International Journal of Intelligence and CounterIntelligence, 22: 221–236, 2009

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850600802698200

Routledge
Taylor & Francis Group

JUSTIN R. HARBER

Unconventional Spies: The Counterintelligence Threat from Non-State Actors

In the wake of the 11 September 2001 (9/11) terrorist attacks on New York City and Washington, D.C.—when overseas experience and Arabic language credentials became so crucial to the Global War on Terrorism (GWOT)—Nada Nadim Prouty appeared to be the ideal candidate for operations work at the Central Intelligence Agency (CIA).[1] Prior to joining the Agency in 2003, the Lebanese-born Prouty served as a special agent with the Federal Bureau of Investigation (FBI).[2] At the Bureau, according to her plea agreement, the 37-year-old Prouty accessed FBI files without authorization regarding Hezbollah, the Lebanese terrorist organization with representatives in the Lebanese government, and exfiltrated classified documents to her home.[3]

Of particular concern is Prouty's brother-in-law, Talil Khailil Chahine, who had earlier fled to Lebanon. In 2002, Chahine attended a fund-raising event, with Hezbollah's former spiritual leader in attendance. Today he stands accused of funneling $20 million from Detroit-area restaurants he owns back to Lebanon.[4]

While, technically, Hezbollah is part of the Lebanese government, the Prouty affair highlights an increasing, if not well publicly-documented, concern for intelligence officials: the counterintelligence (CI) threat from violent non-state actors (NSAs). How prevalent is the CI threat from these groups? How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S. national security? What policy prescriptions can mitigate the potential damage from this menace?

Justin R. Harber is a graduate of the Virginia Military Institute, with an M.A. in Security Studies from Georgetown University and currently lives and works in Washington, D.C.

COUNTERINTELLIGENCE PENETRATIONS BY NON-STATE ACTORS

Recent history is peppered with CI penetrations, ranging from Aldrich Ames of the CIA to Robert Hanssen, Katrina Leung, and Leandro Aragoncillo of the FBI. Overall, however, CI has been largely characterized as a ''neglected element'' of the intelligence discipline.[5] Denigrated as less intellectual than analysis, less thrilling than foreign intelligence collection, contrary to the notion of democratic norms, it is usually considered, at best, a necessary evil to support operational security.[6] In a 2000 article surveying the intelligence challenges of the twenty-first century, then–Director of Central Intelligence (DCI) George J. Tenet never mentioned CI in his assessment, let alone the unique challenges posed by NSA penetrations.[7]

Indeed, at first glance, NSAs make unlikely candidates as spies to infiltrate the U.S. federal government. Dissimilar from their state-level counterparts, they are significantly less capable of mustering the enormous financial, technical, and training resources necessary to infiltrate the national security architecture of foreign powers.[8] Traditional state-level adversaries, such as Russia and China, constitute a more plausible CI threat because these countries operate their own intelligence apparatuses that, in a diffracted way, mirror America's own intelligence infrastructure. They have whole ministries with burgeoning bureaucracies and a dedicated cadre of intelligence officials willing to commit millions of dollars to collect intelligence on American targets, whereas the collection capabilities of non-state actors are largely relegated to gathering intelligence for operational purposes, such as downloading information on aerial spraying for biological or chemical agents, or casing potential bomb targets.

Yet, given the renewed impetus in thwarting terrorism after 9/11, U.S. CI efforts against belligerent NSAs have enjoyed a newfound limelight. The 2007 U.S. *National Counterintelligence Strategy* explains the threat quite clearly:

> The United States faces a wide range of threats to its security from foreign intelligence activities, *terrorist elements, and other non-traditional adversaries* designed to achieve advantage over US military, diplomatic, and economic interests at home and abroad.... Foreign intelligence collection establishments and *terrorist groups* acquire resources, train and deploy personnel, and execute both clandestine and covert intelligence operations against us.[9] [emphasis added]

The *Strategy* goes on to characterize CI as an integral component to the counterterrorism agenda: ''To further support counterterrorism, the counterintelligence community will review operations and intelligence

reporting to detect attempts by terrorist entities to penetrate and manipulate us.''[10] In the same vein, the 2005 Silberman-Robb Commission, more commonly known as the WMD Commission, argued that it ''is not only major nations which employ aggressive intelligence services. Terrorist groups like Hezbollah and al-Qa'ida also conduct intelligence operations within the United States.''[11]

Given their scarce resources and the daunting challenges intrinsic to intelligence collection against foreign governments, why would NSAs seek penetrations against the U.S. national security infrastructure? William Rosenau of the RAND Corporation offers at least two reasons. First, much like foreign intelligence services, NSAs can garner ''invaluable information about the government's capabilities, intentions, and weakness.''[12] In addition, NSAs may exploit infiltrations for their own CI purposes: ''penetration can give terrorists and insurgents opportunities to plant false information, redirect the state's potentially lethal gaze, force the authorities to misallocate resources, and otherwise derail the state's campaign.''[13]

Today, CI officials fear that terrorists may employ some of the same tradecraft in intelligence collection as state adversaries.[14] Indeed, alleged al-Qaeda training media include lessons on how to collect open source intelligence, conduct surveillance, interrogate detainees, and recruit agents working in a foreign government.[15] As one Naval Criminal Investigative Service (NCIS) official commented: ''It would be naïve to believe that terrorists weren't infiltrating the Navy.''[16] Currently, the CIA is concerned that a number of its recent applicants may have been foreign agents.[17] As reported in *The Christian Science Monitor*, ''This would fit Al Qaeda's pattern, according to Michael Scheuer, a former top CIA counterterrorism official. Al Qaeda operatives, he says, have already penetrated several security agencies in Middle Eastern countries.''[18]

Perhaps more troubling than the thought of an actual terrorist getting beyond the screening process and being hired is the notion of a violent NSA recruiting an asset who already works in the IC. Again, given these groups' relatively sparse financial resources, enlisting the help of an insider through material incentives seems unrealistic. Yet, violent Islamist NSAs may employ other inducements—namely a sense of kinship or a common religious identity—to persuade potential recruits. Two variables, in particular, interact to raise the chances of this threat from belligerent Islamic extremist groups: the increased need for intelligence officers with specific cultural and language credentials, and the practice of ''ethnic recruiting.''

First, given the heightened tempo in counterterrorism and military operations in Africa, the Middle East, and Central Asia, the IC has an

increased need for intelligence officers (not unlike Prouty) who can navigate the cultural geography of these regions and speak their languages fluently. These officers, despite being U.S. citizens, will have a greater chance of being raised abroad and may retain familial ties and some vestige of loyalty to their respective cultures.[19]

Second, as former CI officer Frederick L. Wettering has observed, the majority of foreign intelligence services that seek to collect against American targets "practice ethnic recruiting, that is, seek to recruit persons of the same ethnic background as the foreign intelligence officer."[20] These vulnerable individuals "may more often become motivated to do so [commit espionage] due to feelings of obligation or loyalty to foreign country or foreign friends and relatives."[21]

Many Middle Eastern and Central Asian states are governed by autocratic despots who have garnered little domestic legitimacy during their tenure. Sympathy for dissident groups that violently oppose these regimes (and the nations that support them, such as the U.S.) may be traced in part to public animosity toward the decadence, secularism, and apathy of the ruling powers. Without any sense of loyalty or patriotism for these autocrats, terrorists may then employ Islam, or an ambiguous sense of cultural identity, as the vehicle of public support to forcefully oppose these governments.

By extension, belligerent NSAs may seek to convince potential recruits that they are serving the interests of their common religious or ethnic identity by spying on the U.S. They may argue that, by serving in a government that colludes with the despotic repressor of their homeland, the recruit is betraying his or her own people—he or she is literally aiding the war against Islam and supporting the oppression of their fellow countrymen. Political or ideological recruitment methods are not unknown to NSAs. Islamic extremist training material attributed to al-Qaeda specifically references "political orientation" as a potential tool for recruitment.[22] Though Ana Montes of the Defense Intelligence Agency (DIA) spied for Cuba, her case illustrates "that a strong sense of obligation to serve the needs of a 'world homeland' can, under some circumstances, provide sufficient motivation for espionage."[23] As indicated by Lisa Kramer and Richards Heuer, the former DIA officer attributed her espionage "to her belief in the moral righteousness of her actions, [and] expressed no remorse for helping Cuba 'defend itself' against what she described as unfair and oppressive U.S. foreign policies."[24]

Thus, as the U.S. Intelligence Community sees a growing need to fill its ranks with officers with firsthand knowledge of regions pertinent to the GWOT, non-state actors may perceive better opportunities to recruit insiders sympathetic to religious or ideological ploys.

INTELLIGENCE LIAISONS—THE FRIEND OF MY FRIEND MAY BE MY ENEMY

The 9/11 terrorist attacks fundamentally altered the IC's center of gravity as it pertains to intelligence liaisons with foreign services. As before, the U.S. remains staunch allies with the Commonwealth nations (UK, Australia, Canada, and New Zealand), but has now embraced a whole host of other foreign intelligence services to combat global terrorism.[25] These new relationships include even adversarial countries such as Syria.[26] As Stéphane Lefebvre has noted, "With 9/11 and the initiation of military operations against al-Qaeda in Afghanistan, these established relationships had to be complimented with vigorous new ones involving Middle Eastern and Central Asian countries, often making for strange alliances."[27]

While the United States has vast technical collection platforms at its disposal, the Global War on Terror demands human intelligence expertise in specific languages and cultures for which these new alliance partners are in some cases better suited. Many of these countries were only all too eager to embrace an American partnership. As Lefebvre also points out:

> No one agency can do and know everything. . . . The United States, France, Germany, and the United Kingdom are particularly attractive partners for less fortunate services that can trade human intelligence for the more sophisticated and expensive technical products to which they would not otherwise have access.[28]

To be sure, these new intelligence liaisons may reap a bountiful harvest in human intelligence, yet they also burden the IC with at least two significant CI risks exploitable by non-state actors.

First, foreign intelligence partners may find lower security thresholds tolerable, and feel no need to exercise high CI standards or operational integrity. In fact, little doubt remains that belligerent NSAs have penetrated the foreign governments of American allies. Jamaat-e-Islami, a Bangladeshi terrorist organization with ties to al-Qaeda, is suspected of either recruiting or seeding Jamaat sympathizers into the highest echelons of the Bangladeshi government.[29] In 2006, al-Qaeda claimed that it had infiltrated the government of the United Arab Emirates (UAE).[30] Terrorism expert Lorenzo Vidino adds that, if the penetration were true, "it . . . reveals that even though they are our friends, al Qaeda seems to have people on the inside in the UAE, just as it has in Saudi Arabia, Pakistan, Qatar, and Kuwait."[31] Finally, senior military leaders in Colombia have come under suspicion for supplying intelligence to the narcotrafficking Revolutionary Armed Forces of Colombia (FARC), as well as to the Norte del Valle drug cartel.[32] The leaked intelligence included "the secret positioning of U.S. naval vessels and aircraft in the Caribbean early [in 2006], part of a

carefully coordinated web designed to stop cocaine from reaching the United States, according to high-ranking Colombian military officials.''[33] Regardless of the benefits, by pairing with these compromised services, the U.S. puts its own intelligence operations at risk.

Second, many of these new or reestablished liaisons may not necessarily be penetrated by violent NSAs, yet parochial interests within the services themselves may collude with groups hostile to the U.S. Elements of the Pakistani Directorate for Inter-Services Intelligence (ISI), for instance, continue to retain close ties to extremists in Afghanistan.[34] Martin Rudner writes that ''recent deals between the Pakistani government and tribal elders in the Federally Administered Tribal Areas (FATA) along the border with Afghanistan look suspiciously like capitulation to the Taliban, orchestrated by Pakistani intelligence agencies with ties to known extremists.''[35]

Reinvigorating fears that partisan militias permeate the Iraqi government, the Independent Commission on the Security Forces of Iraq concluded: ''The Ministry of Interior is a ministry in name only. It is widely regarded as being dysfunctional and sectarian, and suffers ineffective leadership. . . . The Iraqi Police Service . . . is compromised by militia and insurgent infiltration.''[36]

While these ''strange alliances'' may fill in gaps in human intelligence collection, some of them also jeopardize the integrity of U.S. operations through porous or factionalized foreign intelligence services.

NON-STATE ACTOR COUNTERINTELLIGENCE THREAT ASSESSMENT

Since CI challenges by hostile NSAs are ubiquitous, if not increasing, how dangerous are infiltrations by these groups? Are they more or less of a security threat than typical state actors? In truth, CI penetrations by NSAs share some of the same risks identified with their state-level counterparts. Yet, given these disparate groups' ability to rapidly link up for common cause, the NSAs also present a unique dilemma for CI officers.

Penetrations by both NSAs and state actors generally threaten U.S. national security by revealing America's ''capabilities, intentions, and weakness.''[37] Both groups may then use this intelligence to their mutual advantage—including as offensive CI to thwart the collection efforts of the infiltrated agency. A hostile non-state actor may act on intelligence to plot its next bombing campaign or to disrupt military operations against one of its cells. For state actors, however, the utility of harvested intelligence is dramatically increased because foreign governments are more inclined to have the resources at their disposal to best exploit any new information. Russia or China can build quieter submarines and more effective collection platforms, or develop better-informed grand strategies, by exploiting the intelligence they have pilfered from the U.S. government. Thus, state

actors have significantly broader targeting requirements across the economic, military, scientific, and political spheres. Smaller, less-well funded NSAs may share some of the same targeting requirements with their larger counterparts (particularly with regards to policy and military matters), but will most likely be concerned with information as it pertains to counterterrorism, counternarcotics, classified policy decisions, military objectives, and other relevant subjects.

Globalization and advances in information technology have made the exfiltration of classified information easier, as well as more difficult to detect, for both foreign governments and NSAs. Today, information storage devices are constantly decreasing in size while their storage capacity regularly increases.[38] In addition, the greater frequency of global travel and international contacts across industries has led to the "increased opportunity for the transfer of classified and other protected information to foreign entities."[39] State actors as well as NSAs are equally likely to exploit the latest technology to steal state secrets. Again, given their sizeable financial resources, state actors are better at developing the "cutting-edge" information technology to gather and transmit data. Non-state actors will instead be most likely limited to the best "off-the-shelf" commercial technology available, usually of a lower caliber than the tools at the disposal of state-level operators.

ASSESSING THE DESIRABILITY OF SHARING

What are the incentives for states and NSAs to share collected intelligence with foreign governments or even ideologically likeminded organizations? Since states invest significant financial resources in planting or recruiting agents, or harvesting intelligence from expensive collection platforms, they remain, at the very least, highly selective regarding the intelligence they share.[40] Of course, given the nature of the business, intelligence liaisons entail a measure of risk. As Chris Clough points out, "[N]ational intelligence agencies have always cooperated when the potential benefits have outweighed the risks—and international cooperation is without question a risky business."[41] Thus, even when intelligence liaisons across foreign governments are well lubricated, they remain subject to a thorough screening process, so that only the most relevant intelligence is shared to ensure that the relationship continues in mutual interest.

Conversely, NSAs are significantly less hampered in their intelligence links with other organizations, and are not bogged down by the legal, bureaucratic, and political restrictions that impede state actors. In fact, these groups may be more inclined to openly share the intelligence they collect with allied organizations, in the same way they exchange military tactics or ideological support. It is fair to assume that, given the global

terrorist network architecture and the rapidity with which these groups may link up and cross-pollinate, intelligence gleaned from non-state actor penetrations could be easily transmitted to other hostile groups. As Seth Jones points out, in today's GWOT, ''Islamic militants in Iraq have provided information on tactics through the internet and face-to-face visits to the Taliban, HIG [Hezb-i-Islami Gulbuddin, an Afghan terrorist group] and foreign fighters from eastern and southern Afghanistan and Pakistan's tribal areas.''[42] Peace in Northern Ireland has led Irish Republican Army (IRA) militants to offer their services to Colombia's FARC.[43] From Afghanistan and Iraq to Colombia, narcotraffickers and insurgents have often found common cause in undermining government efforts to thwart their mutual enterprises—a collusion which may include an intelligence-sharing dimension.[44]

POLICY PRESCRIPTIONS

How can the U.S. Intelligence Community best protect itself against the onslaught of potential NSA counterintelligence operations? Many of the latest developments in CI reform are largely due to the 9/11 terrorist attacks and recent penetrations. If turncoats Hanssen, Ames, Montes, and others left any legacy, it is a clarion call for stauncher security practices in government agencies responsible for national security. These include more thorough background investigations and periodic reviews; regular personal finance disclosure for national security officials and their families; and more frequent polygraphs. These efforts do lead to more effective CI, but they do not entirely safeguard against the unique threat posed by NSAs. For example, given the sparse financial resources of many terrorist groups, they are unlikely to pay for an insider's services, and are more inclined to rely on ideological drivers to motivate recruits. The suggestions argued here include some previously voiced policy prescriptions, but also include new practices that could help to counter, or at least mitigate, the NSA threat.

Offensive Counterintelligence

First and foremost, perhaps no instrument of U.S. counterintelligence will bear more fruit than knowing the intelligence targets and collection capabilities of its adversaries. The IC must be willing to go on the CI offensive against terrorist elements—in particular the IC must work to infiltrate the networks and organizations of violent NSAs. Such aggressive CI tactics as offensive penetrations serve much the same function as foreign intelligence collection: they reveal the capabilities of adversaries, their targeting requirements, and the effectiveness of their operations.

Perhaps most importantly, they can also create an opportunity to impede hostile collection efforts through a variety of disinformation measures.

Former National Counterintelligence Executive (NCIX) Michelle Van Cleave has argued that "[b]y working the foreign intelligence service as a strategic target globally, U.S. counterintelligence should be able to leverage insights into adversary activities and vulnerabilities to direct CI operations to maximum effect."[45] According to Frederick Wettering, "The most effective sources of identification of U.S. spies are defecting intelligence officers and the spies themselves."[46] In its investigation regarding the implementation of security protocols after the Hanssen penetration, the Justice Department's Office of the Inspector General stated that "the recruitment of human assets in hostile intelligence services is the most valuable tool for identifying moles in the Intelligence Community."[47]

While offensive CI clearly remains one of the best possibilities the IC has in discovering that its security has been compromised, intelligence officials face myriad challenges to infiltrating NSAs. National intelligence services are relatively inert targets for unfriendly collection. Their officers often follow the same tactics, stemming from the same training, no matter where they are operating. They work in large, state-run bureaucracies, in what are often identifiable ministry buildings; and, in some cases, they even have public Websites for access.[48] Terrorist organizations, on the other hand, pose a considerable penetration challenge.[49] Given their smaller size, these groups are much more adept at quickly modifying their tactics to avoid detection, such as altering their communication techniques. Global terrorist networks are also able to coalesce and dissolve cells rapidly and efficiently, making these groups fluid, dynamic targets difficult for intelligence services to collect against with any manner of effectiveness. In addition, many violent non-state actors, particularly Islamic extremist networks, are constructed from communal or family ties. Thus, for the "outsider" to gain any level of trust within the group is particularly difficult.

The best chances for the U.S. IC to gain access to these organizations may be through the cooperation of an inside dissenter; to seed a low-level agent; or to turn a member of the group being held in U.S. custody into a double agent. Naysayers would correctly contend that all three routes entail grave risks. The dissenter may be extremely difficult to contact (let alone compel to spy), given the tight network many of these organizations exhibit. Seeding a low-level recruit may be possible, but the return on investment may take years to mature as the plant slowly works up the organizational hierarchy. While a detained terrorist may have already earned credibility with the host organization, returning such an individual to the battlefield in the hopes that he or she will collect intelligence for the U.S. is obviously a risky gambit that very nearly defies consideration.

Despite the serious drawbacks to infiltrating an NSA, the potential bonanza of information merits continuously weighing such opportunities as they arise. Thus, the IC should constantly explore ways to penetrate these quintessentially impregnable fortresses with human assets.

Tailored Counterintelligence Training at Home

If the West's adversaries are tailoring their recruitment techniques to match their targets, then the U.S. and its allies must adopt countermeasures that echo that specificity. To that end, since some foreign intelligence services and NSAs may practice ''ethnic recruiting,'' the IC should consider specifying its CI training platforms for those most likely to be targeted in the national security infrastructure. These classified training programs could cover such topics as recent developments in Islamist intelligence activities, Chinese recruitment tactics, or annual Israeli targeting requirements.

Training does not have to burden every single Intelligence Community agency with unnecessary obligations—which may result in variations in standards—and instead could be coordinated and provided by the NCIX across the IC. This would also allow intelligence officials from disparate elements of the IC to come together and jointly gain a greater understanding of how foreign services seek to target them.

Understandably, offering CI training based on employees' personal backgrounds, or social or professional positions, may run contrary to current notions of objectivity in government. Of course, the IC cannot mandate training of this sort for national security officials—they themselves must elect to participate. As controversial as it may sound, however, those U.S. and allied personnel most likely to be targeted deserve to be made aware of how foreign intelligence services and NSAs perceive them as potential recruits. By the nature of the occupation, the police officer leaving his or her home each day understands that he or she may be confronted with violent criminals while on duty. But the ability to tell that officer that the average street thug is more likely to carry a knife than a gun arms that officer with the information to better meet the day's criminal challenges.

Admittedly, tailored CI training carries with it the serious shortcoming of making treachery easier for an insider spy who has penetrated the IC. Although this sort of program may be helpful in communicating the intelligence threat to targeted members of the Community, it also provides the turncoat who receives this training with valuable information on how successful the U.S. is in deterring foreign intelligence collection. In addition, such training opportunities may provide insider spies with a list of other potential recruits among the personnel from across the spectrum of government agencies that jointly participate.

Counterintelligence Training with Liaison Partners

The post-9/11 world demands closer intelligence links with foreign services. But how can the U.S. continue to protect its own intelligence assets when it must collaborate with services from abroad that might be less than completely reliable? The challenge for the U.S. is to maintain the favorable balance between sharing intelligence on threats of mutual interest with other governments, while simultaneously protecting U.S. assets.[50] The U.S. can buttress these alliances through training foreign services on how to practice better CI in their own organizations.

Counterintelligence training across international boundaries can take on a range of forms—from better information technology security, to internal investigations, and to classified material safeguards. Any cross-training program should account for the nature of the intelligence relationship, and take into consideration the strengths, vulnerabilities, size, and threats to the partner service. Many of the U.S.'s allies could particularly benefit from training that deals with the intelligence threats from homegrown insurgencies or hostile NSAs—especially since several of these partner states in Africa and the Middle East face such challenges today.

Critics may denigrate such programs as revealing valuable secrets about how the U.S. IC goes about performing its intelligence duties. In fact, however, the U.S. has helped to train other foreign services on a range of intelligence-related topics,[51] and cooperation on CI matters is simply an extension of this relationship. Building up the CI capability of America's security partners not only helps the U.S. IC to protect its own assets and those of its allies, but may also serve as an additional exchange through which to bolster trust in such alliances.

Track All Access to Classified Material

In 1989, the CIA discovered that Felix Bloch, a diplomat with the U.S. State Department, was a mole working for the Soviet KGB.[52] As federal law dictates, the CIA alerted the FBI to Bloch's spying activities and the Bureau immediately began its investigation. Once Robert Hanssen became aware of Bloch's detection through the FBI's Automated Case System (ACS), he alerted his Russian handlers, and ultimately squashed the investigation against the State Department mole.

Hanssen's case is not an isolated incident. Both Leandro Aragoncillo and Nada Nadim Prouty abused their government access to perform searches on classified information irrelevant to their jobs. These cases illustrate the urgent need for a tracking mechanism for classified material. The Department of Justice's Inspector General made similar recommendations to the FBI following Hanssen's arrest, but the extent to which Sentinel the Bureau's successor to the ACS will perform this function remains unclear.[53]

Moles benefit from enjoying the widest scope of access possible within their intelligence services. This helps them retain value to their handlers by exfiltrating a wide array of intelligence, and may also alert them to possible mole hunts within their own organization. Both state and non-state penetrators benefit from unfettered access to their host's files, but, for NSAs, this is particularly valuable because they have more specific targeting requirements. An Islamic extremist penetrator who works on counternarcotics issues will be much more hesitant to research intelligence on Israel if he (or she) realizes that such searches will be recorded. Consequently, an infiltrator in such a scenario is also more likely to be caught when CI officers begin to question why that person is performing searches outside of the assigned scope of work. While the newly unveiled Intelligence Integration Program, aimed in part in making intelligence more accessible across the IC, is designed to deny access outside of an analyst's portfolio, this same information sharing platform could serve as a record's system to track who is accessing what.

POLITICAL COMMITMENT TO MEETING CHALLENGES

The post–Cold War security environment is populated with an entire host of intelligence collection challenges, ranging from WMD proliferation, to drug trafficking and, of course, terrorism. Added to these threats is the ascendancy of intelligence collection against the U.S. by NSAs. Much like their state-level counterparts, NSAs understand the enormous potential that penetrating the U.S. national security architecture may bestow. While they may lack many of the collection capabilities and exploitation methods of state-level actors, NSAs pose a particularly unique, if not urgent, CI challenge because of their inherent difficulty as a collection target and their willingness to share information across organizational boundaries. Indeed, the number of penetrations by NSAs in other foreign services is weighty, and should give the U.S. IC pause in considering the gravity of this threat.

Decades of refining recruitment and applicant screening processes have done much to safeguard the IC against hiring a potential non-state operative (though the Prouty affair, despite her real or imagined ties to Hezbollah, invites skepticism about the IC's hiring process). Nonetheless, since today's intelligence demands require more officers with foreign credentials, the real chance that an NSA may recruit a sympathetic insider has been increased. In the same vein, the Global War on Terror has thrust the U.S. into collaboration with a new corps of foreign intelligence services—some of which either lack a competent CI capability, or are cleaved along factions with elements befriending groups hostile to the U.S.

The counterintelligence menace from non-state actors is a daunting, yet not informidable, challenge to American national security. The U.S. Intelligence Community has the tools in place to effectively thwart NSA penetrations and bolster the security of its alliance partners. The future of American CI to meet this threat will largely depend on the willingness of the nation's political leadership to commit the necessary resources to meet this challenge. The flagrant revelations of the recent Prouty affair may help catalyze a newfound impetus to do so.

REFERENCES

[1] Michael Isikoff, et al., "Dangerous Liaisons; Nada Prouty Worked for the FBI and CIA. Now There's Worry She's Not Who They Thought She Was," *Newsweek*, 26 November 2007, p. 35.

[2] Joby Warrick and Dan Eggen, "Ex-FBI Employee's Case Raises New Security Concerns: Sham Marriage Led to U.S. Citizenship," *The Washington Post*, 14 November 2007, p. A3.

[3] Josh Meyer, "The Agent with a Secret Past; She Forged Her Way to Citizenship, Joined the FBI and CIA, and Then Accessed Computers for Restricted Information," *The Los Angeles Times*, 14 November 2007, part A, p. 1.

[4] Michael Isikoff, "Dangerous Liaisons," p. 35.

[5] Roy Godson, *Dirty Tricks Or Trump Cards: U.S. Covert Action & Counterintelligence* (New Brunswick, NJ: Transaction Publishers, 2007), pp. 6–18.

[6] *Ibid.*

[7] George J. Tenet, "The CIA and the Security Challenges of the New Century," *International Journal of Intelligence and CounterIntelligence*, Vol. 13, No. 2, Summer 2000, pp. 133–143. To his credit, Tenet does presciently mention the terrorist threat and the challenges of infiltrating such an organization prior to 9/11. Yet, he does not articulate the terrorist menace in the context of the counterintelligence agenda.

[8] Important deviations to this rule deserve consideration. Aum Shinrikyo (today Aleph), the Japanese cult that perpetrated the 1995 sarin gas attack in the Tokyo subway, enjoyed multiple offices in several countries, tens of thousands of members worldwide, and, at its lowest estimate, claimed $20 million in assets. See David E. Kaplan, "Aum Shinrikyo (1995)," in *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Jonathan B. Tucker, ed. (Cambridge, MA: MIT Press, 2001), pp. 209–210.

[9] *The National Counterintelligence Strategy of the United States of America (2007)*, p. 1, emphasis added, at http://www.ncix.gov/publications/policy/CIStrategy.pdf

[10] *Ibid.*

[11] *Commission Report on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 31 March 2005, at http://www.wmd.gov/about.html

[12] William Rosenau, *Subversion and Counterinsurgency*, RAND Corporation, 2007, pp. 6–7, at http://www.rand.org/pubs/occasional_papers/2007/RAND_OP172.pdf

[13] *Ibid.*

[14] Paul Davis, ''The Spy is an Eye: The Naval Criminal Investigative Service is Guarding Against Terrorist Spies,'' *The Journal of Counterterrorism and Homeland Security International*, Winter 2005, Vol. 11, No. 1.

[15] *Declaration of Jihad (Holy War) Against the Country's Tyrants*, Eleventh and Twelfth Lessons, as translated by the U.S. Department of Justice, at http://www.justice.gov/ag/manualpart1_3.pdf

[16] Paul Davis, ''The Spy is an Eye.''

[17] Faye Bowers, ''US Unready for Rising Threat of 'Moles': A Recent Report on US Intelligence Harshly Critiqued Counter-Spy Efforts,'' *The Christian Science Monitor*, 8 April 2005, p. 1.

[18] *Ibid.*

[19] Lisa A. Kramer and Richards J. Heuer Jr., ''America's Increased Vulnerability to Insider Espionage,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 20, No. 1, Spring 2007, p. 56.

[20] Frederick L. Wettering, ''Counterintelligence: The Broken Triad,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 13, No. 3, Fall 2000, p. 275.

[21] Lisa A. Kramer and Richards Heuer Jr., ''America's Increased Vulnerability to Insider Espionage,'' p. 56.

[22] *Declaration of Jihad (Holy War) Against the Country's Tyrants*, Twelfth Lesson.

[23] Lisa A. Kramer and Richards Heuer Jr., ''America's Increased Vulnerability to Insider Espionage,'' p. 58.

[24] *Ibid.*

[25] Martin Rudner, ''Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 17, No. 2, Summer 2004, p. 194.

[26] Richard J. Aldrich, ''Dangerous Liaisons: Post-September 11 Intelligence Alliances,'' *Harvard International Review*, Fall 2002, p. 51.

[27] Stéphane Lefebvre, ''The Difficulties and Dilemmas of International Intelligence Cooperation,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 16, No. 4, Winter 2003–2004, p. 527.

[28] *Ibid.*, p. 534.

[29] Selig S. Harrison, ''A New Hub for Terrorism?: In Bangladesh, an Islamic Movement with Al-Qaeda Ties Is on the Rise,'' *The Washington Post*, 2 August 2006, p. A15.

[30] Niles Lathem, ''Qaeda Claim: We 'Infiltrated' UAE Gov't,'' *The New York Post*, 25 February 2006, p. 2.

[31] *Ibid.*

[32] Juan Forero, ''Traffickers Infiltrate Military in Colombia; Officers Provided Secret Information On U.S. Navy Ships,'' *The Washington Post*, 8 September 2007, p. A9.

[33] *Ibid.*

[34] Richard J. Aldrich, "Dangerous Liaisons," p. 51, and Seth G. Jones, "Pakistan's Dangerous Game," *Survival*, Vol. 49, No. 1, March 2007, p. 15.

[35] Martin Rudner, "A False Choice in Pakistan," *Foreign Affairs*, July/August 2007, Vol. 86, No. 4, pp. 85–102.

[36] James L. Jones, et al., *The Report of the Independent Commission on the Security Forces of Iraq*, Center for Strategic and International Studies, 6 September 2007, p. 10, at http://media.csis.org/isf.pdf

[37] William Rosenau, *Subversion and Counterinsurgency*, pp. 6–7.

[38] Lisa A. Kramer and Richards Heuer Jr., "America's Increased Vulnerability to Insider Espionage," p. 51. See also Paul Davis, "The Spy is an Eye."

[39] Lisa A. Kramer and Richards Heuer Jr., "America's Increased Vulnerability to Insider Espionage," p. 53.

[40] There remain important exceptions to this generalization, however. For instance, since World War II, the U.S. and the UK (and the wider Commonwealth states) have enjoyed an increasingly and unabashedly open intelligence-sharing relationship.

[41] Chris Clough, "Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence*, Vol. 17, No. 4, Winter 2004–2005, p. 602.

[42] Seth G. Jones, "Pakistan's Dangerous Game," p. 22.

[43] John F. Murphy Jr., "The IRA and the FARC in Colombia," *International Journal of Intelligence and CounterIntelligence*, Vol. 18, No. 1, Spring 2005, pp. 76–88.

[44] Paul Rexton Kan, "Counternarcotics Operations within Counterinsurgency: The Pivotal Role of Intelligence," *International Journal of Intelligence and CounterIntelligence*, Vol. 19, No. 4, Winter 2006–2007, pp. 586–599.

[45] Michelle Van Cleave, "Strategic Counterintelligence: What Is It, and What Should We Do About It?" *Studies in Intelligence*, Spring 2007, Vol. 51, No. 2, p. 4.

[46] Frederick L. Wettering, "Counterintelligence: The Broken Triad," p. 285.

[47] *A Review of the FBI's Progress in Responding to the Recommendations in the Office of the Inspector General Report on Robert Hanssen*, Office of the Inspector General, Oversight and Review Division, U.S. Department of Justice, September 2007, p. 10, at http://www.usdoj.gov/oig/special/s0710/final.pdf

[48] To be fair, many Islamist and other NSA groups operate their own Websites for propaganda purposes and recruiting. For state-level services a Website puts a "public face" on their organization—in part to dispel any conspiratorial suspicions of a shadow government agency operating outside the law.

[49] Martin Rudner, "Hunters and Gatherers," p. 193.

[50] Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," p. 537.

[51] Shlomo Shapiro writes how the U.S. helped to build up the intelligence capability of the Palestinian security forces after the Oslo Accords. See Shlomo Shapiro, ''Intelligence Services and Political Transformation in the Middle East,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 17, No. 4, Winter 2004–2005, pp. 584–585.

[52] *United States of America versus Robert Philip Hanssen*, Affidavit in Support of Criminal Complaint, Arrest Warrant and Search Warrants, United States District Court for the Eastern District of Virginia, Alexandria Division, February 2001. See also Bill Gertz, *Enemies: How America's Foes Steal Our Vital Secrets—And How We Let It Happen* (New York: Crown, 2006), pp. 101–125.

[53] In particular, the report notes ''the FBI has classified the specific monitoring capabilities it has deployed for FBI information systems, as well as additional measures the FBI has taken to address other information security deficiencies.'' *A Review of the FBI's Progress in Responding to the Recommendations in the Office of the Inspector General Report on Robert Hanssen*, p. 22, at http://www.usdoj.gov/oig/special/s0710/final.pdf