From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 20 • NUMBER 3 • $15 SINGLE COPY PRICE
Spring/Summer 2014

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
Web: www.afio.com, E-mail: afio@afio.com

Guide to the Study of Intelligence

Understanding Terrorism Analysis

by Philip Mudd

Intelligence and law enforcement analysis has changed dramatically since 9/11 with dramatically increased interagency fusion of information from a wide variety of sources. Intelligence Community analysts supporting the pursuit of individual al-Qa'ida members and cells have developed tactical skills to supplement their traditional analytical tradecraft focused on strategic assessments of nation states. This change in focus, with its requirement to sort through massive new data sets — from phone and email information to content on social media sites – has led analysts to grow the discipline of network analysis. Analysts adapt rapidly emerging software tools to help make sense of what has become known as "Big Data." This tactically focused analysis, often referred to as "targeting" analysis"[1] was in its inception before the 9/11 attacks. It is now a core analytic function.

Other post-9/11 changes in the analytic profession are proving equally profound. Intelligence Community analysts who previously focused on overseas targets now work together with federal, state, and local law enforcement professionals to confront al-Qa'ida-inspired actors within the US. As the push for information sharing domestically among federal, state, and local entities took shape, cooperation overseas among disparate US agencies also mushroomed. In the war zones of Iraq and Afghanistan, tactical fusion centers, which combine intelligence, military, and law enforcement analysts and operators, undertook data-intensive analyses of networks of foreign fighters and specific terrorist groups on a day-to-day basis. These fusion centers enabled 24-hour raid cycles by the US military, its allies and partners that became a hallmark of real-time efforts to disrupt adversary networks.

Changed Focus of Intelligence

The impetus for this revolution in intelligence analysis, with its emphasis on tactical support, domestic partnerships, and global, real-time fusion among US agencies, reaches beyond the global counterterrorism campaign. At the core of this tactical intelligence work has been the effort to understand sub-national entities and individuals — from foreign fighters funneling suicide bombers into Iraq to al-Shabaab fundraisers in the United States — and the networks in which they participate. As a result of the emergence of the kinds of digital data that emanate from everyday life in the 21st century — from individuals' financial transactions and travel data to the electronic feeds from the ubiquitous communications devices people everywhere now carry — analysts can accelerate mapping people geographically and within networks by rapidly arraying the digital trails they leave. Targeting analysis is here to stay. It has applications that clearly apply to criminal cartels, human traffickers, and gangs. Further, the tools and methodologies that proved increasingly effective in foreign battlefields seem likely to become common practice as analysts confront new networks in the United States and overseas.

This data-intensive analysis, based on new tools to automate the understanding of networks, also has led to changes in analytic culture, with far more analysts embedded with, or supporting, field operators than in previous decades. The need for rapid analysis to feed rapid reaction operations led to more deployments of analysts overseas; closer partnerships between analysts and operators in headquarters units; and the growth of an entire cadre of analyst "targeteers," who built not only careers but also a new analytic profession out of the capability to sort information quickly enough to find, fix, and finish a rapidly moving target in a battlefield environment.

Tactical Fusion of Intelligence Drives Operations

The fusion model was critical on the battlefield, where 24-hour operations centers, manned by analysts and operators from a wide range of US federal agencies and the military, combined SIGINT, tactical and strategic HUMINT, imagery, detainee interrogation reports, and a vast array of data collected in raids (e.g., hard drives, thumb drives, email and phone

1. Targeting analysis uses sophisticated methods to map within a network either potential terrorists or, occasionally, to identify potential sources and their access for recruitment.

numbers) to piece together a steadily changing picture of networks of foreign fighters, facilitators, and insurgent factions. By feeding in and then assessing new information every day, analysts could chart and then re-chart fluid network analyses of networks, prioritizing targets for a next round of raid operations after adjusting the network picture to account for the previous night's operations and the intelligence gained. This tactical analysis proved critical in supporting operators conducting raids against al-Qa'ida and foreign fighter cells around the world.

The fusion model also fed the maturing intelligence architecture surrounding the use of unmanned aerial vehicles (UAV – commonly referred to as "drones") that allowed for enhanced collection against al-Qa'ida targets. The authorization of the use of UAVs for intelligence-led strikes against al-Qa'ida targets in areas such as Pakistan, Afghanistan, Yemen, and Somalia changed the battlefield. Using standoff weapons that did not require US personnel on the ground, drone operations decimated the al-Qa'ida organization and eliminated leaders with unprecedented precision.

Cross Agency and Foreign Partnerships

Strategic analyses in Washington also evolved as a result of the requirement to fuse a wider variety of data sources. The post-9/11 emphasis on "information sharing" among agencies was instantiated by combining analysts and data from across the US government in the new National Counterterrorism Center (NCTC).[2] In the past, analyses that reflected the combined work of analysts from across the Intelligence Community were infrequent, with interagency assessments from the joint National Intelligence Council (assessments such as all-agency National Intelligence Estimates) forming the backbone of episodic and largely strategic interagency cooperation. Today, NCTC produces not only the core US Government appraisals of al-Qa'ida's overall strength but tactical assessments of emerging threats or even new persons of interest who appear to be affiliated with al-Qa'ida.

These cross-agency partnerships today also include agencies outside the defined post-World War II Intelligence Community. The nature of the terrorism target itself drove these partnership changes. In the past, law enforcement might have faced criminal threats in major US cities while intelligence professionals focused on foreign militaries and stability in far-flung capitals. The globalization of threats to reach across borders, so that al-Qa'ida operators in the tribal areas of Pakistan might be communicating with a trainee in a European of North American city, meant that threats simultaneously involving both federal intelligence professionals and US federal, state, and local law enforcement officers became commonplace. Evidence of this mixture of foreign and domestic threats is now spread across the US intelligence landscape, with the rapid growth in FBI-led Joint Terrorism Task Forces (JTTF), which combine a wide variety of agencies, to the posting of NYPD officials in major cities overseas to partner with foreign police services.

The prominence of the US homeland in plots of al-Qa'ida and its affiliates, and, more generally, the political push to involve new entities in the US intelligence infrastructure, from state and local police to US companies and federal agencies responsible for missions such as transportation, border, port, and coastline control, and customs — also led to the creation of the Department of Homeland Security (DHS). This new constellation of agencies, under one roof, is still in the midst of building a capability to partner more with corporations and law enforcement outside the traditional Washington orbit of federal bureaucracies.

Old intelligence partnerships grew as well, with the pace and depth of US engagement with foreign security services expanding in tandem with the spread of the al-Qa'ida ideology to affiliates around the world. During much of the post-war history, the traditional responsibilities of US intelligence was collecting, reporting, analyzing, and disseminating intelligence information on issues ranging from the Soviet nuclear threat to instability in Latin America. With the intensification of counterterror operations worldwide, however, US intelligence focused on identifying, capturing and detaining terror suspects. In this the partnering and support for foreign security services proved crucial. These services not only provided substantial support in the global counterterror campaign – and often unique intelligence from surveillance against terror targets in their countries and human sources (HUMINT) inside terror organizations — they also grew substantial capabilities internally, sometimes with financial, technical, and training support from US agencies.

Detainee information mushroomed during the

2. A variety of study groups after 9/11, particularly the 9/11 Commission, highlighted the fractured, stovepiped nature of the US Intelligence Community, with its separate data pools and chains of command at major components including CIA, DIA, NSA, State Department, the FBI, and the various intelligence-generating components of what would become DHS (including intelligence drawn from customs, immigration, transportation, and border control agencies).

post-9/11 period, including both tactical information from fighters detained on the battlefield, in Iraq and Afghanistan, and the intelligence provided by "high-value" al-Qa'ida members held at "black sites" — secret facilities overseas — maintained by the CIA to hold prisoners that it and partner security services had captured in overseas raids. As the number of senior al-Qa'ida members in detention increased, detainee information, coupled with traditional HUMINT, SIGINT and intelligence provided by friendly security services, provided a rapidly clarifying picture of the al-Qa'ida network, and the damage the core group suffered as its leaders tried to recreate their group in the tribal areas of Pakistan.

In another twist in the secret world of intelligence, US industry became a key consumer of intelligence information and analysis, and various US agencies built mechanisms to foster contacts and information sharing between the federal government and US companies. Terrorists looking for iconic targets, from aircraft to major oil facilities, hotels, and retail outlets, drove industry to grow its own internal threat units, and to reach out to government to learn more about how terrorists might target the private sector.

The Changing Threat From Al-Qa'ida

This drive to share information nationally, among federal, state, and local agencies that had not been close partners, grew out of the changed threat facing the United States. From intelligence operations in Vietnam in the 1960s through the continuation of the Cold War through the 1970s and 1980s to the later focus on "rogue" states (e.g., Iran, North Korea, and Iraq), the US Intelligence Community had focused on large foreign threats operating overseas. There was not much need to work with state and local partners, nor to target collection against potential threats domestically. Historically, in the world of terrorism, the domestic and the international worlds did not overlap: domestic terrorism in the United States during the 1970s was high, but groups lacked an international nexus. Conversely, Palestinian groups in the 1970s and beyond, and state sponsors of terrorism (most prominently Iran, sometimes working through its ally Lebanese Hizballah), typically operated overseas.

The advent of al-Qa'ida and its affiliates in countries from the Philippines through South Asia, the Middle East, Africa, and Western Europe, bridged the gap between domestic and foreign terror. Al-Qa'idist ideology emphasizes the importance of attacking the "far enemy" (including the United States) rather than expending energy on the "near enemy" (local governments such as those in North Africa and the Arabian Peninsula). The theory is simple: if al-Qa'ida attacks can inflict enough casualties to persuade the United States to withdraw its forces (as it did in Lebanon and Somalia) from Muslim countries, the corrupt leaders of those countries then would lose US backing and thereby become more vulnerable to Islamist overthrow. So al-Qa'ida brought attacks to the US homeland, under the assumption that the US would not have the will to maintain an overseas presence in Islamic countries after taking casualties in terror attacks.

This melding of domestic and overseas threats became more complex as the decade of the 2000s progressed. In the wake of the attacks in 2001, the primary intelligence focus remained overseas, penetrating the core al-Qa'ida leadership in Pakistan to try to stop plots emanating from that tight group. As the decade passed, though, more affiliated organizations — groups that adopted al-Qa'ida's ideology but retained some independence of action — cropped up, expanding the potential threat to US interests overseas and raising the specter that these new affiliates would take the initiative from the embattled al-Qa'ida core to stage attacks in the United States. The failed attempt by Faisal Shahzad to detonate a vehicle-borne improvised explosive device in Times Square on May 1, 2010 underscored this emerging threat from affiliates: Shahzad's plot was sponsored by a Pakistani militant organization (Tehrik-e Taliban Pakistan — TTP) that was affiliated with, but not a part of, the al-Qa'ida organization.

Controversies

The change in threat and the US counterterror response has not been without controversy. The blurring of domestic and international lines, in the age of globalized terror organizations, led to changes in the intelligence business, and questions about what the government should collect in a digital world. The revelations of former NSA contractor Edward Snowden about the extent of National Security Agency (NSA) collection of information, such as domestic phone and email data, has led to a national debate — along with Congressional scrutiny and potential legislative changes — about how much data the government collects on its own citizens. The collection itself stemmed from the government's interest in combing through these new, vast data collections to find link-

ages within the US as new plots, and new players, emerged. This data allowed for an unprecedented ability for government analysts to automate how they map networks, and to make connections across vast data warehouses that would have been unthinkable in the previous century.

The operation of "black sites" by CIA and harsh interrogation techniques on detainees have also been controversial both in the US and in other countries.

The use of UAVs armed with weapons also ignited debates, about the use of lethal force outside war zones[3] and the future of US intervention against targets in ungoverned spaces, such as extremist-inhabited areas of Africa.

The Future

While the attraction of al-Qa'ida has declined in the group's key recruiting and fundraising areas during the past decade, from Indonesia to Saudi Arabia and the United Kingdom, the persistence of its now-globalized ideology will challenge security services, including those in Europe and the United States, to remain focused on al-Qa'ida spinoffs for years to come. Al-Qa'ida hotbeds remain in key areas, from the Sunni extremist groups in Iraq to al-Qa'ida's sympathizers in Pakistan, Yemen and north Africa. Further, Syria now serves as a magnet for foreign fighters, including hundreds from Europe, raising the prospect that those fighters will gain contacts and experience that they will transfer west when that campaign dies down.

The success or failure of governments to control these battlegrounds — and to limit the chances that al-Qa'ida offshoots will find safe havens that will allow them to plot against the West, as groups in Yemen and Somalia have done in recent years — will hinge on the question of whether governments show the will and capability to disrupt safe havens. In Somalia and Yemen, for example, government forces' sustained operations against entrenched al-Qa'ida affiliates have resulted in significant pressure on extremist groups and their leaders. They then are forced to spend their time and resources defending local territory, with less time to develop foreign-focused terrorist wings.

Counterterrorism analysis will remain a requirement for years to come. While the large, centralized al-Qa'ida adversary has declined, newer spinoffs have adopted the group's globalist ideology. The threat from these groups has ebbed and flowed during the past decade, with hotspots moving from Indonesia and Saudi Arabia to Iraq, Western Europe, Somalia, Yemen, and northern Nigeria and the Sahel. The threat will continue the need for interagency analysis and tactical support for operations. The models developed to counter al-Qa'ida might well serve as templates for the intelligence-led fight against adversaries of the future, such as cartels, human trafficking groups, or cyber criminals. For all the questions as these new intelligence approaches and tools have raised, though, the US Intelligence Community is facing new, still-unresolved, questions about the nature and extent of intelligence operations in America.

The analytic approaches developed for counterterrorism, though, also are driving the public debates about the role of intelligence in democratic societies. The extent of data collection, in an age when individuals around the world freely expose more and more personal information on the Internet, is raising questions about how the digital age will redefine privacy. Unlike the debate about physical privacy — we expect searches in airports, but we would resist a similar search in a grocery store — debates about cyber privacy have not reached the stage where culture has defined boundaries. Camera footage on a public street has become an accepted source of intelligence; personal information on a Facebook page is more questionable. These debates will not slow. Intelligence agencies seeking to identify new threat networks will turn to whatever data is available as the fastest way to map connections among individuals.

Expanding public and political expectations for intelligence and law enforcement also will drive policy and controversy in this era of tactical, data-driven analysis. Preemption has become the standard for intelligence and law enforcement today: public expectations have evolved quickly, and investigating a terror cell after an attack, rather than uncovering the cell beforehand, is seen as a failure. This pressure to develop preventive intelligence will drive law enforcement agencies to use technical and human intelligence to uncover conspiracies before they fully develop, and questions about preemptive investigative techniques, such as human sources who help to advance a plot, will continue in parallel with the emphasis on preemption.

3. The traditional American definition of a war zone does not fit well with modern globalized terrorism. The concept of a war zone, historically defined by geographical boundaries, figures prominently in legal arguments on the use of force. Terrorists, however, move across national boundaries.

READINGS FOR INSTRUCTORS

The website for the Director of National Intelligence (DNI – www.dni.gov) describes the mission, functions and history of the National Counterterrorism Center. The NCTC's own homepage (*www.nctc.gov*) lists the various partner agencies that man this interagency entity (although some aspects of this website are out of date).

Michael Bayer, the former head of the Department of State's transnational criminal investigative section of the Diplomatic Security Service, addresses the issues of partnerships between law enforcement and intelligence. He critiques the primacy of the US military approach to counterterror operations over international law enforcement. See Michael D. Bayer, *The Blue Planet: Informal International Police Networks and National Intelligence*, Washington, DC: National Defense Intelligence College Press, February 2010.

For a wide-ranging review of legal issues related to counterterrorism, see Lynne K. Zusman (ed.), *The Law of Counterterrorism*, Washington, DC: American Bar Association, 2011. Of particular note is Chapter VII, "Intelligence and the Law: Introduction to the Legal and Policy Framework Governing Intelligence Community Counterterrorism Efforts," by W. George Jameson, former CIA general counsel.

Annual country reports on terrorism can be found on the Department of State website (*http://www.state.gov/j/ct/*).

The United States Military Academy at West Point maintains the Center for Combating Terrorism. Its journal, *Sentinel*, includes articles on terrorism, counterterrorism, homeland security and internal conflict.

Georgetown University professor Bruce Hoffman's *Inside Terrorism* (revised edition), (New York: Columbia University Press, 2006) remains one of the fundamental texts on the subject.

John Horgan, director of the international center for the study of terrorism at Pennsylvania State University, and Kurt Braddock have edited a series of articles on terrorism and counterterrorism in their *Terrorism Studies: A Reader* (New York: Routeledge, 2012) that provide a wide-ranging look at the topic.

A number of institutions maintain databases on terror incidents. These include the University of Maryland (*http://www.start.umd.edu/gtd/*), which is supported by the Department of Homeland Security; the RAND Corporation (*http://www.rand.org/nsrd/projects/terrorism-incidents.html*), and others.

Philip Mudd is Director of Global Risk at SouthernSun Asset Management, in Memphis, Tennessee. He served as Senior Intelligence Adviser at the FBI until 2010, and he was Deputy Director of CIA's Counterterrorist Center during 2003-05.