1980s United States. Actively involved with Egyptian Islamic Jihad from the early 1980s, Ali Mohammed also held various positions within al-Qaeda, including that of senior instructor, security coordinator, and intelligence officer.[82] Mohammed, who had earlier served as an intelligence officer in the Egyptian Army, enlisted in the U.S. Army, where he served as a supply sergeant with the Special Forces at Fort Bragg before being discharged in 1989. Mohammed used his position to acquire classified U.S. Army documents that were subsequently found in the home of one of those convicted in the 1993 World Trade Center bombing.[83] Mohammed also reportedly applied for a job as a Federal Bureau of Investigation (FBI) translator, a position that would have granted him access to some of the FBI's most sensitive counterterrorism operations.[84] Mohammed's attempt to infiltrate the FBI is indicative of an understanding of how counterterrorist investigations are conducted. He seems to have understood that Arabic translators would have access to some of the largest and most sensitive counterterrorist operations conducted by the FBI. Translations would most commonly be required on evidence and intelligence gleaned by covert technical means, such as listening devices and telephone intercepts. This would have placed Mohammed in an ideal position to alert al-Qaeda about investigations into its U.S.-based, and possibly overseas, operations. Similar attempts to infiltrate Western intelligence services by exploiting their campaigns to recruit and employ much needed Arabic and Urdu translators continue to the present day.[85]

2003 Yemen. Yemeni security forces arrested senior al-Qaeda member, Mohammed Hamdi al-Ahdal, who is believed to have played a central role in the bombings of the USS *Cole* in 2000 and the French oil tanker *Limburg* in 2002. Al-Ahdal, also known as Abu Assem al-Makky, was at the time of his arrest in the process of forming small, independent cells aimed at infiltrating Yemeni security, and gathering intelligence to frustrate the Yemeni government's attempts to capture wanted militants.[86]

2003 Australia. French national Willie Brigitte entered Australia for the suspected purpose of attacking a military base in Sydney. Believed to be a member of LeT, with further links to al-Qaeda, Brigitte married an Australian, Melanie Brown, a recent Muslim convert and former Australian Army signals officer. Whether Brigitte married Brown because of her military background is unclear, but he showed intense interest in her

former military activities following their marriage. Indeed, he asked Brown to write down those activities in which she had participated during her time in the army, explaining that ''God and Muslims needed this information.'' She became so concerned about Brigitte's interest in her activities that she burned three notebooks that she maintained during her time in the Army. When Brigitte learned that his wife had destroyed her notebooks, he forbade her to destroy any other documents relating to her past without his approval.[87]

Moles, or those merely sympathetic to the *jihadists*' cause, are thus ideally placed to provide an additional layer of security to al-Qaeda and its supporters. Through their ability to warn operatives of impending arrest or covert operations, moles and well-placed sympathizers may be of assistance where the *jihadists*' otherwise passive counterintelligence measures have failed. For instance, a missed opportunity to arrest Khalid Sheikh Mohammed in Qatar in 1997 likely resulted from a leak from within the Qatari security services or the Emir of Qatar's immediate circle.[88] The presence of moles or sympathizers in sensitive positions can also provide the type of intelligence needed to identify potential targets.[89]

GRASPING REALITY FOR *JIHAD*

Ultimately, al-Qaeda's use of counterintelligence provides strong evidence of a grasp on reality intended to maximize the likelihood of its achieving a range of strategic and symbolic objectives. Creating a secure operating environment as the precursor to action is the principal goal of al-Qaeda's counterintelligence activities. Its abilities in this regard can be traced directly to an unrelenting drive to uncover all it can about those forces operating against it. These counterintelligence protocols, along with the organization's commitment to building a detailed intelligence picture of the target and its surroundings, come together to provide al-Qaeda a significant measure of control over its operating environment, upon which its ability to construct and execute successful operations depends. Given the adversarial nature of that environment, al-Qaeda understands that much of the uncertainty associated with its activities is generated by the actions of the security forces. Advocating a counterintelligence doctrine that calls for a detailed "knowledge of the enemy," al-Qaeda has established the collection of information on the methodologies and practices of its foes as a major intelligence priority. In this way, the anticipated activities and reactions of the security forces can be factored into the planning process, thereby further reducing uncertainty. Indeed, *The Encyclopedia* describes a basic rule of security as ''[t]he ability to think ahead and predict the future.''[90] Ultimately, the collection and use of intelligence to support al-Qaeda's security efforts demonstrates a sophistication at odds with widespread

notions of its having a distorted and simplified worldview due to ideological zeal or the pursuit of goals considered more metaphysical than real.

Counterintelligence also has the symbolic utility of emphasizing to multiple audiences al-Qaeda's reach and power. Consistent with the organization's desire to construct perceptions of a cosmic war between good and evil, counterintelligence involves a direct, albeit covert, clash with these security forces. In a struggle in which al-Qaeda claims to be performing the work of God against the forces of evil and unbelief, operational failure has the potential to distort and blunt the impact of its political and ideological message. Successes are, therefore, likely to provide further evidence of the government's vulnerability and the relative strength and righteousness of al-Qaeda and its ideological cause. As an organization that exists and functions in isolation from its constituency and supporters, its capacity to influence and control is derived in large part from the imagery created through its acts of violence. Perceptions of power needed to mobilize and retain the loyalty of supporters must come from successful attacks that are able to inspire and encourage. Operational success, rather than fear and intimidation, is central to al-Qaeda's capacity to communicate its omnipotence and garner support and obedience. Counterintelligence is fundamental to al-Qaeda's capacity to achieve those operational victories.

REFERENCES

[1] Sayf Al-Adl, "Legal Vision," *Al-Battar Training Camp*, No. 1, 3 January 2004.

[2] *The Encyclopedia of the Afghan Jihad*, n.d., p. 7. An eleven-volume manual totaling approximately 8,000 pages, it covers a range of topics, including tactics, the manufacture of explosives, and security and intelligence. Although the identity of the author or authors of this manual cannot be stated with certainty, evidence indicates that it was compiled by the Afghan Service Bureau (*Mekhtab al-Khidemat* or MAK), a body created by Osama bin Laden and Abdullah Azzam to organize the increasing number of foreign *mujahidin* entering Afghanistan in the mid-1980s. Indeed, the first two dedications in the manual are to Azzam and bin Laden. It is also believed that the manual was compiled some time between 1991 and 1993. Full Arabic version of manual is in author's possession.

[3] Sayf Al-Adl, "The Principles of Security," *Al-Battar Training Camp*, No. 2, 15 January 2004.

[4] Al-Qaeda, *Declaration of Jihad against the Country's Tyrants, Military Series*, n.d., p. 65. This 180-page training manual was recovered in the home of al-Qaeda member Anas al-Liby in Manchester, England, in May 2000. Full copy in author's possession.

[5] Sayf Al-Adl, "Legal Vision," no. 1.

[6] Desmond Ball, "Desperately Seeking bin Laden," in Ken Booth and Tim Dunne, eds., *Worlds in Collision: Terror and the Future of Global Order* (New York: Palgrave, 2002).

[7] Osama bin Laden, *A Declaration of War Against the Americans Occupying the Land of the Two Holy Places: A Message from Osama bin Muhammad bin Laden unto his Muslim brethren all over the world generally, and toward the Muslims of the Arabian Peninsula in particular*, at http://www.pbs.org/newshour/terrorism/international/fatwa1996.html, 1996 (accessed 24 April 2005).

[8] Romesh Ratnesar, "Confessions of an Al-Qaeda Terrorist," *Time*, 23 September 2002, pp. 37–38.

[9] Sayf Al-Adl, "The Principles of Security," No. 2.

[10] Sayf Al-Adl, "The Principles of Security," *Al-Battar Training Camp*, No. 3, 2 February 2004.

[11] Haroun Fazil, "The Letter from El Hage's Computer," at http://www.pbs.org/wgbh/pages/frontline/shows/binladen/upclose/computer.html, 1997 (accessed 2 November 2004).

[12] Al-Qaeda, *Declaration of Jihad*, p. 57.

[13] Sayf Al-Adl, "The Principles of Security," No. 2.

[14] Yosri Fouda and Nick Fielding, *Masterminds of Terror: The Truth Behind the Most Devastating Terrorist Attack the World Has Ever Seen* (New York: Arcade, 2003), p. 19.

[15] An example of countersurveillance is provided in Italian Prosecution documents relating to the arrest of an al-Qaeda cell operating in Italy in 2001. Through intercepted telephone conversations involving some of the suspects, one of the parties, Mokhtar Bouchoucha, described how, while traveling on a train in London with two associates, he suspected they were being followed by police. One of these associates subsequently got off the train to determine if they were being followed. This person, through the use of a telephone, was able to confirm to his two companions on the train that they were indeed being followed. Public Prosecutor's Office Milan (Italy), "Case number 13016/99 against Marouf, Tarek; Essid Sami; Ben Khemais; Kammoun, Mehdi; Bouchoucha, Mokhtar; Ben Soltane, Adel; Tlili, Lahzar Ben Mohammed; Charaabi, Tarek and Thaer, Mansour" (Indictment), 2001.

[16] Sayf Al-Adl, "Legal Vision."

[17] Stephen Ulph, "A Guide to jihad on the Web," at http://www.jamestown.org/terrorism/news/article.php?articleid=2369531, The Jamestown Foundation, 31 March 2005 (accessed 14 July 2006); Anne Broache, "Al-Qaida Proving Elusive on the Net," *The New York Times*, 14 October 2005.

[18] *Ibid.*

[19] Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, and Brian Michael Jenkins, *Countering the New Terrorism* (Santa Monica, CA: RAND, 1999), pp. 45–46.

[20] Yosri Fouda and Nick Fielding, *Masterminds of Terror*, p. 163.

[21] Public Prosecutor's Office Milan (Italy).

[22] Susan B. Glasser, "A Terrorist's Guide to Infiltrate West," *The Washington Post*, 9 December 2001; Alan Cullison, "Inside al-Qaeda's Hard Drive," *The Atlantic Monthly*, September 2004, p. 61.

[23] Al-Qaeda, *Declaration of Jihad*, p. 67.

[24] *The Encyclopedia of the Afghan Jihad*, p. 1.

[25] Paul Wolfowitz, ''Prepared Testimony of Deputy Secretary of Defense Paul Wolfowitz for the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence: Joint Inquiry Hearing on Counterterrorist Center Customer Perspective,'' at http://intelligence. senate.gov/0209hrg/020919/wolfowitz.pdf, 19 September 2002 (accessed 8 August 2006).

[26] *The Encyclopedia of the Afghan Jihad*, p. 4.

[27] For a detailed description of al-Qaeda's operational intelligence capabilities, see Gaetano Joe Ilardi, *From the IRA to al-Qa'eda: Intelligence as a Measure of Rational Action in Terrorist Operations*, Global Terrorism Research Centre, School of Political and Social Inquiry, Monash University, 2007. Unpublished Ph.D. Dissertation.

[28] Abdul Hameed Bakier, ''Jihadis Adopt to Counter-Terror Measures and Create New Intelligence Manuals,'' The Jamestown Foundation, at http://www. jamestown.org/terrorism/news/article.php?search=1&articleid =2370062, 13 July 2006 (accessed 17 July 2006).

[29] Muhammad Khalil al-Hakaymah, *The Myth of Delusion*, al-Maqreze Center Site, at http://cryptome.org/mod-usintel.pdf, n.d. (accessed 12 December 2006). Egyptian born al-Hakaymah is believed to have recently sworn allegiance to al-Qaeda, and, according to some observers, is positioning himself to become that organization's intelligence authority. Brian Fishman, ''Al-Qa'ida's Spymaster Analyzes the U.S. Intelligence Community,'' Combating Terrorism Center, at http://www.ctc.usma.edu/MythofDelusion.pdf, 6 November 2006 (accessed 7 January 2007).

[30] Abdul Hameed Bakier, ''The New Issue of Technical Mujahid, A Training Manual for Jihadis,'' The Jamestown Foundation, at http://www. jamestown.org/terrorism/news/uploads/TM_005_006.pdf, 29 March 2007 (accessed 3 April 2007).

[31] Peter M. Senge defines a learning organization in the following terms; ''...an organization that is continually expanding its capacity to create its future. For such an organization, it is not enough merely to survive. ''Survival learning'' or what is more often termed ''adaptive learning'' is important—indeed it is necessary. But for a learning organization, ''adaptive learning'' must be joined by ''generative learning,'' learning that enhances our capacity to create.'' Peter M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization* (Sydney: Random House, 1992), p. 14. For a detailed discussion on organizational learning in terrorist groups, see Brian A. Jackson, John C. Baker, Kim Cragin, John Parachini, Horacio R. Trujillo, and Peter Chalk, *Aptitude for Destruction. Volume One. Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism* (Santa Monica: RAND, 2005); Brian A. Jackson, John C. Baker, Kim Cragin, John Parachini, Horacio R. Trujillo, and Peter Chalk, *Aptitude for Destruction. Volume Two. Case Studies of Organizational Learning in Five Terrorist Groups* (Santa Monica: RAND, 2005).

[32] Al-Adl, "The Principles of Security." Al-Adl has also emphasized the importance of adopting a flexible approach to security planning, one which is responsive to the measures utilized by the opposing force. Al-Adl, "Legal Vision."

[33] Abu Mus àb al-Suri (1958–). Also known as Mustafa Setmariam Nasar, he was born in Syria, where, in the early 1980s, he took part in a revolt by the Muslim Brotherhood. In 1985, he moved to Spain, and then spent the next sixteen years in Europe, where he is believed to have assisted al-Qaeda to establish cells in Italy and France. He was arrested in Pakistan in October 2005. Murad Al-Shishani, "Abu Mus'ab al-Suri and the Third Generation of Salafi-Jihadists," The Jamestown Foundation, at http://www.jamestown.org/terrorism/news/article.php?search=1&articleid=2369766, 11 August 2005 (accessed 12 September 2005).

[34] Sayf Al-Adl, "*Message to Our People in Iraq and the Gulf Specifically, and to Our Islamic Ummah in General: The Islamic Resistance Against the American Invasion of Qandahar and Lessons Learned*," at http://www.intelcenter.com/Qaeda-Guerrilla-Iraq-v1-0.pdf, 2003 (accessed 23 January 2004).

[35] Al-Qaeda, *Declaration of Jihad*, p. 19.

[36] Alan Cullison, "Inside al-Qaeda's Hard Drive," p. 61.

[37] See, for example, Jason Burke, *Al-Qaeda: The True Story of Radical Islam* (New York: I.B. Tauris, 2004), pp. 22–40; Mark Juergensmeyer, *Terror in the Mind of God: The Global Rise of Religious Violence*, 3rd ed. (Berkeley, CA: University of California Press, 2003), pp. 148–166.

[38] Mark Juergensmeyer, *Terror in the Mind of God*, p. 152.

[39] See, for example, Jerrold M. Post, "Terrorist Psycho-Logic: Terrorist Behavior as a Product of Psychological Forces," in Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind* (Cambridge, UK: Cambridge University Press, 1996), pp. 33–35; Martha Crenshaw, "The Subjective Reality of the Terrorist: Ideological and Psychological Factors in Terrorism," in R.O. Slater and M. Stohl, eds., *Current Perspectives on International Terrorism* (New York: St. Martin's Press, 1988), p. 38.

[40] For instance, Martha Crenshaw observes that "...the situation in which terrorists exist is stressful and uncertain, which contributes to extreme and unrealistic beliefs that are psychologically functional, durable, and resistant to change. Both cognitive processes and motivational factors encourage reliance on a set of unchanging beliefs that inhibit flexibility and openness. This combination of factors explains the tenaciousness of terrorist beliefs despite their growing deviation from reality." Martha Crenshaw "The Subjective Reality of the Terrorist," p. 13.

[41] White, in his discussion on empathy and intelligence, describes empathy as an "...understanding of others from the inside looking out, not merely from the outside looking in. Empathy requires us to get inside the skin...of an actual or potential enemy and then to imagine what the world would look like through their eyes." Ralph K. White, "Empathy as an Intelligence Tool," *International Journal of Intelligence and CounterIntelligence*, Vol. 1, No. 1, Spring 1986, p. 58. Al-Qaeda's use of deception, like much of its counterintelligence tradecraft,

depends upon an understanding of its adversaries that will allow it to exploit its enemies' perceptions and vulnerabilities. Other *jihadi*-related documents reveal the importance and depth of this knowledge, with one document contending that the ''[m]ujahideen ought to be aware and informed of the enemy's weaknesses. Their intelligence system ought to have gained the deepest access into the enemy's plans and strategies. The Mujahideen also ought to be familiar with the enemy's psychology.'' Mufti Khubaib Sahib, ''Mujahideen and Training,'' *2600 news*, at http://www.2600.com/news/mirrors/harkatmujahideen/www.harkatuulmujahideen.org/jihad/m-train.htm, n.d. (accessed 8 February 2007).

[42] Al-Qaeda's pursuit of empathy serves to weaken certain theories of terrorist psychopathology or personality disorder. For instance, theories that portray narcissism as central to terrorist motivation describe a profound lack of empathy as a hallmark of this personality type. See, for example, the discussion by Andrew Silke, ''Cheshire-Cat Logic: The Recurring Theme of Terrorist Abnormality in Psychological Research,'' *Psychology, Crime and Law*, No. 4, 1998, p. 57; Jerrold M. Post, ''Terrorist Psycho-logic,'' pp. 27–31. Al-Qaeda's efforts to acquire a detailed, even profound, understanding of its adversaries through the methical collection of intelligence suggest an ability to construct accurate images of others without resorting to the narcissist's tendency to underestimate or belittle. Indeed, distorting reality in this way is the antithesis of the terrorist organization's reason for collecting intelligence in the first instance.

[43] Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), p. 170.

[44] Peter Nesser, ''Jihad in Europe. A Survey of the Motivations for Sunni Islamist Terrorism in Post-Millennium Europe,'' FFI (Forsvarets Forskningsinstitutt), Norway, at http://rapporter.ffi.no/rapporter/2004/01146.pdf, 2004 (accessed 24 January 2005), pp. 32 and 36.

[45] Bernard Lewis, *The Assassins: A Radical Sect in Islam* (New York: Oxford University Press, 1987), p. 25; Arzina R. Lalani, *Early Shi'I Thought. The Teachings of Imam Muhammad al-Baqir* (London: I.B. Tauris, 2000), pp. 88–92.

[46] Cyril Glassé, *The Concise Encyclopaedia of Islam* (London: Stacey International, 2001), pp. 450–451.

[47] *The Encyclopedia*, pp. 22–23. The principle of deception can also be found in key Islamist texts, such as *The Neglected Duty* by Muhammad al-Farag. A member of Egyptian Islamic Jihad, Farag wrote that ''... Muslims are free to choose the most suitable method of fighting so that deception, which is victory with the fewest losses and by the easiest means possible, is realized.'' Cited in Johannes J.G. Jansen, *The Neglected Duty: The Creed of Sadat's Assassins and Islamic Resurgence in the Middle East* (New York: Macmillan, 1986), pp. 210–211. The virtues of *taqiyya* continue to be spread in the post 9/11 period. See, for example, Sheikh Abu Muhammad Asim Al-Maqdisi, *Precaution, Secrecy and Concealment: Balancing Between Negligence and Paranoia*, At-Tibyan Publications, at http://www.geocities.com/rijecistine1/Makdisi—Precaution_Secrecy_and_Concealment.pdf, n.d. (accessed 15 February 2007).

48 Maxwell Taylor and Ethel Quayle, *Terrorist Lives* (London: Brassey's, 1994), p. 19.

49 Al-Qaeda, *Declaration of Jihad*, pp. 26, 53.

50 Alan Cullison, ''Inside Al-Qaeda's Hard Drive,'' p. 61. This doctrine of assimilation even extends to al-Qaeda's approach to security. It discourages security activity that may lead to ''*ifrat*,'' acting in a manner that makes something more noticeable. *Al-Battar Training Camp* explains, ''. . . the individual who is over protective in his cautiousness and secrecy—and does await any benefit from it—drags attention to him and exposes him to danger and security questioning . . .'' Sayf Al-Adl, "Legal Vision," No. 10.

51 United States District Court, *United States of America v. Osama bin Laden* et al., 6 February 2001, pp. 212–213.

52 United States District Court, *United States of America v. Mohamed Sadeek Odeh*. Southern District Court of New York. Sealed Complaint, 26 August 1998, p. 5.

53 Cited in Yosri Fouda and Nick Fielding, ''*Masterminds of Terror*,'' p. 120.

54 Peter Lance, *1000 Years for Revenge: International Terrorism and the FBI—The Untold Story* (New York: Regan Books, 2003), pp. 258–259.

55 Abdul Hameed Bakier, "Jihadis Adopt to Counter-Terror Measures and Create New Intelligence Manuals,'' The Jamestown Foundation, at http://www.jamestown.org/terrorism/news/article.php?search=1&articleid =2370062, 13 July 2006 (accessed 17 July 2006).

56 United States District Court, *United States of America v. Mokhtar Haouari*. Southern District of New York, 3 July 2001, p. 650.

57 Jack Roche is the first Australian to be charged with, and convicted of, being a terrorist. A member of *Jemmah Islamiyah* (JI) after swearing the *bayat* (oath of allegiance) to JI cofounder, Abdullah Sungkar, he was tasked by the Australian JI leadership to travel to Afghanistan in early 2000 to receive training and directions from the al-Qaeda leadership. During this time, Roche met and was tasked by JI's senior operational leader, Hambali, al-Qaeda's senior planner Khalid Sheikh Mohammed, and al-Qaeda's operational commander, Mohammed Atef. He was subsequently directed to conduct surveillance on Israeli targets in Australia and form an operational cell.

58 Jack Roche, interview with author, 26 August 2005.

59 United States District Court, *United States of America v. Osama bin Laden* et al., 21 February 2001, p. 1178.

60 ''Riyadh Attack Death Toll Mounts,'' BBC News, at http://newswww.bbc.net.uk/1/hi/world/middle_east/3254385.stm, 9 November 2003 (accessed 9 April 2005).

61 Keith Jones, "Stolen Police Cars in Militants' Hands,'' *The Washington Times*, at http://www.washingtontimes.com/world/20040627-120847-1083r.htm, 27 June 2004 (accessed 9 April 2005).

62 United States District Court, *United States of America v. Osama bin Laden* et al., p. 170.

63 The practice of using aliases continued outside the training environment. Khalid Sheikh Mohammed, for example, is believed to have used nearly 30 aliases. It was

also common practice for militants to use *kunyahs*, Arabic pseudonyms adopted from the names of the Companions of the Prophet and Islamic heroes. For instance, each of the 19 hijackers involved in the 9/11 attacks adopted a *kunyah*. Mohammed Atta, for example, adopted the *kunyah* Abu 'Abdul' Rahman al-Masri, literally meaning "father of the servant of the Beneficent, the Egyptian." Yosri Fouda and Nick Fielding provide a full list of the *kunyahs* used by all 19 hijackers. *Masterminds of Terror*, pp. 45, 97, 110–112.

[64] Jack Roche, interview with author, 26 August 2005.

[65] The notion of concealment also has a place in Islamic doctrine. The word *kitman*, which means to hide or conceal, typically refers to the hiding of things or activities in process until complete. This, like *taqiyya*, has a religious utility, which spread from its Shi'ite roots, ultimately becoming an accepted practice of defense among Sunnis. Adda B. Bozeman, *Strategic Intelligence and Statecraft* (Washington: Brassey's, 1992), p. 98.

[66] United States District Court, *United States of America v. Mokhtar Haouari*, p. 642.

[67] United States District Court, *United States of America v. Ali Mohamed*. Southern District of New York, 20 October 2000, p. 15; Jack Roche, interview with author, 26 August 2005.

[68] United States District Court, *United States of America v. Osama bin Laden et al.*, pp. 236–237.

[69] Ian O. Lesser et al., *Countering the New Terrorism*, pp. 52 and 65; Desmond Ball "Desperately Seeking bin Laden," pp. 62–64.

[70] Al-Qaeda, *Declaration of Jihad*, p. 29.

[71] Sayf Al-Adl, "Communications Security," *Al-Battar Training Camp*, No. 5, 28 Febuary 2004.

[72] Cited in Joel Mowbray, "How They Did It: An 'Evil One' Confesses, and Boasts," *National Review*, Vol. 54, No. 24, 2002, p. 37.

[73] *The Encyclopedia*, p. 100. Al-Adl defines cover in similar terms, describing it as "...a veil or an outward appearance that hides behind it aspects of covert action by individuals, organisations, and groups. It provides the person with justification for being at a certain time and place to operate in secrecy." Sayf Al-Adl, "Cover," *Al-Battar Training Camp*, No. 10, 14 May 2004.

[74] Joel Mowbray, "How They Did It: An 'Evil One' Confesses, and Boasts," p. 37.

[75] United States District Court, *United States of America v. Osama bin Laden* et al., p. 26; Richard H. Shultz and Ruth Margolies Beitler, "Tactical Deception and Strategic Surprise in Al-Qai'da's Operations," *Middle East Review of International Affairs*, Vol. 8, No. 2, 2004, pp. 66–67; Peter L. Bergen, *Holy War, Inc.: Inside the Secret World of Osama bin Laden* (New York: The Free Press, 2001), p. 106.

[76] United States District Court, *United States of America v. Ali Mohamed*, p. 26.

[77] The counterintelligence literature confirms that a principal function of counterintelligence is to create a safer operating environment. Abram Shulsky observes that "...active [aggressive counterintelligence] measures...try to understand how a hostile intelligence service works to frustrate or disrupt its

activities and ultimately to turn those activities to one's own advantage..." Abram N. Shulsky, *Silent Warfare: Understanding the World of Intelligence* (Washington, D.C.: Brassey's, US 1991), p. 109.

78 Jason Burke, "Think Again: Al-Qaeda," *Foreign Policy*, No. 142 (May/June 2004), pp. 33–34; Richard A. Clarke, *Against All Enemies: Inside America's War on Terror* (New York: Free Press, 2004), p. 227.

79 Stephen Ulph, "New Online Book Lays out al-Qaeda's Military Strategy," The Jamestown Foundation, at http://jamestown.org/news_details. php?news_id=100, 18 March 2005 (accessed 26 July 2006).

80 Abu Bakr Naji, "*The Management of Savagery: The Most Critical Stage Through Which the Umma Will Pass*," at http://www.ctc.usma.edu/ Management_of_Savagery.pdf, n.d. (accessed 12 December 2006), p. 52.

81 Naji acknowledges that aggressive counterintelligence of this sort is highly specialized, requiring training unique among *jihadis*. For instance, he observes that due to the extended period of time required to effectively penetrate organizations, "so that he can master his role in the institution which he is infiltrating," the *jihadi* should be provided an educational program to "safeguard his piety without revealing it." *Ibid.*

82 United States District Court, *United States of America v. Ali Mohamed*, pp. 26–28.

83 Peter Lance, *1000 Years for Revenge*, pp. 31–35.

84 Peter J. Fitzgerald, *Statement before the National Commission on Terrorist Attacks Upon the United States*, 16 June 2004.

85 P. Wilson, "Dead Men Tell Very Few Tales," *The Australian*, 5 July 2006.

86 N. Christian, "Al-Qaeda Plot to Blow Up British Embassy," *The Scotsman*, at http://www.scotsman.com/international.cfm?id=1372772003, 14 December 2003 (accessed 18 August 2004).

87 "Transcript of Testimony of Melanie Brown Before Anti-Terrorism Judge, Jean-Francois Ricard," Four Corners, at http://www.abc.net.au/4corners/content/ 2004/s1132151.htm, 2004 (accessed 11 August 2006).

88 Richard Clarke, *Against All Enemies*, pp. 152–153.

89 A case in point is the 2007 British-based plot (named "Operation Gamble" by counterterrorism officials) which reportedly involved a plan by a group of Islamists to abduct and murder a serving British soldier, whose execution was to be broadcast on the Internet. Reports at the time indicate that the group was found in possession of a list containing the names and addresses of 25 serving British Muslim soldiers. While the source of the list remains unknown, it is suspected that it was leaked by someone within the Ministry of Defence. Daniel McGrory and Russell Jenkins, "Fears of Terror Mole in UK Defence," *The Weekend Australian*, 3–4 February 2007.

90 *The Encyclopedia*, pp. 26–27.