

## **Reflections on 10 Years of Counterterrorism Analysis**

*Jeffrey A. Builta and Eric N. Heller*

---

“  
***Those in the CT community have had nearly a decade of creative experimentation and learning, which has led to equally, if not larger, changes [than those mandated by commissions].***  
”

### ***Introduction***

Numerous government commissions, academics, book writers and journalists have dissected the 9/11 attacks and focused on the presumed failure of intelligence to disrupt al-Qa'ida's attacks. These examinations have played a role in reshaping the look, feel, operation, and, particularly, the bureaucracy of the counterterrorism (CT) community and, by extension, the larger Intelligence Community (IC).

At the same time, those in the CT community have had nearly a decade of creative experimentation and learning, which has led to equally, if not larger, changes. Perhaps more than any conflict of the modern era, the war on terrorism has required operators to depend on intelligence for a range of requirements, from defining the enemy to determining and targeting their critical vulnerabilities. Along the way, the IC has had to adapt old processes and develop new ones to improve effectiveness, efficiency, and accountability.

The operation that resulted in Usama bin Ladin's death in May 2011 has generated much-deserved congratulation throughout the IC. Bin Ladin's death, the result of sustained cooperation and focused long-term analysis, demonstrates the impact of bringing to bear disparate relationships, organizational constructs, and capabilities throughout the CT intelligence community. Nevertheless, euphoria over the monumental event should not prevent a dispassionate analysis of the IC's progress over the past decade or its continued shortfalls. A decade after 9/11, we, as experienced practitioners in the CT field, offer answers to four questions that we believe provide the measure of the CT intelligence community's—particularly Defense Department's—adaptation since 9/11.

- How has the IC adapted its information-sharing practices to meet the amount, pace, variety, and disparate sensitivities of information collected?

---

The endnotes for this article can be found in its digital version on [cia.gov](http://cia.gov).

---

*All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.*

---

---

*In terrorism, perhaps more than in any other kind of conflict, tactical events and data have strategic impact.*

---

- How has the IC's analytic cadre adapted to meet the evolving adversary?
- What organizational constructs have proven successful?
- How has the IC changed to address the CT issue as a holistic problem, as opposed to a narrow problem of hunting high-value targets (HVT)?

Each of these questions could be addressed separately, but because we believe the answers are so intertwined we will look at them together, in the following broad areas: how the IC has responded through integration, fusion, diffusion of information flows, and cooperation via centralized mission sets and broadened situational awareness. We contend the IC has some answers to the questions above, however, the current state of the CT intelligence community and the degree of institutionalization of best practices leaves much room for progress.

The expression "lessons learned" is a common and recognizable nomenclature, in actuality, most of the practices we will describe could more properly be termed "lessons relearned" or "lessons reinforced," as few are completely new to the IC. Most have been cultivated and successfully employed by small intelligence organizations supporting spe-

cific operations for the better part of three decades. Unfortunately some of best practices were learned long ago and scrapped, only to be resurrected after a terrorist attack or attempted attack. Employing these practices today, collectively across our broad CT enterprise, will require another level of implementation and institutionalization.

Some readers may perceive in our insights lessons mainly for tactical, rather than strategic intelligence support. In terrorism, perhaps more than in any other kind of conflict, tactical events and data have strategic impact. The tactical success or failure of one counterterrorism operation and the resulting insights could, and frequently do, have strategic consequences for the United States and its allies.<sup>1</sup> Thus, the high-risk nature of today's terrorist adversary inherently blends traditional levels of war—strategic, operational, tactical—and makes these lessons applicable to all levels of counterterrorism professionals. Moreover, the obligation of intelligence organizations to deliver actionable intelligence to affect tactical CT targets in the near-term continue to be levied along with long-range, threat estimates intended for executive, policymaking levels.<sup>2</sup>

---

*Improvements in intelligence sharing and new information sources have been leveraged, but shortcomings in these areas continue to impede mission success.*

Our most important and persistent challenge is the need to continually enhance the amount and quality of intelligence available to CT operators and planners and to more efficiently share that intelligence among key players. Multiple recommendations within the 9/11 Commission Report centered on issues related to information sharing, but within Defense intelligence, lack of sharing remains the most-often cited impediment to mission success in the CT arena.<sup>3</sup>

Experience in the war on terror has reinforced the importance of making intelligence data available to all elements of national power. The data available—and conversely the intelligence gaps that exist—determine where an element of national power expends intellectual energy, finite analytic capacity, and collection resources. The availability and precision of information needed for counterterrorism operations and to track diffuse transnational terrorist networks have expanded to a level not dreamed of prior to 9/11. This development has reinforced for many counterterrorism intelligence professionals that the

need to share intelligence must trump the old paradigm that put protection ahead of sharing. Codifying this notion, the 2008 US Intelligence Community Information Sharing Strategy demanded a shift in mindset from “need-to-know” towards “a responsibility to provide.”<sup>4</sup>

In the deployed and intelligence task force environments created to carry out the intelligence operations in this conflict, information sharing often works well, driven by a sense of shared purpose based on operational urgency, mission focus, and personal relationships that form in these environments. Moreover, rapid feedback on intelligence analysis culminating in CT successes provides tremendous satisfaction and reinforces effective information sharing practices.

Historically, lessons in information sharing have been learned and relearned through tragic circumstances. Following the 2000 attack against the *USS Cole* in Aden, Yemen, the Cole Commission recommended that the secretary of defense embed analysts from the national, commander-in-chief (CINC) (now, Combatant Command)-level, and component command level to the joint task force level.<sup>5</sup> The Downing Commission Report, which investigated the 1996 attack against Khobar Towers in Saudi Arabia highlighted the

---

*In the deployed and intelligence task force environments created to carry out the intelligence operations in this conflict, information sharing often works well.*

---

need for fusion centers to combine national intelligence with local intelligence collection and provide the result to tactical forces. This was to enable pattern identification, prevent information from falling through cracks, and focus US and allied intelligence services on the same pieces of information at the same time. Equally important, the function emphasized timely delivery of useful information to the tactical commander.<sup>6</sup> Then Maj. Gen. Michael Flynn, G2 of NATO forces in Afghanistan, wrote in 2010 about the need to increase US and allied focus on population-centric intelligence and described the CT successes that resulted from work on enemy-centric intelligence carried out in fusion centers in Iraq and Afghanistan.

*By assembling bright, capable individuals under the same roof, Fusion Centers were able to coordinate classified SIGINT and HUMINT, and real-time surveillance video, allowing commanders to “action” the information with airstrikes and special operations that led to the death or capture of notorious terrorists... The concept has been replicated [from Iraq] in*

*Afghanistan and has achieved important successes.<sup>7</sup>*

Recently, however, we have been reminded of the information-sharing challenges that continue to hinder force protection, even within the continental United States. A congressional report on the attack against Fort Hood personnel by Maj. Nidal Hassan found that

*DoD and FBI collectively had sufficient information necessary to have detected Hasan’s radicalization to violent Islamist extremism but failed both to understand and act on it... Specific and systemic failures in the government’s handling of the Hasan case [raises] additional concerns about what may be broader systemic issues.<sup>8</sup>*

In Washington, the establishment of the Terrorist Threat Integration Center in 2004 and then the National Counterterrorism Center (NCTC) represented starts of this kind of fusion at the national level. In NCTC the US government has worked through legal, technical, security, and policy issues and brought more than 30 intelligence networks into one shared environment—and

---

*When analysts complete deployments or interagency task force assignments and return to jobs at their home agencies they rarely keep the level of access they had enjoyed.*

---

information is shared well within the building.<sup>9</sup> This unprecedented access has helped to ensure that NCTC analysts have as close to all the information available to the US government on a given topic as is possible.

Because of the agreements the center has made with the agencies and departments providing the networks, however, the data access in NCTC is largely physically bounded within its property. Even with these accesses, most analysis remains focused on production supporting policymakers at the most senior levels of the US government.<sup>10</sup> However, those mandated to support forces operating against terrorists—those who seemingly need the highest level of fidelity of information—sit outside NCTC, at CIA, DIA, the Combatant Commands, FBI, and elsewhere. In addition to hindering analysis, such an arrangement can create an “us versus them” environment in which professional tensions fester.

Despite what is frequently trumpeted as major success in information sharing, the practical reality for most IC analysts is that information sharing among CT intelligence organizations is in many ways no further along in sum than it was

on 10 September 2001. To be clear, the information sharing challenges today are different from those that existed before 9/11. Since then, the volume of intelligence data available to all analysts has expanded dramatically. While some of that expansion has been the result of policy and process improvements, much more of it resulted from expanded collection capacity and emphasis. Consequently, many of today’s problems are rooted in the problem of having too much data, too many diverse stovepipes creating it, and difficulties in scrutinizing the abundance across unique data sets. Nevertheless, information-sharing still is hampered by too many restrictions against sharing high-value data with the wider, expert CT analytic community because of operational concerns.

Some of the concerns about sharing operational data are justified, but too often the concerns seem to be based on perceptions without foundations, with the result that useful material is denied to the broader CT analytic community. In the field, these barriers tend to break down and the sharing of data within deployed and task force environments is good, but dependence on such environmental factors does not

represent a systemic solution to the problem, as can be seen by the fact that when these analysts complete deployments or interagency task force assignments and return to jobs at their home agencies they rarely keep the level of access they had enjoyed.<sup>11</sup>

Personal relationships and practices in a particular building in Northern Virginia are not a systemic answer to the problems laid out by the 9/11 Commission. Instead, we must build on the successes we have had to deploy information architecture and cross-domain data sets to secure CT communities of interest (sets of analysts covering the same or similar CT issues) managed by, but outside of, NCTC. Such an effort should include cross-leveling common databases and tools across the CT community, a community that already must deal with more databases than analysts can reasonably be expected to use.

In his July 2011 confirmation hearing, Director of National Intelligence (DNI) James R. Clapper noted the need for a single repository of terrorism-related data as a foundation against which a variety of sophisticated technologies and tools could be applied. Clapper described it as a robust search engine that could range across a variety of data and data constructs to help connect information. At present, Clapper

commented, the IC is spending too much manpower doing manually things that could be done by machines.<sup>12</sup>

We can achieve fundamental improvement in our intelligence structure in relatively short order by mandating data access across a defined, audited, and controlled—but distributed—intelligence community-of-interest, modeled on the success at NCTC, so that CT intelligence professionals have equal access to terrorism data, within reasonable need-to-know parameters, in Langley, Washington, Stuttgart, Baghdad, Kabul and wherever else our expertise is deployed.

Analysis of recovered documents and media have been key to successes, but they are likely to become diminishing assets. Intelligence gleaned from detainees and from captured documents and media has been key to US CT success for nearly a decade now. This kind of data accounts for the single largest boon to CT analysis and operations, providing information unavailable before operations began in Afghanistan and Iraq. Indeed, countermeasures taken as a result of document, media, and detainee exploitation have contributed to preventing a repetition of a large-scale attack in the United States.

Exploitation of such sources has also been crucial to countless tactical CT operations in

---

*Analysis of recovered documents and media have been key to successes, but they are likely to become diminishing assets.*

---

Iraq, Afghanistan, and other locations. It has also provided unprecedented insights into the inner workings of al-Qa'ida that form the baseline of our strategic knowledge of the network.

The work of the US Military Academy's Combating Terrorism Center with its Harmony database is an exemplar of the insights on terrorist groups, networks, and ideology captured documents provide.<sup>13</sup> In 2007, the center produced a report entitled *Al-Qa'ida's Foreign Fighters in Iraq*, which was based on a cache of recovered documents detailing the processes and personnel involved in facilitating the movement of foreign fighters into Iraq in support of al-Qa'ida in Iraq. The report provided information about the flow rates of foreign fighters, their identities, and their home countries. Moreover, the type of information in those documents could have been used to identify and target terrorists and disrupt terrorist attacks elsewhere. Other notable examples include the exploitation of information contained in laptops that had belonged to senior members of al-Qa'ida and which were procured in the fall of 2001. The contents of these computers included communication among senior leaders, budgets, training manuals, reconnaissance reports, bureaucratic squabbles, and theologi-

cal debates, all providing strategic insight into al-Qa'ida's inner-workings.<sup>14</sup>

Our current short-term challenges in this area center largely on maintaining sufficient resources—such as translators, analysts, and technologies to process and analyze this material. However, we should note we are beginning to face larger challenges that will increase in the mid- to long-term. These center on diminishing US advantages in this area. Among them are greater terrorist awareness of our exploitation capabilities and the looming end of combat operations in Iraq and eventual troop reductions in Afghanistan. These events will diminish media and document exploitation and detainee interrogation opportunities. A recent study by the Center for a New American Security, though focused on intelligence networks, is easily extrapolated to media exploitation and detainee interrogation:

*A second-order effect of the rapid withdrawal of military forces from Afghanistan is the probable collapse of intelligence networks on both sides of the border that currently enable targeted counterterrorism operations. The presence of US forces in Afghanistan, closely work-*

---

*In order to sustain counterterrorism operations in the most efficient and effective ways possible, the IC has developed and institutionalized a coherent and consistent process to make intelligence operationally useful for counterterrorism forces.*

---

*ing with the local population as well as allied security services, maintains an irreplaceable intelligence infrastructure in support of continued operations. Targeting transnational terror groups becomes nearly impossible without the intelligence provided by networks on the ground.<sup>15</sup>*

---

*Evolved processes and empowered analysts have driven the CT mission forward: the future CT environment will challenge business methods.*

In order to sustain counterterrorism operations in the most efficient and effective ways possible, the IC has developed and institutionalized a coherent and consistent process to make intelligence operationally useful for counterterrorism forces. The method is a continuous, non-linear cycle of “finding, fixing, finishing, exploiting and analyzing” (F3EA) targets.<sup>16</sup> In this cycle intelligence drives operations, which, in turn produce new intelligence for new operations. The four steps are shown in the figure on the right. Identify a critical node, develop intelligence to target it, employ an element of national

power, and finally, gather intelligence related to how components of the targeted network react, using the new intelligence for future, generally near-term, CT actions. These concepts can also be applied to CT targets addressed by other elements of national power—political, social, economic, or something else.<sup>17</sup>

The need for a standardized process is driven in part by the *granularity of intelligence required to support current CT operations*. Counterterrorism commanders require a high level of shared situational understanding, delivered with unprecedented speed and accuracy. Terrorism targets are very granular by nature, and often fleeting. This requires optimal use of all-source analysis and collection, to include persistent intelligence, surveillance, and reconnaissance tools.<sup>18</sup>

The F3EA process, a tactical process supported by operational and strategic elements, nests into larger strategic frameworks of terrorist networks. Through the F3EA process, all facets of a terrorist network are collected, analyzed, and intelligence products prepared. The reliance by terrorists on global travel and communications are also vulnerabilities that the United

States can exploit in preventing terror attacks and degrading networks.<sup>19</sup> As described by the 2003 US National Strategy for Combating Terrorism,

*The terrorist threat is a flexible, transnational network structure, enabled by modern technology and characterized by loose interconnectivity both within and between groups. In this environment, terrorists work together in funding, sharing intelligence, training, logistics, planning, and executing attacks... The terrorist threat today is both resilient and diffuse because of this mutually reinforcing, dynamic network structure.<sup>20</sup>*

Employing the F3EA process against those layered processes and network components, including those that give terrorist networks their resilience and facilitate travel, finance, and communications of operatives and their leaders, is and has been essential for effectively combatting terrorists.

The United Kingdom’s success in August 2006 in stopping a planned attack against several airliners and the Christmas Day 2009 “underwear bomber” attempt against a Northwest Airlines flight to Detroit provide interesting contrasts. The UK plot was disrupted because of successful

surveillance and sharing of data among the UK's counterterrorism departments and agencies and the United States and Pakistan.<sup>21</sup> The Christmas Day attempt failed because of the terrorist's own limitations. That he got as far as he did was at least partially a failure to connect data points in intelligence channels and in some data sets not traditionally considered CT intelligence.<sup>22</sup>

In congressional testimony following the Christmas Day incident, one witness highlighted the range of information available, which in isolation might not have been thought of as "counterterrorism" information. Some of these data sets included passenger manifests, flight paths, as well as other information such as method of payment, whether luggage was taken, and co-travelers, which in aggregate provides valuable clues to aid terrorist threat analysis.<sup>23,24</sup> As another expert testified in the wake of the UK disruptions, "the West built these networks and must find ways to use them against terrorists more effectively than the terrorists use them against us."<sup>25</sup> The persistent challenge in exploiting this kind of information continues to be making it available for CT purposes while at the same time protecting civil liberties of innocent travelers.

The institutionalization of the F3EA process and its use across



the CT enterprise has generated critical successes for the US and its allies, but as restrictions on unilateral US CT operations grow, along with troop withdrawals in Iraq and Afghanistan, even greater precision will be needed. Similarly, enhancing the accuracy of intelligence inputs into the cycle and maximizing intelligence gain following operations will be of utmost importance.

There are two separate but parallel phenomena that threaten the effectiveness of the F3EA process: resource constraints and withdrawal from conflict zones. Because the potential political consequences of CT operations outside of combat zones are high—especially so in today's

resource-constrained environment—arguments against conducting such operations will be more powerful. Second, as noted earlier, the diminished intelligence resulting from US withdrawals from the conflict zones will have adverse effects. In this environment, the CT community would be faced with trying to find ways to compensate for decreases in intelligence resulting from a diminished presence and operations in conflict areas.

As the intelligence processes supporting counterterrorism efforts have evolved, so too have the roles of intelligence analysts. Arguably one of the most vital of these changes has been the tethering of analysts to their "finishing forces."

---

*The key for analysts and their managers is to balance development of long-term subject matter expertise with support for the dynamic priorities of policymakers and operational elements.*

---

Whether this “force” is a policymaker, law enforcement official, collector, or military operator, analysts must be acutely aware of the decision cycles and intelligence requirements of that force. Put another way, analysts must simply know for what purpose they are producing a given product. Not every product can or should translate into a direct operational decision.

In this context the report of the Downing Commission should be remembered. Assessing intelligence reporting before the Khobar Towers attack, the commission criticized the singular focus on current events and the distribution of an amalgamation of threat reporting, surveillance incidents, and general advisories. The commission concluded that the military intelligence community lacked a sufficient, in-depth, long-term analysis of trends, intentions, and capabilities of terrorists.<sup>26</sup> The key for analysts and their managers is to balance development of long-term subject matter expertise with support for the dynamic priorities of policymakers and operational elements.

Additionally, because of the fidelity and complexity of intelligence supporting CT actions, all-source analysts have

learned the intricacies of single-discipline collection from their HUMINT, SIGINT, IMINT, OSINT, GEOINT counterparts; they have learned what questions to ask to accurately confirm or deny reporting and to drive further collection. By more accurately and completely understanding targeting and collection, they can more accurately guide these systems and in turn provide more useful intelligence to both efforts.

Another element of the CT, to be addressed in more detail later, involves analytical support to operational efforts to address the environmental factors that lead to terrorism and the efforts of local foreign leaders to address the problem. This kind of analytical support also provides the strategic framework for an “all-of-government” approach that will allow movement beyond the “whack-a-mole” approach to manhunting. Understanding of environmental factors demands of CT analysts understanding of issues beyond those involved in simple targeting. To gain expertise in these topics CT analysts have needed to work with geographical and functional experts and with organizations that can provide political, military, ideological, social, and economic information and analysis

as it relates to counterterrorism.

Finally, many CT professionals have developed simultaneously as strategic and tactical analysts. Reflecting the networks they investigate, through consistent movement between deployed operational and tactical-level units and back to headquarters, as well as with various IC agencies and policymaking venues in Washington, DC, analysts gain the skills to support tactical CT operators, collectors, *and* policymakers. As policymakers have become attuned, so too have analysts recognized the strategic relevance of tactical developments, leading them to think about how they can tailor their follow-on analysis, both to the most tactical operators and the most senior policymakers.

---

*Focused organizational constructs and international cooperation to address counterterrorism networks have been vital, but these mechanisms and relationships need to be institutionalized.*

Collaboration works best in situations in which analysts and operators (the intelligence consumers) are co-located as close to their targets as practicable. Joint Inter-Agency Task Forces (JIATFs) and similar organizations abroad are exemplars of effective interagency

activities overseas. Interagency integration can take place virtually, but such approaches are generally harder to make truly effective in the absence of physical ties into operational environments. In order to be most effective, CT organizations must have forward-deployed components as well as rear-garrison support. When they do, forward and rear area people can collaborate on analysis of common problems and can offer tailored support both to deployed CT forces and to policymakers at home.

Complementing deployed analysts, a cadre of formal liaison officers (LNO) has been optimized and professionalized. LNOs establish new network nodes and thicken the existing network, both on the battlefield with the battlespace owners and throughout the community of agencies involved in the CT fight. The record of today's LNOs shows that the custom of filling liaison positions with less-capable employees is a thing of the past.

Getting interagency integration right depends principally on engagement, and leading through continuous engagement is one of the most critical roles for CT managers. This function, however, places heavy costs on organizations. One of them is the personnel grind; a second is the demand for continuity. Professionals in CT organizations are in a constant

---

*Complementing deployed analysts, a cadre of formal liaison officers has been optimized and professionalized.*

---

state of deployment, recovery, and preparation for redeployment. In addition, to be effective, CT managers require a 24/7 reachback capability to subject matter experts, an interaction that places heavy demands on those at home to maintain situational awareness through a rigorous schedule of regular video teleconferences and other means to discuss developments and operational planning.

Experts at home are well-positioned to research and present the strategic picture in which tactical operations are, or should be, developed. When optimized, a continual cycle of analysts from headquarters to the field and back ensures a cadre of deeply knowledgeable CT experts, capable of operating at strategic and tactical levels and sensitive to the requirements of both.

Notwithstanding the costs of the CT effort, inevitably intelligence managers are asked to continue to support their agency's own organic production and priorities, a difficult challenge in light of the demands of CT work. In today's resource environment, this tension is unlikely to change as the focus on CT activity, deployments, and rotational assignments remain the norm. Thus,

today's intelligence officers must be trained to work in all sorts of environments, from war zones to the White House and many places in between. Despite the costs to the other priorities of home agencies, the intelligence, insights, experience, and skills gained by intelligence officers engaged in CT-related support activities, far outweigh the costs of providing it. Furthermore, deployments to joint operational components exemplify the spirit of the ODNI's Joint Duty Program as professional development vehicles, cultivating cross-organizational networks, expanding knowledge of IC programs and operations, and facilitating information sharing.<sup>27</sup>

The same principles for improving and maintaining the collaboration of agencies and departments—i.e., co-location in physical or virtual environments—should also apply to individual analysts, operational planners, and collectors. As the IC has pursued integration and collaboration, we have and must continue to de-emphasize internal boundaries between disciplines and agencies and focus on the CT mission.

Within the CT community, the benefits of fusing operations and intelligence have been real-

---

*The results have been improved accuracy, credibility, relevance, and responsiveness of analysis and collection.*

---

ized in a number of examples, including movement toward fusion efforts in the Defense Intelligence Agency after the October 1983 attack against the US Marine unit in Beirut and creation of CIA's Counterterrorism Center in the late 1980s.<sup>29 28</sup> In the latter, elements of the CIA's directorates were brought together and directed against the CT problem. The IC's response to 11 September and lessons learned during Operation Iraqi Freedom greatly expanded the fusion of operations and intelligence. The Department of Defense doctrinally instituted some of these lessons into Joint Intelligence Operations Centers as the vehicle to combine intelligence disciplines and operations.<sup>30</sup>

The results have been improved accuracy, credibility, relevance, and responsiveness of analysis and collection. The measures have enhanced the ability of the IC to drive and focus collection to support all-source analysis by improving the quality of reporting, providing more informed oversight of the vetting of sources, making collection more responsive to fleeting targets of opportunity, and creating hybrid all-source targeting officers.

Despite the success in bringing operations and intelligence professionals closer together,

there remain impediments to intelligence support to prosecutorial and law enforcement efforts. While our expertise is limited to the CT experience within defense intelligence, we believe lessons learned by law enforcement deserves its own treatment by practitioners in that field. Still, we hold that there are opportunities and challenges that persist at the seams of defense intelligence and law enforcement.

Interpretations of legal restrictions and evidentiary chain of custody issues continue to impede defense CT intelligence from providing intelligence and operational opportunities to law enforcement partners where military options are not possible or prudent. Although some positive steps have been taken, such as the formation of the fusion centers and coordination groups to provide information to INTERPOL, as well as to CONUS-based state, local, and tribal law enforcement, gaps remain in timeliness, access, and fidelity of information. Some efforts have been heralded as driving a level of unprecedented connection between field personnel, providing extremely high levels of situational awareness. Others describe federally-coordinated intelligence products as not meeting the needs of local law enforcement in terms of

subject matter or timeliness. Especially during international terrorist events, local US leaders rely upon the media more often than from the reporting of government officers overseas.<sup>31</sup>

<sup>32</sup>

Any one nation's counterterrorism programs or organizations will not by themselves prevent attacks by terrorist networks spread across the world. The threat to the US homeland frequently emanates from terrorists operating in areas in which the United States lacks authorities or access. Many of our successes today and in the future will rely on our ability to quickly disseminate specific, reliable intelligence on terrorists to foreign partners and to convince them to act on our information.

Another trend that speaks to the need for international cooperation is the growth of local extremists with global ambitions. As al-Qa'ida expands its influence via franchise endorsements of regional terrorists in Pakistan, North Africa, Yemen, and Iraq, we have seen groups elsewhere change their targeting criteria and strategic views to resemble al-Qa'ida's anti-Western outlook.<sup>33 34</sup> For example:

- The failed effort of the Christmas Day 2009 operative Umar Faruq Abdulmutallab reflects an increasing threat from al-Qa'ida's regional affili-

ates, in this case from al-Qa'ida in the Arabian Peninsula.<sup>35</sup>

- The attempt of Faisal Shazad to explode a vehicle bomb in Times Square in New York City in May 2010, highlights the close ties Tehrik-e Taliban in Pakistan maintains with senior al-Qa'ida leaders, the critical support TTP provides to al-Qa'ida, and the shared radical, global goals of both networks.<sup>36</sup>

Two CT successes involving international cooperation during the past decade demonstrate the importance of international intelligence partnerships. One was the aforementioned disruption of the plot to blow up airplanes coming from the UK in 2006. A second, more recent, example was disruption of terrorists' attempts to ship improvised explosives devices as air cargo in 2010.<sup>37</sup> A consistent application of cooperative efforts in the years to come, will require, in our judgment, use of the same techniques for integration and fusion of intelligence efforts with foreign partners that we have used in US CT intelligence operations.<sup>38</sup>

We believe, much of the burden for success in this area lies with the US Intelligence Community rather than with our foreign partners—who, along with local law enforcement, should be seen as another set of

---

*in the long-term, the US government's ability to understand and address—or enable others to address—the root causes of terrorism will also depend on our ability to collect, analyze, and carry out activities that shape the environments from which terrorists and their networks emerge.*

---

“finishing forces.” With expanded international cooperation comes several challenges, among which are cultural bias within the IC, overclassification, and variations in how the United States and its international partners perceive threats. And while expanding the CT network to international partners inherently increases the risk of compromises of secret information on both sides, the benefit of and need for their support and actions must outweigh these risks.

---

*Addressing terrorism effectively means addressing root causes and providing intelligence support to efforts to address them.*

Intelligence and operations targeting the activities, locations, identities, social networks, and operational planning of terrorists will continue to be critical in the fight against terrorists. However, in the long-term, the US government's ability to understand and address—or enable others to address—the root causes of terrorism will also depend on our ability to collect, analyze, and carry out activities that

shape the environments from which terrorists and their networks emerge.

*A key lesson from [high-value target case studies] is that targeting of enemy leaders does not work unless it is contained within a larger strategy. Finding the right balance between broader counter-insurgency efforts and HVT activities is vital... A myopic focus on the removal of insurgent or terrorist leaders at the expense of broader initiatives often has negative consequences.<sup>39</sup>*

These kinds of activities, so-called “indirect lines of operation,” as defined by a former vice commander of the US Special Operations Command, include

*those in which we enable partners to combat extremist organizations themselves by co-tributing to their capabilities through training, organizing and equipping. This includes efforts to deter active and tacit support for violent extremist organizations in areas where the existing government is*

---

*The group of issues we have discussed will endure as the prime drivers of effectiveness in the CT community and the topics around which decisions concerning the CT community's evolution should evolve.*

---

*either unwilling or unable to remove terrorist sanctuaries.<sup>40</sup>*

In many ways, these kinds of operations are far more difficult to support and conduct than traditional CT operations because of the scope and the range of analytic skills and organizational entities required to carry them out. To develop effective plans and approaches, analysts and operators must understand the roles of religious leaders, local politicians, and non-governmental, international and multi-national organizations present in a region, together with understanding of foreign internal defense forces, civil affairs, and the public, in effect, all those that shape the environment in which terrorist networks are spawned and operate.<sup>41</sup>

This is no small task and worthy of an entirely separate discussion. Suffice it to say for our purposes in this evaluation, analysts and operators will have to build even more diffuse communities of interest and sources of information than are normally considered for lethal operations against terrorists.<sup>42</sup> In addition, different ways of thinking about timelines must be developed as efforts to engage others in "indirect lines of operation" will take place over much longer for periods of time from conception, to development, to execution, and finally to results. And lastly, all we have said above about the importance of engaging foreign partners applies equally if not more so in this realm.

## **Conclusion**

Over the past nearly 10 years, the US CT community has restructured and implemented new processes to optimize the CT effort. Many of these have been mandated from above; others have been institutionalized through battlefield successes and failures. The implacable nature of the CT threat means future terrorist attacks will undoubtedly occur, and when they do post-event commissions will most likely offer new suggestions and wiring diagrams for improvement. But our experiences during the post 9/11 decade suggests that the group of issues we have discussed will endure as the prime drivers of effectiveness in the CT community and the topics around which decisions concerning the CT community's evolution should evolve.

❖ ❖ ❖

### Endnotes

1. The concept of compressed strategic, operational, and tactical spheres is discussed in the context of counterinsurgency in Michael Flynn, et al, "Fixing Intelligence: A Blueprint for Making Intelligence Relevant in Afghanistan," in Center for a New American Security Journal (January 2010): 25 at [www.cnas.org](http://www.cnas.org), accessed February 2010. Counterterrorism, as a component of counterinsurgency and as a form of low-intensity conflict, also reflects these compressed spheres.
2. Troy S. Thomas, *Beneath the Surface: Intelligence Preparation of the Battlespace for Counterterrorism* (Washington, DC: Joint Military Intelligence College, 2005), 2.
3. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (Washington, DC: Government Printing Office, 2004), 385.
4. "U.S. Intelligence Community Information Sharing Strategy," 22 February 2008, [http://www.dni.gov/reports/IC\\_Information\\_Sharing\\_Strategy.pdf](http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf), accessed 08 April 2011.
5. *Holloway Commission Report on the Attack Against the U.S.S. Cole*, available from <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB63/doc8.pdf>, accessed April 2011.
6. *Report to the President and Congress on the Protection of U.S. Forces Deployed Abroad*, [http://www.dod.gov/pubs/downing\\_rpt/](http://www.dod.gov/pubs/downing_rpt/), accessed 14 April 2011.
7. Flynn, "Fixing Intelligence," [www.cnas.org](http://www.cnas.org), accessed April 2011, 21.
8. "Ticking Time Bomb" Fort Hood Massacre Could Have Been Prevented, Senate Committee on Homeland Security and Governmental Affairs. 3 February 2011. [http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord\\_id=ecb97fed-5056-8059-767c-6e90f14b8736](http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=ecb97fed-5056-8059-767c-6e90f14b8736).
9. "About the National Counter Terrorism Center," NCTC website, [http://www.nctc.gov/about\\_us/about\\_nctc.html](http://www.nctc.gov/about_us/about_nctc.html); accessed on 17 February 2009.
10. Congressional testimony after the Christmas Day attempt to destroy Northwest Flight 253 highlighted information sharing dynamics in NCTC. One of the successes in information sharing, which differed from the situation prior to 9/11, was that certain information on Umar Faruq was sent to NCTC. However, this information was not further disseminated to the rest of the Intelligence Community. Parallel to that development, was a problem witnesses describe as "no one was in charge." Although changes have been implemented since the attempt, the information sharing progress allegedly has been negated by the bureaucratic set up. In "The State of Aviation Security: Is Our Current System Capable of Meeting the Threat?" Hearing Before the Committee on Commerce, Science, and Transportation, U.S. Senate, 20 January 2010, Serial No. 111-598.
11. Perspectives similar to ours were offered during January 2010 Congressional Hearings on "The State of Aviation Security: Is Our Current System Capable of Meeting the Threat?" cited above. Of note, cochair of the 9/11 Commission, Lee Hamilton, stated that while other intelligence failures occurred during the failed attack against Northwest Flight 253, this was not a repeat of the information-sharing failures present before 9/11/2001. Rather, the challenge is how analysts understand, manage, and integrate vast amounts of information. As such, the US government requires better management of data. However, NCTC Director Leiter, during the same hearing, noted that while key intelligence reporting related to the attack was relayed back to headquarters, it was not disseminated in a way that made it widely available to the rest of the IC. In "The State of Aviation Security."
12. "Hearing of the Senate Select Intelligence Committee: Nomination of Lieutenant General James Clapper to be Director of National Intelligence, Chaired by Senator Dianne Feinstein," 20 July 2010.
13. For further information on the USMA CTC, see <http://ctc.usma.edu>.
14. Alan Cullison, "Inside al-Qaida's Hard Drive," *The Atlantic* (September 2004), available from [www.theatlantic.com/magazine/archive/2004/09/inide-al-qaeda-s-hard-drive/3428](http://www.theatlantic.com/magazine/archive/2004/09/inide-al-qaeda-s-hard-drive/3428).

## Lessons Learned in CT Analysis

15. David W. Barno (LTG, USA Ret.) and Andrew Exum, "Responsible Transition: Securing U.S. Interests in Afghanistan Beyond 2011," in *The Center for a New American Security*, (December 2010), URL: [www.cnas.org](http://www.cnas.org).
16. Ltg Michael Flynn, et al., "Employing ISR SOF Best Practices," *Joint Forces Quarterly*, Issue 50, 3rd Quarter 2008, URL: [www.ndu.edu/inss/Press/jfq\\_pages/editions/i50/15.pdf](http://www.ndu.edu/inss/Press/jfq_pages/editions/i50/15.pdf).
17. Ibid.
18. Ibid.
19. James A. Lewis, "Combating Terrorism: Lessons Learned from London," Testimony before the House Government Reform Subcommittee on National Security, Emerging Threats and International Relations. September 19, 2006. URL: <http://www.csis.org/media/csis/congress/ts060919jimlewis.pdf>, accessed on 17 February 2009.
20. 2003 U.S. National Strategy for Combating Terrorism, URL: <http://georgewbush-whitehouse.archives.gov/news/releases/2003/02/20030214-7.html>.
21. On 10 August 2006, a plot to use liquid explosives to blow up transatlantic flights headed to the United States and Canada was foiled by UK authorities. The eight men arrested were allegedly close to carrying out the attack. They planned to use liquid explosives disguised as commonly-consumed beverages onto seven planes from London Heathrow Airport, within a period of approximately 2 and a half hours, and explode them while flying over the Atlantic Ocean. Targeted flights were bound for Montreal, Toronto, San Francisco, Chicago, New York, and Washington DC. Information from [www.tsa.gov/press/happenings/terror\\_plot\\_hearings.shtm](http://www.tsa.gov/press/happenings/terror_plot_hearings.shtm).
22. Lewis, "Combating Terrorism: Lessons Learned from London."
23. "Securing America's Safety: Improving the Effectiveness of Antiterrorism Tools and Interagency Communication," Hearing Before the Committee on the Judiciary, U.S. Senate, 20 January 2010, Serial No. J-111-71.
24. "The State of Aviation Security"
25. Lewis, "Combating Terrorism: Lessons Learned from London."
26. *Downing Report on the Attack Against Khobar Towers*, URL: [http://www.dod.gov/pubs/downing\\_rpt/](http://www.dod.gov/pubs/downing_rpt/).
27. Office of the Director of National Intelligence, "Intelligence Community Joint Duty Program Highlighted in Nationwide Public Television Series," ODNI News Release No. 24-09, 30 June 2009, URL: [www.dni.gov/press\\_releases/20090630\\_release.pdf](http://www.dni.gov/press_releases/20090630_release.pdf), accessed 14 April 2011.
28. Duane R. Clarridge, *A Spy for All Seasons*, (New York: Scribner Publishing: 2002).
29. *Report of the DoD Commission on Beirut International Airport Terrorist Act*, 23 October 1983, URL: <http://www.ibiblio.org/hyperwar/AMH/XX/MidEast/Lebanon-1982-1984/DOD-Report/index.html>. The report recommended the SECDEF establish an all-source fusion center to tailor and focus intelligence support to US military commanders involved in military operations in high-threat areas.
30. Joint Chiefs of Staff, *Joint Publication 2-0, Joint Intelligence*, 2007
31. Michael Leiter, Director of NCTC, "Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland," Statement for the Record to Senate Homeland Security and Government Affairs Committee, 22 September 2010.
32. "The Future of Fusion Centers: Potential Promise and Dangers," Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, 1 April 2009, Serial No. 111-15.

33. Dennis C. Blair, Director of National Intelligence, “Annual Threat Assessment of the Intelligence Community for the Select Senate Committee on Intelligence,” 12 February 2009, URL: [www.dni.gov](http://www.dni.gov).
34. John Brennan, “US Policy Toward Yemen,” Presentation to the Carnegie Endowment for International Peace, 17 December 2010. <http://carnegieendowment.org/files/Brennan-transcript.pdf>
35. Leiter, “Nine Years after 9/11.”
36. Ibid.
37. Brennan, “U.S. Policy Toward Yemen.”
38. Lewis, “Combating Terrorism: Lessons Learned from London.”
39. Matt Frankel, “The ABCs of HVTs: Key Lessons from High Value Targeting Campaigns Against Insurgents and Terrorists,” in *Studies in Conflict and Terrorism*, 34 (2011): 20.
40. LtGen. Eric E. Fiel, then vice commander of the US Special Operations Command, explained the difference between direct and indirect operations in letter to the Air Commando Association newsletter in February 2011 in <http://content.yudu.com/Library/A1tk6q/ACANewsletterFebruar/resources/2.htm>, accessed 25 Sep 2011.
41. Troy S. Thomas, “Beneath the Surface: Intelligence Preparation of the Battlespace for Counterterrorism,” 239.
42. A robust discussion of “non-red force” intelligence is handled in Flynn, “Fixing Intelligence,” 25. Specifically, the authors argue that the US Intelligence Community is largely blind on local economics and landowners, powerbrokers and possible ways to influence them, correlation between development and cooperation by locals, among other non-enemy-centric intelligence gaps. This is largely due to the focus of US COIN analysts on classified intelligence sources rather than other open sources where this information can be located.
43. Not used. United States Army Field Manual Number 3-24, Counterinsurgency Field Manual, The University of Chicago Press; Chicago and London, 2007, page 35.
44. Not used. Office of the Director of National Intelligence, National Intelligence Estimate: The Terrorist Threat to the U.S. Homeland, July 2007, URL: [www.dni.gov/press\\_releases/20070717\\_release.pdf](http://www.dni.gov/press_releases/20070717_release.pdf).
45. Not used. “Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland,” Statement for the record by Michael Leiter, Director of NCTC, Senate Homeland Security and Government Affairs Committee, 22 September 2010.
46. Not used. “The State of Aviation Security: Is Our Current System Capable of Meeting the Threat?” Hearing Before the Committee on Commerce, Science, and Transportation, U.S. Senate, 20 January 2010, Serial No. 111-598.



