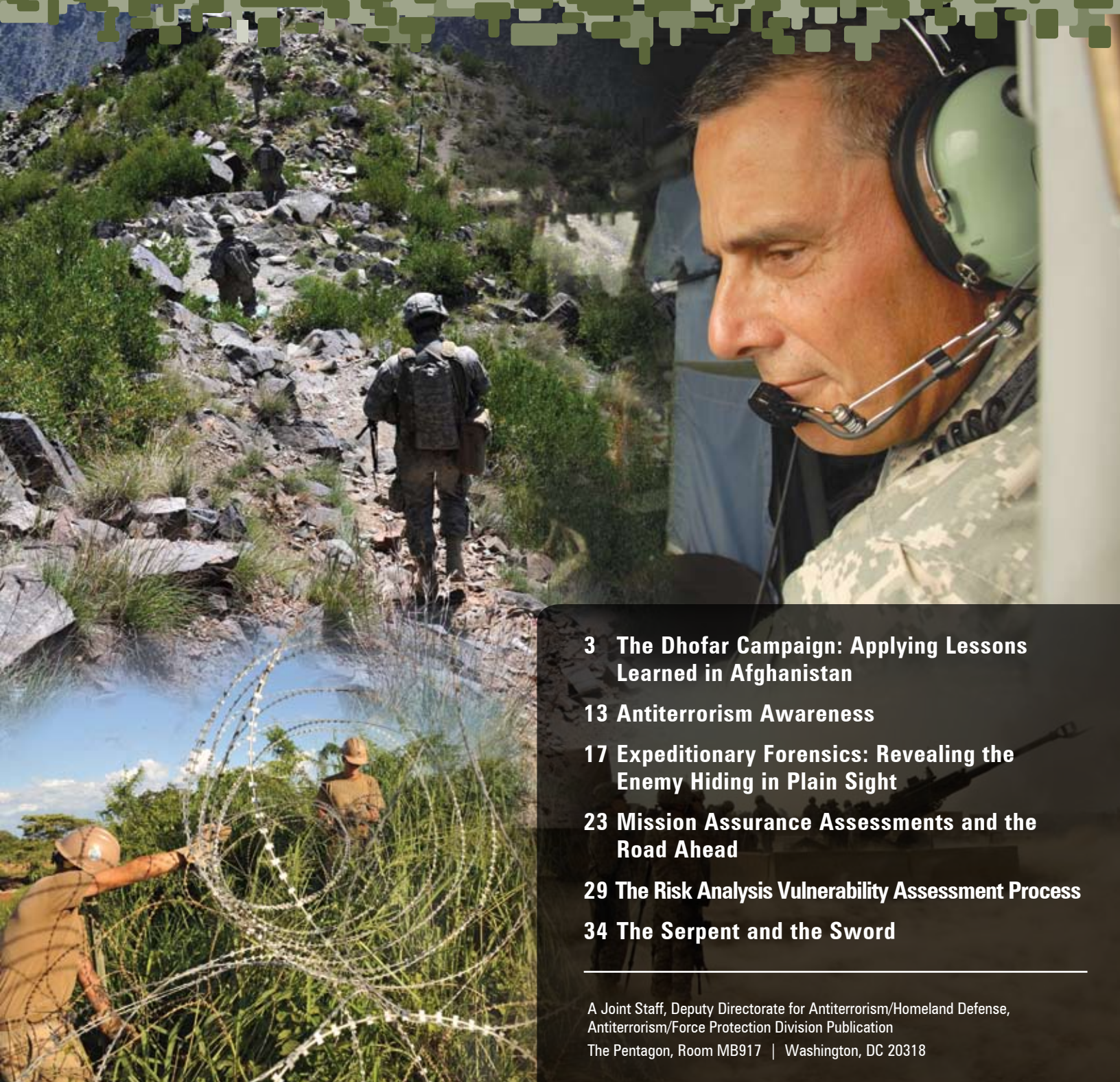
Summer 2010 | Volume 12 | Issue 2

THE GUARDIAN

THE SOURCE FOR ANTITERRORISM INFORMATION



A Joint Staff, Deputy Directorate for Antiterrorism/Homeland Defense, Antiterrorism/Force Protection Division Publication

The Pentagon, Room MB917 | Washington, DC 20318

[In] an interconnected world where dangers can emerge suddenly, we have to protect ourselves against the full range of threats—from a terrorist network bent on striking our homeland, to nations and violent extremists seeking weapons of mass destruction, to transnational threats such as cybercriminals and narco-traffickers. To keep America safe, my administration is strengthening and integrating every element of our national power — military and economic, diplomacy and development, homeland security, law enforcement and intelligence. And this final element — timely, accurate intelligence — is uniquely important because it is critical to all the others.

—Barack Obama, President of the United States of America
Director of National Intelligence Nomination Announcement,Washington, D.C.
5 June 2010

Overall, I think that there was general agreement on five points: first, that our effort is moving in the right direction; second, that the road ahead will be long and hard; third, that the elements of success — troops, civilians, strategy, growing ANSF and government capacity — are in place, or well in progress; fourth, that we have regained the initiative; and fifth, that progress is being made, slowly but steadily and sustainably.

—Robert Gates, Secretary of Defense
NATO Headquarters, Brussels, Belgium
11 June 2010

Protecting those we are here to help nonetheless does require killing, capturing, or turning the insurgents. We will not shrink from that; indeed, you have been taking the fight to the enemy and we will continue to do so.

—GEN David Petraeus, ISAF Commander
Open Letter to Troops, Kabul, Afghanistan
5 July 2010

The Guardian

The Guardian is published for the Chairman of the Joint Chiefs of Staff by the Antiterrorism/Force Protection Division of the J-34 Deputy Directorate for Antiterrorism/ Homeland Defense to share knowledge, support discussion, and impart lessons and information in a timely manner.

The Guardian

Summer 2010 | Vol 12, Issue 2

Guardian readers,

Welcome to the *The Guardian* Summer 2010 edition. I am especially pleased to introduce this issue as it will be my final opportunity as the J-34 Deputy Director for Antiterrorism/Homeland Defense. *The Guardian* is loaded with resources for Antiterrorism/Force Protection (AT/FP) professionals and addresses a broad range of timely and relevant topics:

- **The Dhofar Campaign** – The author applies lessons learned by British and Omanis in Dhofar, Oman to Operation ENDURING FREEDOM in Afghanistan.
- **Antiterrorism Awareness** – August is the Army AT Awareness month. AT is an integral part of force protection, key to ensuring a force capable of achieving mission success, and is every commander's responsibility.
- **Expeditionary Forensics** – Forensic science and technology have matured and are now important operational capabilities. Expeditionary labs are having a real impact on in C-IED and Force Protection efforts in Iraq and Afghanistan.
- **Mission Assurance Assessments and the Road Ahead** – The Defense Critical Infrastructure Protection (DCIP), Assessments and Resource Division provides a current overview of resources available to assess and mitigate AT vulnerabilities.
- **RAVA: The Risk Analysis Vulnerability Assessment Process** – This process quantitatively measures threats, assets, vulnerabilities, and risks associated with large and/or small government facilities.
- **The Serpent & the Sword** – An analysis of the current range of biological threats and DOD's AT/FP capabilities to counter the growing number of biological threats.

During my time on the Joint Staff, the AT/FP community has continued to adapt to evolving domestic and international threats, ranging from IEDs in Afghanistan to domestic terror plots. I am confident the AT/FP community will continue to champion and advocate for robust and forward-leaning AT programs, increased training and education, and responsive policy. Please contact your Service, Command or Agency representatives with suggestions, articles, and comments via SharePoint regarding the rewrites of DODD 2000.12 *DoD Antiterrorism (AT) Program*; DODI 2000.16 *DoD Antiterrorism (AT) Standards*, the updates to the Level I AT Training modules and the revision of Joint Publication JP 3-07.2 *Antiterrorism*.

Upcoming opportunities for AT/FP-related professional education include the Joint Staff Antiterrorism Executive Seminar 19-21 October 2010. Additional resources for professional development include J-34's AT-focused professional reading list and book reviews. AT policy, training, and assessment tools exist on the Antiterrorism Enterprise Portal (ATEP) at Army Knowledge Online (AKO) and J-34's new Intelink SharePoint portal on the SIPRNET.

It has been a privilege to serve as the J-34! The expertise, integrity, and resourcefulness of the men and women with whom I have had the honor of serving never ceased to impress me. Please continue to assist J-34 in building and fostering strong AT/FP programs by submitting your comments, suggestions, and articles at the guardian@js.pentagon.mil or via ATEP. Thank you for sharing your knowledge and experience with the larger AT/FP community via *The Guardian*.

Check Six!

Jonathan "Tracer" Treacy
Brigadier General, USAF
Deputy Director for Antiterrorism/Homeland Defense

THE DHOFAR CAMPAIGN

U.S. Army photo by Staff Sgt. William Tremblay/Released

Applying Lessons Learned in Afghanistan

By Mr.Nick Higgins

A little-known and successful counterinsurgency correlates closely with the campaign in southern Afghanistan—and can serve as a template for our efforts there.

Everything in war is simple, but the simplest thing is difficult.
—Carl von Clausewitz, *On War*

Introduction

The aim of this article is to draw people's attention to a little-known counterinsurgency campaign that was successful under conditions similar to those currently being faced in Afghanistan. From 1971 to 1975, a small but hard-fought counterinsurgency campaign was waged in Dhofar, the southernmost province of Oman (see Figure 1). In fact, the flag of rebellion had been raised much earlier, in 1962; by 1970, the communist-backed tribal guerillas controlled the whole of the Jebel Dhofar region ("jebel" [English spellings vary] is the Arabic word for "mountain," "hill," or "slope").

The inept operations of the mostly northern Omani sultan's army had done little to stem the insurgency but everything to drive recruits toward the rebels' cause. The sultan's army failed to come to grips with the guerilla groups and lashed out at the local civilian population.

In 1970, things began to change when the old sultan, Said Bin Taimur, was deposed by his son Sultan Qaboos Bin Taimur, with British help. The old sultan had kept the country firmly rooted in the Middle Ages with his feudal system of government and his refusal to allow any kind of modernization. There were no roads, no schools, no hospitals, and no development of water resources for home or agricultural use. Speaking to Omanis about this era on a recent visit to Oman, the author was told that the country was like "one big prison in which the people were allowed to do nothing."

FIGURE 1. Political Map of Oman Showing Provincial Boundaries

Many of the young men left the country in frustration to work elsewhere in the Middle East; others traveled to communist northern Yemen or to the People's Democratic Republic of Yemen (PDRY) to attend schools. Exposure to the outside world opened their eyes to the deprivations that existed at home.

Initially, the rebellion in Dhofar was fronted by a political party, the Dhofar Liberation Front (DLF), that had the idealistic slogan of "Dhofar for the Dhofaris" and that pledged to modernize the Dhofar region. Across the border in the PDRY, another group came into being, the People's Front for the Liberation of the Occupied Arabian Gulf (PFLOAG).[1] This organization was backed first by the Chinese and then later by the Soviets with arms, money, and training. The group's ideology was firmly Marxist.

From 1971 to 1975, counterinsurgency was successful under conditions similar to those currently being faced in Afghanistan. A small but hard-fought campaign was waged in Dhofar, the southernmost province of Oman.

The traditional tribal DLF was no match for the highly motivated, communist-inspired members of PFLOAG. Members of DLF were quickly absorbed, despite the communist teaching that there was no God and the expectation that everyone renounce Islam.

Once PFLOAG had control of the area, it tried to break down the tribal system using fear and coercion as its primary tools. Men were blinded for refusing to deny Allah and tribesmen were forced to offer their daughters in marriage to the fighters. Children were taken forcibly from their parents and sent to schools in the PDRY; many young men were sent to train in the Soviet Union and China as guerilla fighters.

PFLOAG, however, seemingly overplayed its hand. The remnants of the DLF old guard responded to an amnesty offered by the new sultan and refused to cooperate further with PFLOAG. This caused PFLOAG to order the total disarmament of DLF, which led to a battle between the two groups. Consequently, 24 of the most hardened fighters from the eastern Jebel came down and surrendered to the sultan.

Military Operations and Civil Development in Oman

The sultan, who had been educated in Britain and commissioned into a British infantry regiment, knew he had several problems. Two things were clear to him: (1) countering the insurgency hinged on civil development and (2) the problems and resulting conflict had to be seen as solved by the Omanis themselves.

He realized that he needed all the help he could get and that his army needed retraining and re-equipping. He decided to use British officers on secondment from the British Army and contract officers hired directly by his own armed forces (usually ex-British or Commonwealth officers). He also requested the assistance of British Army Training Teams (BATTs), which were provided by the elite 22nd Special Air Service (SAS) Regiment.

In 1970, British Lieutenant Colonel John Watts, the commanding officer of the SAS Regiment, and his operations officer flew to Oman to see how the regiment could assist. At the time, many of the troops in the sultan's army were from the Baluchistan region of Pakistan. The fighters were unable to speak Arabic, let alone the local Jebeli dialect, and were of little use. The army was subsequently disbanded. Even the native northern Omani regiments would not have been much better because the Dhofaris and Omanis did not get along.

Watts and others quickly came to the conclusion that local Dhofaris would need to be recruited to do the fighting. They had a nucleus of the 24 surrendered enemy personnel (SEPs), but many more fighters would be needed. It was also understood that this was a national revolutionary war, and Watts was aware of the lessons being learned in Vietnam: that foreign intervention in such a conflict would not succeed. This ruled out the option of using British troops as full-scale units, even though they were respected by Omanis stemming from the Jebel Akhdar campaign in the 1950s. Watts also

realized that any military action had to be based on sound, timely intelligence, without which any unit would be like an elephant blundering around in the dark. In fact, it was precisely that kind of behavior by the sultan's army forces that had driven many young Jebeli males into PFLOAG.

Southern Afghanistan—Helmand and Kandahar provinces in particular—is tribal, undeveloped, and distrustful of the central government and outsiders, much like the Jebel Dhofar was in the 1970s.

The sultan was firmly committed to modernizing the country, including the Jebel Dhofar, once it was secure. To this day, all Omanis receive free cradle-to-grave medical services and free education to the degree level. It was also decided that a robust public information campaign had to be set up. Information about this modernization had to be given to the people, and the virulent lies and propaganda being broadcast by Radio Aden had to be countered. The information campaign was primarily radio based due to the high levels of illiteracy among the population of the Jebel, although there were some leaflet drops during the course of the campaign. It was also decided that the radio station would be 100% honest at all times and would not engage in "black propaganda." It was thought that once people recognized this strategy, they would begin to trust the government again.

It was also understood that people's health and the health of their animals were supremely important, yet there was no provision of medical services, let alone veterinaries. The wealth of the tribes on the Jebel was in their herds of cows and goats, and if those herds could be improved through better health and selective breeding programs, the tribes would be wealthier. Watts knew that SAS was admirably suited to the first task of providing medical assistance to the people. The small SAS patrols had a much higher ratio of medics than the rest of the army and were trained to a far higher standard. (SAS medics in training spend time working in emergency departments at some of the busiest hospitals in the United Kingdom's most violent inner-city areas.) Watts also knew that this approach would only be a stop-gap measure until the Omanis could take over.

The regiment could not provide veterinary services but could tap the Royal Army Veterinary Corps for support.

After Watts' assessment was complete, he recommended that SAS assist the campaign on the following "Five Fronts":

1. Intelligence, by supporting an intelligence cell
2. Public information, by supporting a public information team
3. Civilian health, by providing a medical officer who was supported by the patrol medics
4. Veterinary health, by providing a veterinary officer
5. Security, through raising of local, Dhofari units to fight for the sultan

All of these measures were accepted. For 6 years, members of the regiment served in Dhofar to further the Five Fronts. All of these aims, however, were short term until the Omani government was in a position to assist its own people and to train Omanis to take over, which was the real long-term aim. All military operations were seen as a means to an end rather than the *raison d'être.*

The successful campaign is generally regarded as a model counterinsurgency campaign. Although Watts' Five Fronts were adhered to for the entire campaign, other elements of counterinsurgency contributed to the success and are applicable to current efforts in Afghanistan.

Counterinsurgency in Southern Afghanistan

Southern Afghanistan—Helmand and Kandahar provinces in particular—is tribal, undeveloped, and distrustful of the central government and outsiders, much like the Jebel Dhofar was in the 1970s. Can Watts' Five Fronts approach be successfully replicated in this area?

Let's take the original Five Fronts, generalize them, and examine each one individually to see if it can be applied to southern Afghanistan:

1. **Intelligence.** Identify the enemy and friendly forces by establishing an effective intelligence gathering and collation system.
2. **Public Information.** Communicate clear intent to the population, government agencies, and forces, and, by default, to the enemy.
3. **Civilian Health.** Provide medical aid to the people in areas where there is none.
4. **Veterinary Health.** Provide veterinary services for herds in areas where there are no such services.
5. **Security.** Provide security by helping the locals protect their own areas and by involving them in the overall provision of security.

Identify the Enemy and Friendly Forces

All counterinsurgency campaigns need to be intelligence driven, but all too often this principle is not correctly interpreted or applied. Every single patrol that leaves a forward operating base (FOB), whether on a 2-hour local patrol or on a 5-day patrol going further afield, needs to have clearly defined aims. A member of the intelligence cell should brief the entire patrol before departure, debrief the patrol when it returns, and then generate a written report. This report is then collated with other information. Once collated, the information needs to be analyzed; otherwise, the information is not useful.

FIGURE 2. Map of Afghanistan Showing Helmand and Kandahar Provinces

Once analyzed, the product needs to be disseminated so that it can be acted on. It is pointless to gather and store information without acting on the analysis. This was often done in Northern Ireland until the system was reorganized in the early 1980s. Some sort of central steering committee in a region is useful so that all intelligence flows in and the committee can allocate tasks to which units can respond.

The central steering committee would not take over the tasking of all patrols and operations. Units still run their own areas and ensure constant aggressive patrolling. ("Aggressive patrolling" does not refer to how the troops treat the civilian population but to the fact that patrolling is constant but random.) A well-run patrol program requires monitoring to see that patterns are not being set and that all parts of the area of responsibility (AOR) are being covered, especially where one AOR abuts another.

If a steering committee is set up, then *all* units in theater fall under it, including special forces and covert units. There can be no exceptions.

Local customs can inhibit identification of enemies and friendly forces. Society in southern Afghanistan exists as a closed tribal society that is hard for outsiders to penetrate and understand. There are alliances and divisions that go back years but that shift constantly. Any unit operating in a given area needs to know which tribe controls that area and where it ranks as a tribe. There are minor, unimportant tribes and senior, important tribes, but either way, it is not productive to offend a tribe by bringing outsiders into its region.

Senior officers need to meet with *woliswols* (district governors) as well as with *maliks* (village head men) and *shuras* (governing councils of elders). Junior officers should never be sent to meetings without first having been introduced by a senior officer. *Shuras* must be given the necessary level of respect or the members will take offense.

Military protocol also can inhibit identification of enemies and friendly forces. What makes the difference is getting out on the ground, talking to the locals at length, and making contacts. A personal example of protocol possibly inhibiting intelligence gathering occurred in Helmand Province in 2005, when the author worked as security manager for a large multimillion-dollar aid project. The project had Afghan staff in many areas of Helmand, including an engineer who lived in a village that a Taliban group had moved into. The Taliban group planned to use the village as a operating base from which to conduct operations. The engineer was asked to visit the Provincial Reconstruction Team (PRT) and talk about what was happening in the village, but, quite sensibly, he said no. He did not want to be seen going into the base, but he agreed to talk with the soldiers if they could come to the office. The soldiers, however, were not allowed to come to the office, despite the opportunity to debrief the man and potentially recruit him. In this case, it seemed to the author that although procedure was followed, an opportunity was missed.

Communicate Clear Intent

A well thought out communications program will work wonders. It must tell the truth at all times; otherwise, it just becomes a cynical propaganda tool that people quickly see through. Several local radio stations are broadcasting in southern Afghanistan already. It would be worth looking into what they broadcast and who runs them; for example, a liaison with the BBC Pashto radio program would seem like a good model.[2] Giving out solar-powered clockwork radios is another sound idea, even though it is disheartening to see some of them turning up in the bazaar for sale. If radios are distributed, they should be tunable and not fixed to certain stations. The people will see through that strategy, and it could wind up playing into the hands of the insurgents by giving them something they can use to score propaganda points with the people.[3]

Cultural learning curve. Local customs can inhibit identification of enemies and friendly forces. Society in southern Afghanistan exists as a closed tribal society that is hard for outsiders to penetrate and understand. There are alliances and divisions that go back years but that shift constantly. (U.S. Army photo by Sgt. Teddy Wade/Released)

Support Civilian and Veterinary Health

These two points are obvious and largely self-explanatory. Support in this area should also include agricultural assistance, not just animal husbandry, because agricultural farming is just as important in southern Afghanistan. Farmers (not agricultural experts) could be brought to advise and assist local farmers on how to increase crop yields. These farmers should be people who have actually owned farms in areas with adverse climatic conditions, such as South Africa or Zimbabwe.

Provide Security Assistance to Local Forces

All Pashtun tribes, regardless of importance, have a *lashkar* or tribal war band. If the tribe is willing—a good gauge of how friendly the tribe is toward the PRT—all or part of the lashkar can be employed for FOB security duties. This approach has a two-fold gain: (1) It becomes in the tribe's interest to keep the PRT informed of insurgent activity in the area because that communication protects its people and (2) the PRT creates local employment and puts money into people's pockets.

Another concept from the Dhofar campaign that needs to be examined closely is that of the *firqat* or task force. The firqats were tribally based militias mainly made up of *Adoo* (the name given to the insurgents) who had rallied to the government side.

A great deal of thought was given to how SEPs should be treated. Above all, they were not treated as prisoners of war; on the contrary, they were welcomed back into the arms of the tribe like prodigal sons. A friendly debriefing rather than an interrogation produced a great deal of exploitable intelligence regarding details about hideouts, supply routes, Adoo unit strengths, and commander names. This treatment of SEPs was broadcast on the radio and encouraged others to return.

The firqats were also useful in carrying the government's message to the people because it carried more weight than when it came from foreigners.

The firqats were formed and operated on a tribal basis within their own tribal areas; however, an early experiment with a multitribal firqat failed. Firquats sent

on operations outside their own areas were not very interested in the operation because they could see no direct correlation between their tribal interests and what they were being asked to do.

At the time of this writing, the Shinwari tribe in southwest Afghanistan has just declared itself in favor of the government—the first time a whole tribe led by its elders has done this. The catalyst for change was an attack on Afghan engineers who were overseeing the building of a dike in the tribe's area. This example clearly shows that something in the tribe's own direct interest prompted the change of heart.

The above example would seem to indicate that the tribal lashkars could be used in the same way and that some kind of program could be set up to work with any former Taliban members who decide to rally to the government side. Countergang tactics are another option that could be examined in southern Afghanistan.[4]

Broader Principles of Counterinsurgency

British counterinsurgency doctrine currently recognizes the following six broad principles:

1. Political primacy and political aim
2. Coordinated government machinery
3. Intelligence and information
4. Separating the insurgent from his support
5. Neutralizing the insurgent
6. Longer-term postinsurgency planning.

These six principles very easily dovetail with Watts' Five Fronts and support most, if not all, in a variety of ways.

The first principle is similar to the first principle of land warfare, "Selection and maintenance of the aim," and ties in with the second counterinsurgency principle of coordinated government machinery. It makes the point that all actors must work toward one aim or goal that has to be clearly defined by the political masters.

Principles 4 and 5 also tie together, but separating the insurgent from his support is a long and painful process if the insurgent is indigenous to the population, as is the case with the resurgent Taliban in southern Afghanistan. Separating the insurgent from his support also includes securing the border areas to interdict supply routes in and out of the country.

For Helmand Province, a case could be made for locating a battalion-sized combat group with its own rotary wing assets at Baram Cha on the border. Southern Helmand south of Garmshir or south of the crescent of the river Helmand has always been a wild and lawless area and is controlled mostly by Baluch tribes rather than Pashtun tribes. The Baluch are heavily involved in the movement of narcotics, and this route south through the desert is one of the main smuggling routes out of and into the country: Opium out, men and equipment in.

Watts' Five Fronts cannot be applied in isolation. Two further points to consider when formulating a counterinsurgency doctrine for Afghanistan are the twin demons of narcotics and corruption.

A well-thought-out communications program will work wonders. It must tell the truth at all times; otherwise, it just becomes a cynical propaganda tool that people quickly see through.

Narcotics

The whole opium economy is inextricably linked to the insurgency. The opium trade funds the Taliban to the tune of more than $100 million a year. Groups other than the Taliban also profit from narcotics and therefore have an interest in seeing the insurgency continue. The narcotics trade can flourish in the bubble of anarchy created by an ongoing insurgency.

Narcotics cannot be ignored by the military. One school of thought is that military involvement in countering narcotics at any level will turn the people against coalition forces and undermine any gains from a "hearts-and-minds" campaign. This may be the case in the short term, but it is a temporary setback. The military will have to accept that there will be a loss of popular support brought on by eradication, and the military should plan for this by developing an effective "all-agencies" strategy. Planning for eradication should start 18 months to 2 years in advance of actually moving into the fields.

Figure 3 shows graphically that winning the counterinsurgency campaign must include the removal of the opium industry, one of the main sources of Taliban funding. There is also strong evidence to suggest that al Qaeda remains heavily involved in narcotics for fundraising purposes, so any move to curtail opium production will eventually have an effect. (It is rumored that a 2-year supply of opium, based on the current production rate, is buried in the deserts of Helmand and Kandahar.)

Once the area for eradication is identified, an all-agency planning group with all key stakeholders—international and Afghan—needs to be established. This group would look at the tribal demographic in the chosen area as well as at local officials. Many mullahs in Helmand accept their tithes in opium, so those involved with narcotics need to be identified. Corrupt officials need to be replaced with honest ones as soon as possible.

A concentrated aid plan needs to be drawn up covering roads, health centers, schools, veterinary clinics, well digging and irrigation, agricultural assistance, and micro-finance and micro-credit for farmers not engaged in poppy production. These new schools, clinics, and support facilities need to be staffed and equipped. Much of this aid needs to be free to the people or at least heavily subsidized.

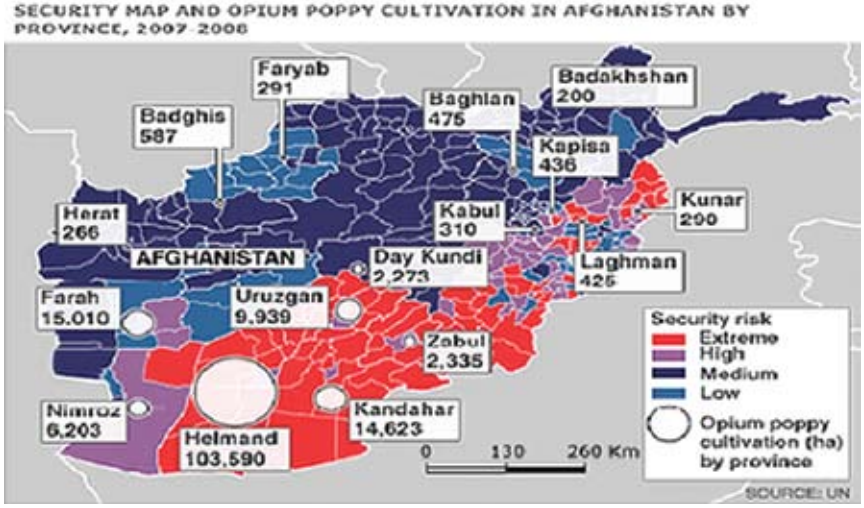


FIGURE 3. Ratio of Insecurity to Opium Production by Province (Annual Report: 2008—United Nations Office on Drugs and Crime)

A powerful public information campaign needs to be instigated as early as possible using radio, billboards, and traveling theater groups to carry a united message to the people. Independent nongovernmental organizations need to be brought into the program so that all the players are working toward a common goal of eradication.

Corruption

Corruption, on a level rarely seen elsewhere, is the other ingredient in the mix that will undermine the success of any counterinsurgency campaign. Undoubtedly, corruption would exist, even if the narcotics did not, because it is part of the way of life in central Asia. What is certain is that even Afghans feel that corruption has gotten out of hand and has reached epidemic levels. Rampant corruption at all levels of government will prevent a coordinated multiagency government approach (the armed forces being but one agency), which is critical to any successful counterinsurgency campaign. One can put forward the argument that with the current levels of corruption in the Karzai regime—from ministers down to the policemen on the street—the insurgency can never really be defeated. This author firmly believes that the Taliban cannot win; however, as it stands now, the Taliban will not be defeated because the people refuse to truly rally around the government. If corruption is not addressed, the insurgency will drag on until the international players grow tired of it and withdraw, one by one, handing victory to the Taliban. The Taliban insurgents are waging a war of a thousand cuts, and time is on their side.

Ignoring corruption in a given AOR gives the population the impression that corruption is condoned, and people will quickly arrive at the conclusion that the PRT must be involved. An extreme example of this may have led to the murder of five British soldiers in November 2009: A local policeman had been raped repeatedly over a period of time by his Afghan commander, and the policeman came to believe that because the British did nothing to stop it, they must have condoned it. That said, it is unlikely that any British troops were aware of the situation because, unlike the BATTs in Dhofar, British forces do not live among the Afghans.

Conclusion

Every insurgency is different, not just for political, ideological, and religious factors but also because of geography, terrain, and climate. In the case of the Dhofar campaign, many factors correlate directly with the campaign in southern Afghanistan and can be used as a template there, despite the gap of years between the two campaigns.

Nick Higgins is employed by CRA Inc. as an instructor for the US Marine Corps Level II Antiterrorism Officers Course. He spent 6 years in the British Army as a member of 2nd Battalion, the Parachute Regiment, including a 2-year tour in Northern Ireland that involved intelligence-gathering duties. From 2003 to 2007, Higgins lived and worked as a security contractor in Afghanistan. During his time there, he spent nearly a year in Helmand and Kandahar provinces. He can be contacted at nhiggins@cra-usa.net.

The author states, "I am indebted to Colonel Tony Jeapes and Colonel I. A. Rigden; the sensible stuff is theirs and any mistakes are my own."

1 PFLOAG changed its name after the British withdrawal from Aden and called itself the People's Front for the Liberation of Oman (PFLO).

2 See http:www.bbc.co.uk/pashto/index.shtml.

3 Chris Hughes, "The SAS squad lead the manhunt for Afghan assassin Gulbuddin," *The Mirror,* 1 May 2009.

4 The author recommends a study of the Selous Scouts from the Rhodesian war and the book *Gangs and Counter-gangs* by General Sir Frank Kitson (see the bibliography). Kitson is the

British officer generally credited with inventing countergang theory as we now know it.

Bibliography

Jeapes, Tony. *SAS Operation Oman*. Nashville, TN: Battery Press, 1982.

Kitson, Frank. *Gangs and Counter-gangs*. London: Barrie & Rockliff, 1960.

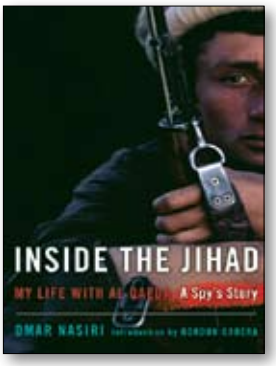
Kitson, Frank. *Bunch of Five*. London: Faber and Faber, 1988).

Kitson, Frank. *Low Intensity Operations: Subversion, Insurgency and Peacekeeping*. Mechanicsville, PA: Stackpole Books, 1991.

Peters, Gretchen. *Seeds of Terror: How Heroin is Bankrolling the Taliban and Al Qaeda.* New York: St. Martin's Press, 2009.

Rigden, I.A. "The British Approach to Counterinsurgency: Myths, Realities, and Strategic Challenges," March 15, 2008. Available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479660&Location=U2&doc=GetTRDoc.pdf

Book Review



Inside the Jihad: My Life with al Qaeda

by Omar Nasiri
Pulitzer Prize Winner (2005)

Review by 1LT Venessa Saucier

Omar Nasiri, a pseudonym for the Moroccan who successfully penetrated al Qaeda's terror network, presents a compelling inside look at life in the Khaldan Training Camp and challenges some common Western misperceptions and stereotypes about al Qaeda.

Nasiri beat al Qaeda's stringent security and vetting processes and infiltrated the terror training camps in Afghanistan while working as an informant for European intelligence services between 1994 and 2000. Nasiri was not actively recruited by intelligence services, and his motives for offering his services as a mole were not altruistic.

Instead, he was driven primarily by a sense of disillusionment and self-preservation. Readers may find the vivid accounts of Nasiri's terrorist training eerily familiar to experiences from Basic Training. At the camp, these mujahedeen pushed their bodies to the limits of their endurance and were instructed in advanced, hand-to-hand combat techniques. Nasiri expressed enthusiasm for the weapons training course and indicated that there was never a shortage of weapons or ammunition at the camp.

In addition to weapons training, recruits learned advanced surveillance techniques and how to create homemade explosives from common household chemicals. Finally, interrogation resistance techniques, such as how to endure and use misinformation after capture, were systematically taught. Nasiri claims these tactics were successfully used by Ibn al-Sheikh al-Libi to bolster Saddam Hussein's connections with al Qaeda:

> No, Ibn Sheikh did not crack under the pressure of torture. He handled his interrogators with the same skill that he used to handle his gun. He knew what his interrogators wanted, and he was happy to give it to them. He wanted to see Saddam toppled even more than the Americans did. As he had told us at Khaldan, Iraq was the next great jihad. Somewhere, in a secret torture chamber, Ibn Sheikh had won his battle.

Whether or not the author's account of events is entirely true, the book is useful for its insights into al Qaeda's training, tactics, and mindset.

1LT Venessa Saucier is the Antiterrorism Officer at Gulfport CRTC, Mississippi.

Recommended Reading

J-34 Antiterrorism Reading List

To assist in the professional military education and development of the AT/FP community, J-34 has compiled a reading list on topics related to antiterrorism.

Benjamin, Daniel, and Steven Simon. *The Age of Sacred Terror: Radical Islam's War Against America*. New York: Random House, 2003.

Coll, Steve. *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001.* New York: Penguin, 2005.

Scheuer, Michael. *Through Our Enemies Eyes: Osama bin Laden, Radical Islam, and the Future of America.*

Hoffman, Bruce. *Inside Terrorism. 2nd ed.* New York: Columbia University Press, 2006.

Horne, Alistair. *A Savage War of Peace: Algeria,1954-1962*. New York: NYRB Classics, 2006.

Joes, Anthony J. *Resisting Rebellion: The History and Politics of Counterinsurgency.* Lexington, KY: University Press of Kentucky, 2006.

Lewis, Bernard. *Crisis of Islam: Holy War and Unholy Terror.* New York: Random House, 2004.

Nagl, John. *Learning to Eat Soup With a Knife: Counterinsurgency Lessons from Malaya and Vietnam.* Chicago: University of Chicago Press, 2005.

Pape, Robert. *Dying to Win: The Strategic Logic of Suicide Terrorism.* New York: Random House, 2006.

Sageman, Marc. *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press, 2004.

Guardian readers are encouraged to submit articles with analysis that expands on or critiques AT-related topics covered in these books. Send submissions to guardian@js.pentagon.mil.

ANTITERRORISM AWARENESS

U.S. Navy Photo by Chief Mass Communication Specialist Jeremy L. Wood/Released

Educating and partnering with the community

By Mr. Richard Vanderlinden and Mr. Craig Benedict

When the members of the military and civilians know what to look for, they can contribute immeasurably to our nation's security.

Terrorists are constantly scheming to attack your Army, your country, and even your family.
—Specialist Gayonont, 3rd US Infantry Regiment, "The Old Guard"

In the debate building up to the adoption of the US Constitution, Thomas Jefferson observed in a letter to George Wythe: "I think by far the most important bill in our whole code is that for the diffusion of knowledge among the people. No other sure foundation can be advised, for the preservation of freedom and happiness."[1] It is unlikely Jefferson was referring to the threat of terrorism when he wrote to Wythe, but when it comes to protecting against that threat today, Jefferson was exactly correct. Our protection is greatly enhanced by the diffusion of knowledge. We call it "antiterrorism awareness" when planning and preparing to protect against terrorist attacks. By increasing AT awareness throughout the DOD community, we build a common understanding of the threat and of protective measures. This encourages initiative within the community, builds confidence, and increases our ability to prevent a terrorist attack.

The Army has fully embraced the concept of AT awareness. The Army's supporting programs take advantage of the intelligence and resourcefulness of the Army community. They reflect the vision expressed in the Army AT Strategic Plan (ATSP) to ensure that "the entire Army will be involved."

From a homeland defense perspective, the Fort Dix Six terrorist plot; the thwarted bombing of Delta Flight 253

in December 2009; and the 1 May 2010 attempted vehicle bombing in New York City's Times Square reinforce the benefits of AT awareness and, at the same time, provide an incentive that drives the current AT initiatives. In each of those incidents, alert citizens—rather than trained security forces—led to the prevention of a full-scale attack and the associated consequences.

Terrorism is an enduring, persistent, and worldwide threat to our nation. Extremist ideologies and separatist movements continue to have an anti-Western orientation. As such, the Army must sustain a strong defensive posture to prevent terrorist acts and protect the Army's most critical assets—people, information, and infrastructure. Our AT plans constitute the defensive element of the Army's combating terrorism program to assess, detect, defend, warn, and recover from terrorist acts. By including everyone in our AT awareness efforts, we employ the maximum possible strength to confront prospective terrorists.

The ATSP, developed by the Office of the Provost Marshal General (OPMG) in direct support to the Office of the Deputy Chief of Staff G-3/5/7, supports and focuses the Army's AT policy. LTG Thurman, the Deputy Chief of Staff, G-3/5/7 of the Army, wrote in the introduction to that strategy, "through constant awareness and vigilance … we will succeed in our goal of preventing terrorist attacks." Observing and reporting suspicious activity or behavior or other indicators of potential terrorist activity is fundamental to a strong AT program. When the members of our Army and our community know what to look for, they can contribute immeasurably to our protection.

Always Ready, Always Alert
Because someone is depending on you

Enhancing AT Awareness

Since October 2008, the Headquarters, Department of the Army (HQDA) AT Branch under the OPMG has taken deliberate and lasting steps to instill a heightened sense of AT awareness and vigilance across the Army. When asked why this new initiative was adopted, Mr. Alex Mascelli, AT Branch Chief, responded to questions regarding the adoption of this new initiative, stating: "We cannot afford to drop our guard or become complacent. Just because we haven't had a successful attack for a while doesn't mean terrorists are not planning for that. In fact, continuing to prevent future attacks becomes even harder, and we must re-double our efforts to ensure terrorist threat awareness and vigilance is maintained."

Army efforts to enhance AT awareness began in earnest in 2008 and are now in full-scale implementation. These efforts began with the realization that sustaining AT awareness throughout our communities is tough, particularly when the majority of our community members feel they live and work within the safest locations in the country.

The Army's first steps to increase focus and resources on awareness are to "enhance AT awareness throughout the Army community" as a goal in the ATSP, followed by the development of a supporting AT strategic communication (STRATCOM) plan. The key parts of the Army AT STRATCOM plan include—

- Provision of AT strategic talking points for commanders
- Establishment of AT-focused themes and messages
- Branding using an AT image (logo and slogan) to support awareness and program recognition
- Senior Army leadership approval and support in the conduct of an Army-wide AT awareness month
- Implementation of the iWATCH ARMY terrorist watch program.

AT Awareness Month

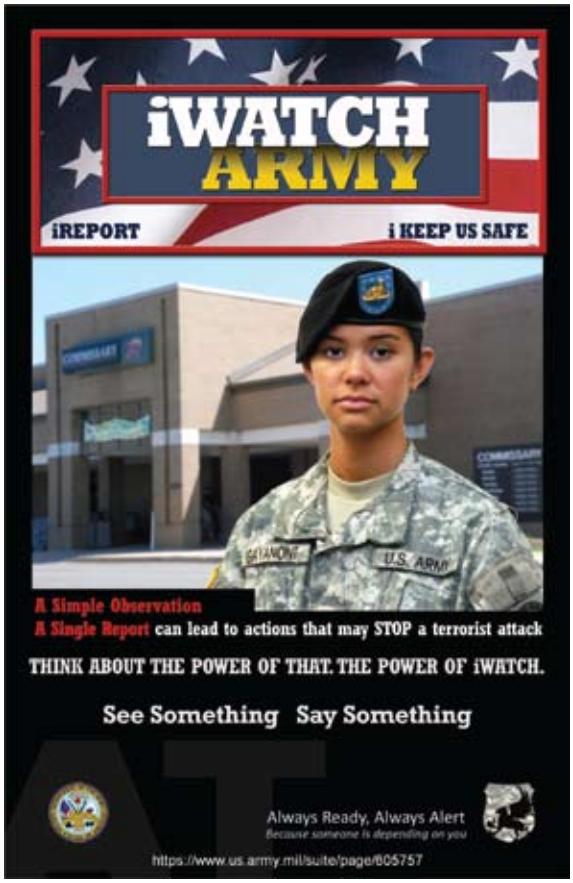
On 16 February 2010, the Department of the Army (DA) senior leadership approved an AT awareness month for August 2010. During this month, Army installations, facilities, and forces will focus their efforts to heighten AT awareness and vigilance to prevent and protect Army communities from acts of terrorism. By integrating AT doctrinal principles with constant AT awareness, the Army ensures the safety and security of its people while ensuring mission success.

The Army's AT awareness month has four themes:

Education and Training: Conducting AT training, education, and awareness for military and DA civilians throughout the month

Suspicious Activity Reporting: Increased emphasis on suspicious activity reporting, including the indicators of potential terrorist behavior and activities,relevant categories of information, and appropriate authorities

Leadership: A review and emphasis of AT roles and responsibilities for unit leaders and staffs across operational units, installations, and stand-alone facilities



Emergency Preparedness: Enhancing AT preparedness through emergency response planning and local civilian and host nation partnerships.

SEE SOMETHING >>

The Army's Military Police (MP) Corps plays an important role in AT security and awareness and provides leadership, advice, and guidance to commanders and managers responsible for the security of our installations and facilities. As the Army initiates a new terrorist watch program—iWATCH ARMY—MP leadership becomes critical to successful implementation.

iWATCH ARMY

iWATCH is a nationwide, modern version of the neighborhood watch program. Modeled after the Los Angeles Police Department's terrorist watch program, iWATCH ARMY encourages and enables citizens to help protect their communities by identifying and reporting suspicious behavior associated with terrorist activities. The passive element of iWATCH ARMY is individual situational awareness of surroundings. That distinction is essentially learning the difference between "normal" and "unusual." The active element of iWATCH ARMY involves individuals taking action to report suspicious behavior or activities to military police or other law enforcement agencies for further investigation. The partnership between the MP and the community builds teamwork that expands information collection and increases opportunities to identify prospective terrorists before they strike.

We know from investigations of successful terrorist attacks that perpetrators conduct reconnaissance and surveillance to determine vulnerabilities, to select targets, and to develop and finalize attack plans. The local community can often observe some of the actions undertaken by terrorists

during the preoperational phase (e.g., videotaping or photographing buildings, asking security-related questions) as suspicious or unusual behavior. By reporting these activities to MP or local law enforcement for investigation, our community members extend our "informal sensor systems," allowing us to better detect and prevent terrorist activities.

COL Chad B. McRee, Chief of Operations for the Office of the Provost Marshal General, put iWATCH ARMY into perspective:

> *The nature of the terrorist threat warrants constant awareness in all missions and all operational environments. The ability to maintain an appropriate level of awareness demands training, education, and leadership. But it also requires a deliberate and sustained out-reach effort which leverages our entire Army-community. Collectively, every member of our Army (Soldiers, DA Civilians, family members, and Army contractors) plays an important role by watching for and reporting suspicious activity. If they see something suspicious, they should report it.*

Disseminating Awareness Products

To ensure the AT STRATCOM messages and products are received and add value at the community level, the Army's AT Branch has undertaken a significant effort in order to disseminate products and tools to assist leaders in the development and implementation of community awareness programs at the installation, stand-alone facility, and unit levels. Ongoing efforts include—

- Mass distribution of more than 1 million AT awareness and iWATCH ARMY products, including posters, brochures, and CD/DVD sets to support commanders and staffs at the local level
- Publication of high-impact AT awareness and iWATCH ARMY posters in the August issue of *Soldiers* magazine
- Provision of information and products to assist commanders and units through the Army Knowledge Online Antiterrorism Enterprise Portal (ATEP).

See Something—Say Something!

A focused effort on AT awareness can empower community members by providing them with the information on the constantly evolving terrorist threat and personal protective measures. In light of the persistent terrorist threat, we must take a long-term approach toward sustaining heightened awareness. As such, commanders and leaders responsible for the protection of people, information, and infrastructure must constantly assess the nature of the terrorist threat and ask whether they are utilizing the full capability of their local community—the "eyes and ears" that scan the environment all day, every day. By making AT awareness and iWATCH ARMY initiatives effective tools in the defense against terrorism, collectively we can prevail and keep our Army safe. President Jefferson foresaw the value of knowledge many years ago. The diffusion of knowledge is indeed our most certain hope for success in preventing a terrorist attack.

Mr. Richard Vanderlinden is a strategic communication analyst for the Department of the Army's Antiterrorism Branch. Mr. Craig Benedict is the strategic planner for the Department of the Army's Antiterrorism Branch. Both are retired Army officers with extensive backgrounds in AT and FP.

1 Peterson, Merrill D. *Thomas Jefferson: Writings.* New York: Library of America, 1984.

EXPEDITIONARY FORENSICS

U.S. Air Force photo by Tech. Sgt. Michele A. Desrochers/Released

Revealing the Enemy Hiding in Plain Sight

By MAJ Michael A. Johnston, USA

Intelligence operations benefit from the rapid forensic exploitation of information and sensitive sites, enabling threat elimination.

Forensic science involves the application of a broad spectrum of sciences to establish factual information and answer questions of interest based on forensic material.

Expeditionary forensics establish facts that combatant commanders can use to determine sources of insurgent arms, ammunition, and explosives. Forensic science methods drive intelligence analysis and subsequent targeting for combat operations. They have the ability to change force protection (FP) measures, identify human remains, and prosecute detainees in the court of law. Intelligence operations benefit from the rapid forensic exploitation of information and sensitive sites, enabling US and coalition forces to eliminate threats by capture, prosecution, or killing.

The current struggle against global terrorism and associated military operations in Iraq and Afghanistan has produced an operational need to expand the use of forensics beyond the traditional historical, judicial, intelligence, and medical realms.

Background: Iraq

A joint expeditionary forensic facility (JEFF) lab was first established in Iraq in December 2006 to address a high number of sniper attacks throughout the Iraqi theater of operations (ITO). The original countersniper lab—now known as the JEFF 3 lab—soon acquired its first piece of evidence: a Dragunov sniper rifle. The JEFF

3 lab enabled local commanders to "conduct firearm/tool mark, latent print, and DNA forensic analysis in general support of U.S. and coalition forces in the entire ITO in order to exploit biometric and forensic evidence resulting in the killing, capturing, or prosecution of anticoalition forces."[1] At that time, the countersniper lab was capable of two things: latent printing and firearm/tool marking. The capability for DNA analysis existed only in the International Zone, which supported a task force that examined extrajudicial killings. When that task force was disbanded, the DNA analysis capability was incorporated into the JEFF countersniper lab. Within 2 years, the lab had processed more than 1,800 cases, resulting in more than 150 biometric identifications.[2] The success of the JEFF labs was evident, and in late 2007, LTG Raymond Odierno (then commander of the Multinational Corps–Iraq) directed the establishment of JEFF labs in each major division area of operation.

The current struggle against global terrorism and associated military operations in Iraq and Afghanistan has produced an operational need to expand the use of forensics beyond the traditional historical, judicial, intelligence, and medical realms.

The JEFF 3 lab, which is under the administrative control of the 733rd Military Police Battalion (U.S. Army Criminal Investigation Command [commonly referred to as the "CID"]/Forensic Exploitation Battalion), provides general support to the Multinational Corps–Iraq, including more than 20 brigade combat teams (BCTs) and various combined joint special operations task force elements. The lab also has close working relationships with weapon intelligence teams, explosive ordnance disposal units, law enforcement professionals, the US Special Operations Command, the CID, theater internment facilities, and detainee holding areas. All of the analysts, examiners, and technicians assigned to the lab are civilians who are specialists in their specific fields and who have volunteered for this expeditionary mission.

Impact of JEFF 3 on the Battlespace

The JEFF 3 lab processes all evidence related to nonimprovised explosive devices, including evidence from sniper attacks, insurgent and terrorist torture houses, various complex attacks on coalition forces, caches, enemy killed-in-action confirmation of high-value individuals on targeted raids, highly sensitive political cases, and select CID cases.

In addition, partnerships with the Combined Explosive Exploitation Cell and document and media exploitation labs allow the coprocessing of cases where additional laboratory analysis is required.

The processing of material at JEFF 3 consists of several steps, beginning with the collection of evidence following an incident, such as a planned site exploitation mission or a response resulting from a routine patrol. The evidence is transported to the lab through a variety of means and normally arrives within hours but processing takes up to a week after an incident, depending on the urgency of the analysis and the needs of the unit.

Triage

The most critical step of the process is triage, which begins when evidence arrives at the lab. Triage is the process used to determine the best method of supporting unit requirements to capture, prosecute, or kill the enemy through the use of forensic analysis. It allows the lab to best prioritize valuable resources by sorting cases into three distinct categories:

1. **Expedite.** "Expedite" cases are associated with an injury to or death of a coalition soldier.
2. **Priority.** "Priority" cases are time-sensitive in nature and are often associated with the release of a detainee or an at-large individual potentially targeted by a unit.
3. **Routine.** "Routine" submissions are placed into the queue for processing, but do not have the same sense of urgency as Expedite or Priority cases.

Triage is conducted by the evidence custodian or case file manager (alternate evidence custodian). Units that submit evidence for analysis must provide documentation of the incident (a significant activity report or a description of the "who, what, when, where, why, and how") detailing how forensic analysis of the evidence can be expected to link the item or person to a specific event.

Triage also involves establishing a chain of custody if it has not already been established by the submitting unit. The submitting unit completes a Department of the Army (DA) Form 4137, Evidence/Property Custody Document; DOD Form 2922, Forensic Laboratory Examination Request; and lab tracking and unit information sheets. The case file manager establishes a case file, and the evidence is properly secured in the evidence room. A record of the evidence is entered into the evidence ledger, the evidence tracker program, and the lab matrix.

U.S. Army soldiers with the Charlie Troop 4-14th Cavalry 2nd Platoon Fort Wainwright, Alaska, search a haystack for weapons cache outside the city of Rawah, Iraq, during Operation Iraqi Freedom Sep 27, 2005. (U.S. Air Force photo by Tech. Sgt. Andy Dunaway/Released)

Operationalizing Forensics

The ability to provide time-sensitive, actionable intelligence to the combatant commander is the most important aspect of the JEFF 3 lab. The turnaround time for analysis in an expedited latent print and firearm/tool mark case is a couple of hours to a day, depending on the number of items submitted. Expedited DNA processing takes 21–24 hours to complete. These short processing times allow units maximum flexibility for targeting or prosecution. JEFF 3 lab staff members have also provided expert testimony in the central criminal courts of Iraq.

The Latent Print Section is very successful at recovering and analyzing prints from a variety of porous and nonporous evidence using various techniques and items ranging from powder to ultraviolet imaging. The Latent Print Section has assisted with cases involving theater internment facility detainees, sniper incidents, anticoalition force threat letters, and al Qaeda intelligence documents.

In addition, firearm/tool mark analysis has proven valuable. State-of-the-art technology enables the Firearm/Tool Mark Section to perform firearm identification and function; ammunition identification and examination; microscopic comparisons of fired bullets, cartridge cases, and tool marks; serial number restoration; physical fracture matching; distance determination; and trajectory analyses. Most notable is the Firearm/Tool Mark Section's ability to match explosively formed projectile cones and liners through tool mark analysis and to link several sniper cases in which coalition members were killed. These capabilities have been used to assist in several high-profile, escalation-of-force incidents involving coalition forces and local Iraqis, and they have also played a critical role in several fratricide cases.

The DNA Section conducts nuclear and Y-chromosomal testing. DNA profiles have been recovered from an amazing list of items, many of which are not traditionally considered viable candidates for DNA analysis. These analyses have proven invaluable in assisting with "duty status, whereabouts unknown" cases in which DNA is obtained from coalition members' personal effects such as shirts, socks, and boots. The DNA analysis capability is used extensively in support of units targeting high-value individuals.

The desired end state of any analysis—latent print,

DNA, or firearm/tool mark—is the tying of forensic evidence to an individual or incident. In the event of a match, or "hit," with existing samples on the database, subjects may be detained. In other situations, a case manager fusing intelligence notifies the submitting unit if forensic information has produced operationally relevant intelligence. This feedback can provide the unit with expedient, actionable intelligence for targeting missions or evidence for prosecution. If the subject of the analysis is detained, a lab law enforcement professional prepares an evidence or prosecution packet for potential use in the Host Nation criminal courts. Law enforcement professionals assigned to labs also provide a critical link to all maneuver units; commanders rely on these evidence experts for guidance and standard operating procedures.

As the governments in Iraq and Afghanistan continue to evolve toward the rule of law, evidentiary detainments and prosecutions will play an increasingly crucial role in developing a stable future. As the situation stabilizes, there will likely be an increase in exploitable evidence used solely for prosecution as opposed to targeting.

JEFF 3 defines success by the ability to provide units with expedient answers to target or prosecute the enemy. There was a 150% increase in caseload at the lab over a 6-month period in 2008 along with a record number of matches in the last 2 months. Apart from the in-theater benefits of JEFF labs, one of the most substantial impacts of forensic analysis on AT efforts is the ability to prevent another incident like 9/11. The thousands of matches made in Iraq and now Afghanistan have allowed us to interdict individuals who want to cause harm to America before they reach US soil.

Lessons Learned for Afghanistan

Listed below are some lessons learned from the US expeditionary forensic experience in Iraq. Although many of these issues are being addressed through the Forensics Capabilities Based Analysis (CBA), the long lead times for the Joint Planning, Programming, Budgeting, and Execution process mean that a number of these capabilities won't be institutionalized any time soon. In the meantime, the lessons learned in Iraq should not be lost because many of these lessons learned apply to our fight in Afghanistan:

Issue 1: Redundancy of Effort

Discussion

This is a multifaceted issue. Currently, multiple labs run by different organizations are conducting forensic analysis using similar capabilities. As individual examiners are very hard to find, and even fewer are willing to deploy, much effort needs to be placed on maximizing the examiners who are currently available to meet the current requirements. Finally, multiple organizations are responsible for training, equipping and funding needed for of each the deployable labs. The resulting stove-piping of information and minimal cross-talk between labs, databases and analysts are especially noticeable in incidents involving accidental submission of evidence to multiple labs.

Recommendation

The development of an enduring capability consisting of a system of modular deployable labs built around commanders' requirements is essential for future operations. This plug-and-play method would maximize responsiveness to mission requirements, maximize available examiner use, and minimize duplication of effort. The US Army Criminal Investigation Laboratory has proposed an Army concept that would provide the enduring capability for such an effort.

Issue 2: Lack of a Common Database

Discussion

Results of forensic analysis and reports are not consolidated on one central database to ensure BCTs and analysts can leverage this information to target or prosecute individuals or to link networks. This unmet need results in unit-level gaps related to targeting and intelligence analysis.

Recommendation

Tangible results could be obtained from the development and use of a common database for reporting (i.e., Combined Information Data Network Exchange or CIDNE). "One stop shopping" for analysts seeking forensic information for intelligence and FP purposes is a critical yet often forgotten piece of battlefield forensics.

Issue 3: Forensic Exploitation Training Gap

Discussion

Pre-deployment training is limited and is performed largely by units through the efforts of the US Army Intelligence Center and the US Army Military Police

School mobile training teams. There is a gap in their ability to ensure all deploying units have adequately trained personnel in basic forensic exploitation.

Recommendation

Efforts are being made at this time for this training to become an enduring requirement for deploying units. This will ensure units can and will fully leverage the benefits of expeditionary forensics.

Issue 4: Expeditionary Forensic Labs as an Enduring Capability

Discussion

Currently, the deployment of most forensic labs in support of overseas contingency operations are executed through a contract solution. In the event operations are concluded in Iraq and Afghanistan, the expeditionary forensic efforts would not be an enduring capability. The Forensics CBA has addressed this gap, and through the efforts of multiple organizations, an enduring solution is being developed.

Richard A. Swearengin, a latent fingerprint examiner assigned to the US Army Criminal Investigation Division, Joint Expeditionary Forensic Facility 6, uses a monitor to compare a latent fingerprint, left, and a recorded fingerprint, right, at Kandahar Air Base, Afghanistan, 4 May 2010. (U.S. Air Force photo by Tech. Sgt. Michele A. Desrochers/Released)

Recommendation

Once expeditionary labs become an enduring capability established within the Services, the warfighter will fully realize the true impact of expeditionary forensics. A lead has been tasked to develop an enduring DOD expeditionary capability.

Issue 5: Increasing the Use of Nuclear DNA

Discussion

During my time as officer in charge in Iraq and through the present, nuclear DNA (nDNA) analysis has provided superior capability in identifying individuals of interest and high-value targets and in providing key linkages to criminal and insurgent networks. This evidence is very hard to cover up because nDNA remains on many objects with which one comes into contact. In contrast to fingerprints, which insurgents constructing, transporting, or placing improvised explosive devices can mask by wearing gloves, nDNA is difficult to disguise.

Recommendation

The educational continuation for commanders on the use of nDNA and the utilization of this capability in support of deployed labs will maximize the detection of individuals of interest.

Conclusions

The road ahead will be a busy one for the expeditionary forensics labs. As the governments in Iraq and Afghanistan continue to evolve toward the rule of law, evidentiary detainments and prosecutions will play an increasingly crucial role in developing a stable future. As the situation stabilizes, there will likely be an increase in exploitable evidence used solely for prosecution as opposed to targeting. From the battlefield to the courtroom, expeditionary forensics is eager to meet this challenge.

MAJ Michael A. Johnston was the officer in charge of the JEFF 3 lab at Camp Victory, Baghdad, Iraq. He holds a bachelor's degree in criminal justice from Kent State University and a master's degree in organizational and business security management from Webster University. An earlier version of this article focused on JEFF 3 lab operations in Iraq was published in Military Police *19-09-01.*

1 Johnston, Michael. "Expeditionary Forensics." *Military Police,* 19 September 2001.


US Army Training and Doctrine Command G2
TRADOC G2 Intelligence Support Activity
Threat Terrorism Integration
Terrorism
KNOW THE ENEMY
THREATS TERRORISM TEAM
T3 Advisory
IRREGULAR FORCES : Handbook No.1.08
Author's Draft
COMMENTS Welcome
FM 7-100.3
OPFOR
U.S. Army TRADOC
TRADOC G2
Handbook No. 1.08
Irregular Forces
Author's Draft April 2010
How the OPFOR Fights... TTP
...Tactics, Techniques, and Terrorism
OE
Actors
Motives
Intent
Design
Indicators
Capabilities
Visit
TRISA website:
AKO Three "Click" Drill-Down
Type TRISA-CTID & "click" 1
TRISA-CTID
Search
Login to AKO/DKO
Login
or
CAC Login to AKO/DKO
CAC Login
"click" 2
Irregular Forces
DoD Organizations
TRISA | TRISA-CTID
3
Irregular Forces
"check & click"
NEW
Irregular Forces
TRISA
KNOW THE ENEMY
TERROR THREAT INTEGRATION
TRADOC G2 Intelligence Support Activity
Threats Terrorism Team (T3)
TRISA
MAY 2010
No. 8-10

MISSION ASSURANCE ASSESSMENTS

>> AND THE ROAD AHEAD

U.S. Air Force photo by Tech. Sgt. Efren Lopez/Released

Improving DCIP and AT Programs

By Maj Keith Derbenwick, USAF

Assessments evaluate the effectiveness of the DCIP and AT programs across DOD—and can offer ways to make them stronger.

Introduction

The Joint Staff Deputy Director for Antiterrorism and Homeland Defense (J-34 DDAT/HD) recently published a report focusing on trends identified within the Joint Staff AT and Defense Critical Infrastructure Program (DCIP) assessment programs.[1] The assessment process serves two distinct purposes: (1) to provide the organization with an assessment of their DCIP and/or AT programs, along with possible mitigations to make their programs stronger, and (2) to provide the chain of command with the "ground truth" of the DCIP and/or AT programs throughout their areas of operation.

Assessment Programs

The Joint Staff is mandated to conduct assessments to evaluate the effectiveness of the DCIP and AT programs across DOD. Specifically, the Joint Staff, J-34, is responsible for three assessment programs to fulfill this requirement and ensure DOD components are properly executing AT and DCIP. These assessment programs are as follows:

1. **Higher Headquarters Assessments (HHAs) of Combatant Command (COCOM) AT and DCIP Programs.** HHAs are conducted by the Joint Staff, J-34, to evaluate AT and DCIP programs at the COCOM headquarters level. The HHAs have recently shown that multiple COCOMs meet 100% of the standards and benchmarks. Although this level of compliance

is commendable, it demonstrates that the assessment process has not kept up with the programs as they mature.

2. **Joint Staff Integrated Vulnerability Assessments (JSIVAs) on AT Programs at the DOD Installation Level.** JSIVAs are conducted by the Defense Threat Reduction Agency (DTRA) on select DOD installations to evaluate AT program implementation. Due to the significant expertise of the personnel on the JSIVA teams and the detailed level of the benchmarks, these assessments continue to provide value to the installations. The primary concern with JSIVAs is the inability to accurately track assessment results and requisite mitigations.

3. **DCIP Assessments.** DCIP assessments are conducted by the Mission Assurance Division (MAD) on selected critical assets across DOD. As of CY 2010, MAD is conducting DCIP assessments independently from the JSIVAs.[2] The JSIVA and DCIP teams have been decoupled to allow the DCIP assessments to focus on the specifically designated critical infrastructure assets for the Joint Staff and OSD without affecting the scheduled JSIVAs. The MAD DCIP assessment teams are currently managed by the OASD (HD&ASA) DCIP office.

Although this article focuses primarily on ways to improve the assessment processes, implementing the following recommendations would also greatly enhance the mission assurance posture of DOD.

How Can We Improve?

Due to the fast-paced and highly dynamic operating environment in which the AT and DCIP programs operate, it is necessary to make continuous improvements to AT and DCIP programs. During a recent J-34 assessment of the Joint Staff Mission Assurance assessment programs, multiple issues were identified. The recommendations with the most impact on AT and DCIP programs are briefly discussed below.

1. Improve the reporting mechanism for vulnerabilities, remediation, and mitigation plans as well as risk management strategies.

Following an assessment, there is no formal mechanism to effectively track the concerns and vulnerabilities reported by the assessment teams. The Core Vulnerability Asset Management Program (CVAMP) is intended to be a repository of vulnerability information that may be used by commands to track vulnerabilities, request funds for mitigation, and report to higher commands on the status of AT measures. CVAMP is structured for AT vulnerability information rather than DCIP, but it can potentially be used for both types of assessments. Unfortunately, CVAMP usage is generally associated with the Combating Terrorism Readiness Initiatives Fund account for the purpose of requesting funds for mitigation of vulnerabilities. This inconsistent usage results in CVAMP being extremely limited in its usability to track vulnerabilities and manage risk. According to a 2007 DTRA report, over the course of six JSIVA assessments across one COCOM, only 56 observations out of 262 were recorded in CVAMP by the installations.[3]

Due to the fast-paced and highly dynamic operating environment in which the AT and DCIP programs operate, it is necessary to make continuous improvements to AT and DCIP programs.

Although JSIVAs constitute only a small percentage of the vulnerability assessments conducted on DOD facilities, there is no formal mechanism for DTRA to track results from Higher Headquarters (HHQ) internal assessments. The limited access to complete and accurate data results in DTRA's and the Joint Staff's inability to produce accurate trends reports, focus future assessments on areas of concern, or track the mitigation of vulnerabilities. On top of the inability to accurately track vulnerabilities, the status of mitigations is unknown until the facilities and assets are revisited for another assessment. This means the lag time in tracking the resolution of concerns and vulnerabilities is often as long as 3 years.[4]

In addition to tracking vulnerabilities and mitigations, the ability to track the assumption of risk is vital. Managing risk is at the heart of JSIVA, DCIP, and HHQ assessments. Unfortunately, none of these assessments measure or evaluate how commands are managing risk. Currently, the assessments determine where commands and assets are vulnerable, but there is no mechanism in place to evaluate how commands respond to those vulnerabilities. Risk can be managed through the mitigation of a vulnerability or assumed by a commander without solving the vulnerability. The problem remains that there is no way to track the assumption of risk or even to track whether a commander has acknowledged the risk. The bottom line is that local commanders are assuming risks in their area of responsibility (AOR) without a mechanism for reporting the assumption of risk to the next-higher echelon of command.

Results from DCIP assessments are equally as disparate. There is no system designated as a repository of vulnerability information following DCIP assessments.

The inability to track concerns, vulnerabilities, and the assumption of risk in a collective system prevents the dissemination of accurate data throughout the chain of command. This lack of data prevents HHQ from having a solid understanding of the DCIP and AT programs on its installations, and this lack of data also limits the ability to track the mitigation of vulnerabilities. (U.S. Army photo by Spc. Charles W. Gill/Released)

CVAMP is a potential tool for reporting DCIP assessment results, but—as currently designed—it is not completely adequate. The Strategic Mission Assurance Data System (SMADS) was designed to incorporate a host of information related to critical infrastructure assets; however, to date, the use of SMADS for tracking asset vulnerability information has been inconsistent and incomplete. A more comprehensive tracking mechanism will ensure greater visibility across DOD and provide better accountability.

The inability to track concerns, vulnerabilities, and the assumption of risk in a collective system or with a reliable method prevents the dissemination of accurate data throughout the chain of command. This lack of data prevents HHQ from having a solid understanding of the DCIP and AT programs on its installations, and this lack of data also limits the ability to track the mitigation of vulnerabilities. Higher-level commanders have no way of knowing whether commanders in their AORs have assumed risk and consciously chosen not to implement solutions. Furthermore, there is no means for higher commanders to assess risk across their AORs.

Following an assessment, there needs to be a formalized chain of documentation to ensure proper tracking of assessments of vulnerabilities, remediation and mitigation efforts, and risk assumption. A possible sequence of events following an assessment would be as follows:

1. The command inputs assessment results into the requisite database.

2. The command develops a risk management plan that includes vulnerability remediation and mitigation strategies and enters those remediation and mitigation strategies into the database.

3. The next-higher-level person in the chain of command receives automated updates on vulnerability data and remediation and mitigation plans.

4. The Joint Staff receives automated aggregated reports from all commands.

This thorough tracking of assessments of vulnerabilities, remediation and mitigation efforts, and risk assumption will provide each chain of command with a clearer understanding of their DCIP and AT programs' status and a more accurate picture of the risks assumed throughout that command's AOR. A vulnerability reporting tool is highly recommended to aid DOD in improving the DCIP and AT programs. In addition to collecting the specific vulnerabilities the tool will facilitate, enhance, and improve risk and vulnerability assessments and tracking, and provide an up-to-date status of remediation and mitigation efforts. By providing these capabilities the programs will eliminate or reduce risks and vulnerabilities and increase awareness of risk assumption. With the proper vulnerability reporting tool, organizations throughout the chain of command will be able to rapidly prepare up-to-date trend analyses. This data will allow for more proactive, AOR-wide vulnerability remediation and mitigation. In summary, a vulnerability reporting tool will provide commanders with higher mission assurance via the tool's unique capability to track remediation and mitigation efforts, risk assumption, and the overall state of the DCIP and AT programs across the AOR.

2. Decentralize DCIP management.

Recent discussions within the DCIP community suggest that too much of the assessment program's oversight and management are centralized at the senior levels of DOD leadership. This program's centralization

was necessary during the early establishment of DCIP to ensure consistency, but now it inhibits progress toward the program's goals. Continued efforts to decentralize DCIP by placing more of the policy-generating and program evaluation functions at the Service and COCOM level will allow the J-34 staff to focus on other critical aspects of the DCIP and AT programs.

3. Revise the standards and benchmarks used for HHAs and fully implement the HHAs to include Military Services and defense agencies.

The standards and benchmarks used during HHAs[5] are in need of review. These standards and benchmarks were originally designed to provide a framework for evaluating the establishment and basic maintenance of DCIP and AT programs at the COCOM headquarters level when the programs were in their infancy. In many cases, the benchmarks simply measure whether a headquarters has a particular AT or DCIP program or policy rather than measuring the effectiveness of that program or policy.

Due to the fact that recent COCOM assessments have resulted in "no deficiencies," it is clear that the basic-level evaluation stage necessary during the development of the programs has quickly become outdated. To prevent programs from outgrowing the assessment process, a series of Measures of Performance should be established to initiate revisions to the HHA standards and benchmarks. The intent is not to make a perfect score unattainable but to ensure that these assessments are refined and continue to add value to COCOM programs.

Because HHAs are currently only performed at the COCOM level, excluding the Services and defense agencies, the Joint Staff is not able to gather an accurate, DOD-wide assessment of the state of DCIP or AT programs. Updating the standards and benchmarks and broadening the scope to include Services and defense agencies will make it possible to effectively monitor DCIP and AT program implementation.

4. Increase active outreach to reinforce the Combatant Commander Initiative Fund as a valid option for vulnerability remediation.

Many commands rely on short-term funding to fix urgent vulnerabilities discovered during JSIVAs and DCIP assessments. By nature, the mitigation of vulnerabilities to a base's AT protection should not have to wait for funding to be programmed in out-years. In many cases, these are urgent fixes to vulnerabilities that create significant potential problems for the command or asset. The COCOM's ability to shape the DCIP and AT programs and remediate current and emerging vulnerabilities will be greatly enhanced by fully leveraging the Combatant Commander Initiative Fund.

5. Develop a DCIP communitywide investment strategy.

The DCIP is a centrally managed and inherently collaborative community; however, the interdependent and overarching nature of critical infrastructure protection requires a cohesive and unified DOD-wide approach. DCIP does not have a short-term or long-term funding mechanism and also lacks a strategy for investment. The community needs a formalized, centrally managed investment strategy to tackle prioritized critical asset vulnerabilities. This is one area in which greater senior-level involvement may aid in defining a collaborative approach, or with development of pending policy.

6. Revise the DOD Antiterrorism Strategic Plan.

In June 2004, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict published the DOD Antiterrorism Strategic Plan,[6] composed of five strategic goals and 35 supporting performance objectives. According to a 2008 DTRA assessment,[7] the AT program was behind schedule on 25 out of 35 strategic goals. Although the assessment was based solely from JSIVA data, it shows that compliance with the strategic goals needs to be emphasized. A working group should be convened in order to study these strategic goals, evaluate the deficiencies in achieving these goals, and implement a new DOD Antiterrorism Strategic Plan.

7. Increase AT and DCIP education throughout DOD.

Over the past decade, antiterrorism and infrastructure protection have been topics of high relevance to DOD, yet they are both areas in which professional military education is lacking. Despite the obvious importance of both fields, there is a widespread lack of knowledge and experience across DOD in these areas. Developing AT- and DCIP-related education and training opportunities which highlight and emphasize existing programs and lead to a culture of mission assurance throughout DOD. Currently, the main focus of AT and DCIP training is on specific billets (i.e., AT Officers) and on senior officers participating in pre-command courses. Junior officers, noncommissioned officers (NCOs), and DOD civilians receive very little formal education on AT unless they are assigned specifically to an AT-oriented position. DCIP training and education are provided on an even more infrequent basis. Development of formal DCIP training is still in its infancy, although the DCIP Personnel Sector[8] is leading an effort to develop this training and certification. Currently, there is insufficient engrained knowledge about both AT and DCIP programs across DOD.

Fully integrating AT and DCIP training into the

military professional development framework would provide officers, NCOs, and DOD civilians with a solid understanding of AT and DCIP. In addition, commanders would be provided with the instruction to properly protect their organizations and infrastructure, which is critical to mission success.

Conclusion

The above recommendations are a static snapshot of the DCIP and AT programs, representing only a portion of the issues and recommendations outlined in the Joint Staff report. Effectively evaluating these programs is a key component of ensuring continued success. These programs have made enormous strides over the past decade to improve DOD's defenses against all threats and hazards, to ensure mission execution, and to protect DOD personnel.

Major Keith "Derby" Derbenwick, USAF is currently serving as an Action Officer on the Joint Staff, J-34 Deputy Directorate for Antiterrorism Homeland Defense (DDAT/HD) Antiterrorism/Force Protection (AT/FP) DCIP, Assessments, and Resources (DAR) Division. After graduating from the USAF Academy he served as an F-16 pilot, followed by time as an Exchange Officer with the United Kingdom Royal Air Force, and also as a Legislative Fellow on Capitol Hill.

---

1 Joint Staff. *DOD AT and DCIP Assessment Trends Report.* 2010.

2 Joint Staff. "DMS Message, Change 1 to CY10 JSIVA, DCIP, & MTT Schedule." November 13, 2009.

3 Defense Threat Reduction Agency. *Mitigation Analysis Report.* 2007. p. 2

4 DODI 2000.16, *DOD AT Standards.* December 8, 2006. p. E3.31.5

5 Joint Staff. *Higher Headquarters AT Program Review Benchmarks*. January 2007.

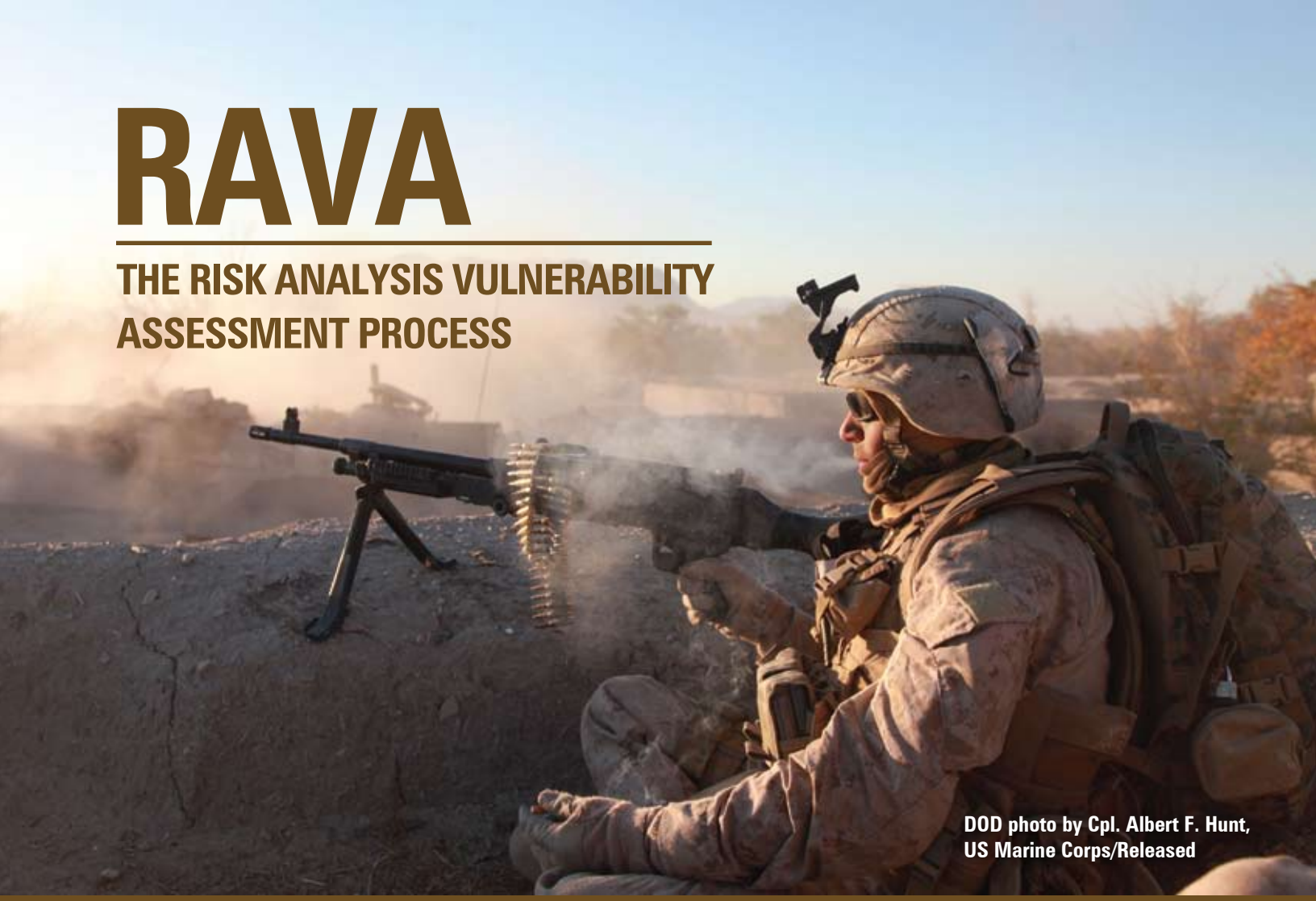
6 DOD O-2000.12-P, *DOD Antiterrorism Strategic Plan.* June 2004.

7 Defense Threat Reduction Agency. *JSIVA Trend Analysis*. 2008.

8 Office of the Undersecretary of Defense for Personnel and Readiness.

RAVA

THE RISK ANALYSIS VULNERABILITY ASSESSMENT PROCESS



DOD photo by Cpl. Albert F. Hunt, US Marine Corps/Released

Quantifying Assets, Threats, and Vulnerabilities

By Mr. Richard Vella

Assessment of the potential risks to personnel and assets from terrorism is a challenge faced by all US Government organizations.

To accomplish its mission, an organization must protect personnel and critical assets from all threats, including acts of terrorism. Assessment of the potential risks to personnel and assets from terrorism is an issue faced by all US Government organizations. DOD is in the crosshairs as the government entity responsible for enforcing US foreign policy around the globe, particularly in the Middle East.

Recent developments in terrorism seem to have focused on the civilian sector. The Fort Hood shootings, the New York City recruiting station attack, and the Fort Dix Six all show that DOD is not immune to targeting and should be a cause of concern for commanders and civilian leaders everywhere. Spending limited funds to protect personnel, assets, and equipment is a delicate balancing act in risk management. The question always arises: "Am I getting enough bang for my buck?" Without a quantitative method for risk assessment and analysis, this question cannot be answered. Responding, "I think so," simply won't cut it.

A quantitative risk analysis and vulnerability assessment methodology called RAVA (pronounced "Ray-Va"; see Figure 1) has been developed by the Antiterrorism Services Branch (CI662), part of the Naval Facilities Engineering Service Center (NAVFAC ESC) in Port Hueneme, California. RAVA assists organizations

in identifying and measuring their greatest risks and determining the most cost-effective countermeasures for mitigating those risks. Although this method is primarily designed to address terrorist threats, the same process is also used to effectively address criminal activity, sabotage, and espionage threats.

CI662 is recognized as a center of expertise within the DOD community for physical security and AT, providing services for any DOD or federal agency. A typical assessment team is made up of subject matter experts specializing in physical and technical security, law enforcement, forced-entry tactics, AT, FP, engineering, criminal and terrorist intelligence, logistics, and quantitative analysis.

Risk Management

In risk management, the estimates calculated from a quantitative risk assessment are used as the basis for making decisions. The following definition of risk management is used in the security engineering field:

> Evaluating alternative countermeasures and design options and selecting from among them. This involves consideration of political, social, economic, and engineering information with risk-related information to develop, analyze, and compare acceptable options and to select the appropriate response to a potential threat. The selection process requires placing value on such issues as the amount of risk considered acceptable, the reduction in risk due to applied countermeasures, and the reasonableness of the costs of countermeasures.

Because risk is quantifiable, it becomes a yardstick that can be used to make decisions about allocating resources (funding and people). Risk is associated with the protection of assets (personnel or property) rather than facilities (see Figure 2).

Security countermeasures tend to be selected based on their likelihood of lowering the risk to the asset as well as on cost effectiveness. In many cases, risk analysis and risk management become an optimization analysis that examines risk reduction values (due to implementing countermeasures) and the associated costs to implement the identified countermeasures through a simple cost–benefit study.

Although performing a detailed risk assessment is complicated, following the RAVA methodology makes it manageable. The results are tailored to an organization's needs and can be used to make informed decisions in the allocation of resources to mitigate risks.

RAVA Methodology

The primary purpose of RAVA is to quantitatively measure threats, assets, vulnerabilities, and risks associated with large and/or small government facilities. It establishes a security baseline, explores upgrades, recalculates vulnerabilities and risks, and recommends optimized features or improvements for facilities. In essence, a RAVA identifies current levels of vulnerability and risk and then identifies improved levels with the implementation of specified countermeasures (see Figure 3). In addition, RAVA identifies the associated cost and impact of the improvements. RAVA includes the performance of six sub-analyses: threat, target, vulnerability, optimization, risk, and cost–benefit.

RISK AS DEFINED BY RAVA

To quantify risk, several factors need to be known:

1. The potential threat against the asset being protected
2. The value of the asset to the threat
3. The value of the asset to the organization (user)
4. The countermeasures in place to mitigate the threat against the assets. The risk formula is further defined as:

RISK =

ASSET VALUE (IMPACT) **X THREAT** (CAPABILITIES & LIKELIHOOD) **X VULNERABILITY** (SUSCEPTIBILITY TO ATTACK)

Risk, as defined by the RAVA methodology, is dependent on five variables:

1. The likelihood that an attack will occur
2. The probability that the attack will be successful (Threat Effectiveness)
3. The weakness of security measure to be exploited by threat sources
4. The importance of the assets to the user
5. The importance of the assets to the threat

FIGURE 1. Risk as Defined by RAVA

Threat Analysis

Threat analysis is based on information collected during the site visit. The information produces a threat rating, which measures the threat likelihood (the probability an attack will occur), and a terrorist effectiveness rating (the probability that an attack will be successful).

Target Analysis

Target analysis is designed to evaluate and measure the value of all targets to the user and to the aggressor. Targets could include any type of asset or target including people, buildings, barracks, hangars, piers, runways, antenna fields, water tanks, and electrical power distribution lines. The end result of the target analysis is a numeric rating based on the target value or criticality to the user and the target value or usefulness to the aggressor.

The major elements of the risk and vulnerabilities assessment process.

THE SITE VISIT:

- User Input: Site definition, preliminary asset identification, identification of potential threats, consequences of loss, local requirements and constraints.
- Local Law Enforcement Input: Local conditions including criminal environment, law enforcement support, and logistics.
- Site Survey Input: A security review of an existing site or project plans to identify existing or planned security measures and document vulnerabilities.

THE ANALYSIS:

- Target Analysis: Identifies and appraises specific assets; overall target value is based on the value of the asset to the user and the aggressor.
- Threat Analysis: Identifies and quantifies specific threats to specific targets; overall threat rating is based on the potential effectiveness of an aggressor, and the likelihood that the threat will be carried out.
- Vulnerability Analysis: Quantifies the vulnerability of a specific target to a specific threat using a scale of zero to one.
- Risk Analysis: Determination of the probability of occurrence and the impact or effect if a given loss occurs.
- Optimization Analysis: Measure that can be applied to reduce or eliminate vulnerabilities and risk.

FIGURE 2. Major Elements of the Risk and Vulnerability Assessment Process

Vulnerability Analysis

Vulnerability analysis is designed to quantitatively evaluate and measure how vulnerable a specific asset is to a specific threat. This phase of RAVA most closely reflects a standard assessment done by either a higher headquarters or the Joint Staff Integrated Vulnerability Assessment Team. In this phase, the countermeasures currently in place for a specific target are assigned a value based on their effectiveness in mitigating threats. Analyzed countermeasures could be either programmatic or procedural. The end result is a baseline vulnerability rating (BVR) associated with the specific target being analyzed.

Optimization Analysis

Optimization analysis is the reapplication of the vulnerability analysis after implementing hypothetical improvements resulting from countermeasures that could be used for a specific asset. Hypothetical countermeasures could include programmatic or procedural options. The end result is an optimized vulnerability rating (OVR) associated with the specific target being analyzed. Based on the optimization analysis, the average vulnerability and risk rating can be identified and stated as a percentage.

Risk Analysis

Risk analysis is the aggregation of the threat, target, vulnerability, and optimization analyses to determine the calculated value of risk associated with a specific asset that is being targeted by a specific threat.

Cost–Benefit Analysis

Cost–benefit analysis compares the potential results of specific countermeasures for reducing or mitigating threats against specific assets. The cost–benefit analysis is based on cost versus reduction in vulnerability and risk.

Defense-in-Depth

RAVA uses the process of defense-in-depth, also known as layers of defense, as a means to gauge the value of protection afforded each asset. Defense-in-depth assumes that each layer of defense provides an opportunity to deter, detect, delay, or prevent aggressors from reaching their ultimate goal. RAVA considers four primary layers of defense when computing the overall value of vulnerability and risk:

Layer 1: installation perimeter

Layer 2: asset enclave perimeter (if there is one)

Layer 3: asset exterior (e.g., building elevation, wall)

Layer 4: an enclaved area within the asset (e.g., secured vault, arms room)

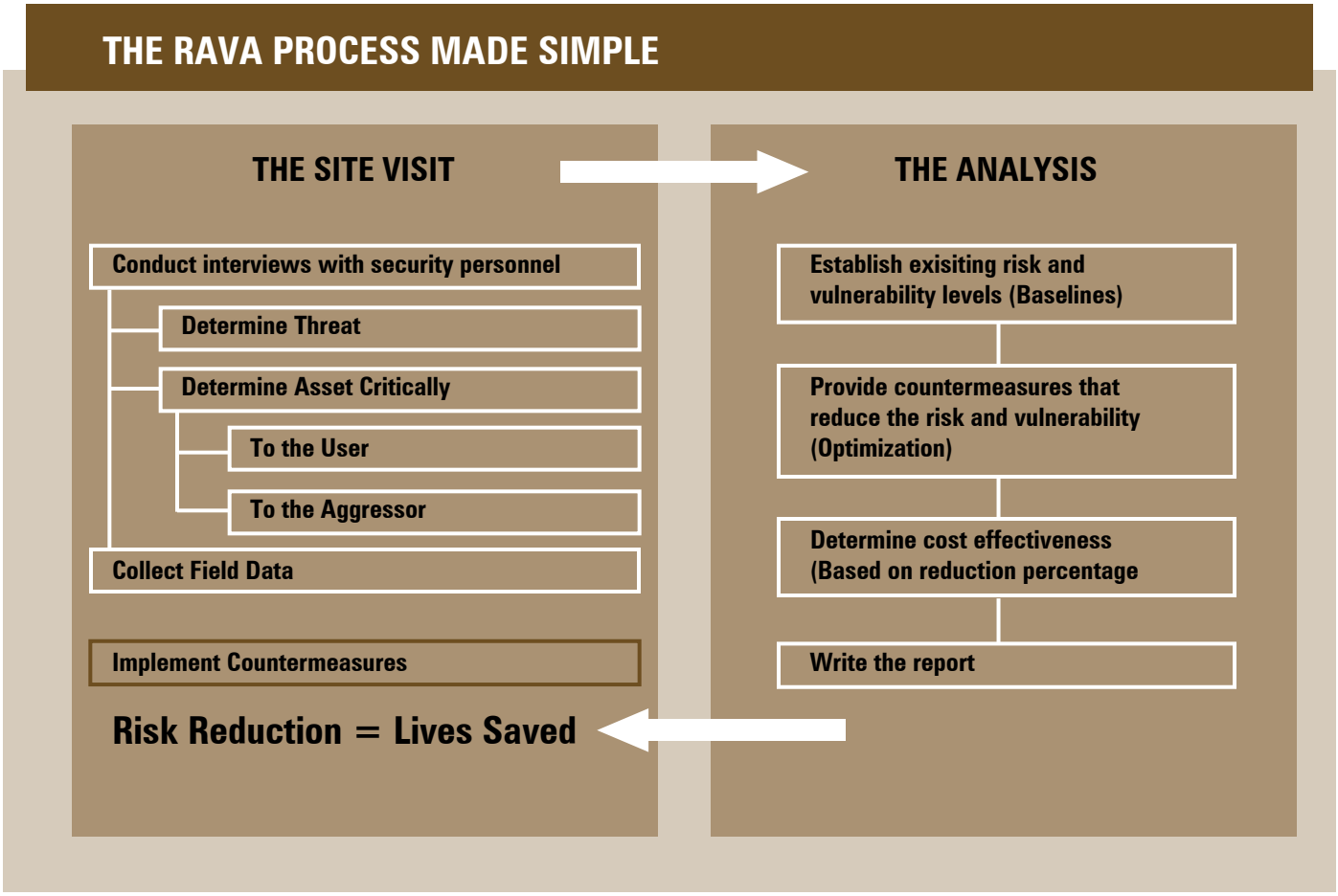


FIGURE 3. The RAVA Process Made Simple

RAVA goes further than simply identifying whether a particular layer exists. It also considers all countermeasures associated with each layer. In most cases, each layer includes 20–50 individually rated countermeasures, all of which are assessed and considered in the RAVA process. In many cases, an asset assessed as part of this effort will not include all four layers. A building asset situated off base, for example, will not include Layer 1, and unless the building has its own enclave, it will not include Layer 2. In all cases, the asset will have Layer 3. If the asset is a building and the building has interior spaces that have been identified as critical areas with controlled access, then it will include Layer 4. In situations involving a stand-alone asset (e.g., water tank, transformer, antenna tower), only Layers 1, 2, and 3 would be considered, with Layer 3 being the actual asset.

Measurement

RAVA is a quantitative assessment using mathematical equations to calculate and measure vulnerability and risk (see Figure 4) versus the standard vulnerability assessment process, which is a qualitative or subjective assessment focusing on regulatory requirements. Both methodologies identify vulnerabilities and recommend countermeasures to mitigate those vulnerabilities; however, RAVA goes further because it identifies current values of vulnerability and then reassesses those values of vulnerability based on implementation of recommended countermeasures.

Not only does RAVA provide quantitative measurements of vulnerability and risk, it also provides cost estimates for the recommended countermeasures developed as part of the RAVA if they were to be implemented. Knowing the BVR and comparing it to the OVR and then calculating the cost to reach the OVR, the RAVA methodology produces a cost–benefit analysis that can be used to prioritize countermeasures or compare one facility to another.

To summarize, RAVA quantifiably measures vulnerability and risk, prioritizes recommended countermeasures, prioritizes facilities, and compares cost and countermeasure effectiveness. Most importantly, RAVA lets the customer know how vulnerable the facility is, what to do to reduce the vulnerability, how effective the recommendations will be in reducing the vulnerability, and at what cost.

Sample RAVA Worksheet Chart and Graph

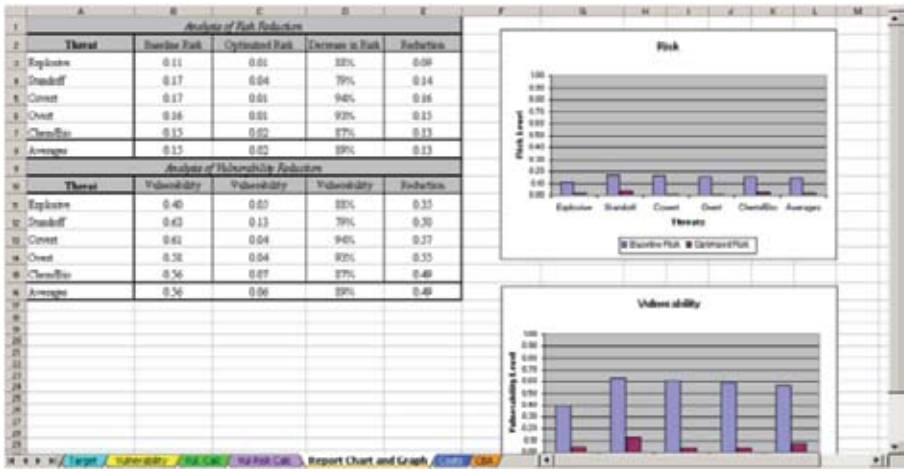


FIGURE 4. Sample RAVA Worksheet Chart and Graph

RAVA Approach

Regardless of the type of analysis or study, the resulting recommendations need to be based on a given threat. As it relates to designing physical measures to counter the identified threats, the CI662 team performing RAVA must have a clear understanding of the design basis threat (DBT) to make appropriate and cost-effective recommendations. The performance of RAVA is not driven by regulation or design standards; therefore, the DBT must be identified before recommendations can be generated.

CI662 works with the customer to identify critical assets warranting RAVA. In many cases, commands use their Mission Essential Vulnerable Area list as a basis for selecting critical assets. Additionally, the customer sometimes considers Single-Point Failure assets as critical assets.

Unlike standard vulnerability assessments, RAVA quantifies vulnerabilities and risk, determines the cost effectiveness of specific improvements, and helps prioritize countermeasures. This in turn allows commanders to plan for and seek hard-to-get funding.

For more information, contact the NAVFAC ESC Antiterrorism Services Branch at (805) 469-2438.

THE SERPENT AND THE SWORD

US Navy photo by Mass Communication Specialist 3rd Class Jake Berenguer/Released)

Outbreak Prevention and Response

by MAJ James P. Harwell, USA

Developing an All-Hazard Approach to Countering Infectious Disease Threats in the 21st Century

In November 2009 the National Security Staff published Presidential Policy Directive 2 (PPD-2), *The National Strategy for Countering Biological Threats*. Released in the midst of the 2009-H1N1 "Swine Flu" pandemic and just before the publication of the Commission on the Prevention of WMD Proliferation and Terrorism's report card, PPD-2 signaled a significant policy shift that aims to better protect the United States against infectious disease threats.

Prior to the publication of PPD-2, executive policy primarily focused on components of the threat spectrum. In 1996, the Clinton Administration released *Presidential Decision Directive National Science and Technology Council 7 (NSTC-7), Emerging Infectious Diseases,* which focused on the development of global surveillance systems to identify and respond to novel pathogens. Under the Bush Administration, policy shifted as transnational terrorists sought to acquire weapons of mass destruction. Homeland Security Presidential Directive 10 (HSPD-10), Biodefense for the 21st Century, changed the focus from passive surveillance to denying potential adversaries access to biological weapons and related technologies.

Unlike these threat-specific policy decisions, PPD-2 adopts an "all-hazards" approach to countering the infectious disease threat. The strategy aims to: (1) enhance international capacity to identify and mitigate the effects of outbreaks, whether naturally occurring or resulting from an accidental or intentional release; (2) increase barriers to misuse without limiting responsible research; and (3) enhance the ability to attribute and respond to biological weapons attacks. By understanding the threat and adopting an all-hazards approach to the infectious disease challenge, DOD has the opportunity to better posture our Service members, civilians, contractors, and families to recognize and mitigate the effects of

infectious diseases. This approach has the potential to reduce both the likelihood that infectious diseases, in the form of biological weapons, will be sought out and used by our adversaries and the impact of outbreaks.

The Infectious Disease Threat Matrix

Infectious disease threats are unique within the chemical, biological, radiological, nuclear, or high-yield explosives (CBRNE) threat spectrum. This is due to the inability of man to control pathogens once they are released, a fact that has long been an inherent deterrent to the battlefield use of biological weapons. Infectious disease threats, unlike their chemical and nuclear counterparts, self-propagate through space and over time. Chemical weapons are inherently limited in scale due to the requirement for adversaries to develop robust production capabilities and delivery systems. Large-scale toxic industrial chemical/material facilities, potential targets for adversaries seeking to inflict harm against unprotected populations, generally possess security and redundant control measures designed to limit access and mitigate the effects of a release.

Nuclear weapons, capable of catastrophic strikes against large urban centers, are still the domain of nation-states; only nine states have demonstrated the capability to deploy nuclear weapons, and only the US has used them against another nation. Having developed from military research, the commercial nuclear industry possesses a culture of security committed to limiting the transfer of nuclear technologies and materials to adversaries. In contrast to both chemical and nuclear threats, infectious disease threats are capable of appearing spontaneously, exacting catastrophic financial and human tolls, and then vanishing back into nature. With the advent of globalization, infectious disease outbreaks are only limited by their access to viable hosts.

Over the last 30 years, the world has seen the end of many traditional infectious disease threats but has also witnessed the emergence of new diseases vying to replace them. Additionally, diseases that had been all but eliminated from the threat matrix have begun to reassert themselves, having developed resistance to existing drugs. In recent years, there have been significant advances in the life science community's understanding of disease-causing organisms. Advances in areas such as genomics have supported the development of vaccines, antivirals, and therapeutics. Although many advanced capabilities are still beyond the grasp of non-state adversaries, the continued development of intellectual capital has increased the risk that infectious diseases will soon be used against the US, our allies, and our interests.

By understanding the threat and adopting an all-hazards approach to the infectious disease challenge, DOD has the opportunity to better posture our Service members, civilians, contractors, and families to recognize and mitigate the effects of infectious diseases.

Emerging and re-emerging infectious disease threats and the growing potential for nations and terrorists to exploit naturally occurring pathogens remind us that infectious diseases will always hold a prominent place in the threat lexicon. To mitigate this risk, it is necessary to understand the challenges facing the nation and DOD forces and to develop a comprehensive strategy for mitigating this risk—today and into the future.

EBOLA — EMERGING INFECTIOUS DISEASE

In August 1976, an outbreak of a novel pathogen began in a Catholic Mission Hospital in Yambuku, Democratic Republic of Congo. Almost simultaneously, the virus appeared in the Nzara region of southern Sudan.

Transmission Electron Micrograph of the Ebola Virus. (Public Domain: Dr. Frederick A. Murphy, HHS/CDC)

These outbreaks surprised World Health Organization officials and international scientists, both by its rapid emergence and lethality, and by the fact that these two regions that were suffering near-simultaneous outbreaks had no discernable connections. The virus—later identified as Ebola, a previously unidentified hemorrhagic virus—infected 318 people, with an astonishing 88% case fatality rate; then, almost as quickly as it appeared, it vanished. In the quarter-century since the outbreak, scientists have been unable to identify the virus' natural reservoir. Study of the virus revealed that it is transmitted through bodily fluids and was not an airborne pathogen. Since those initial outbreaks, the virus has re-emerged sporadically in sub-Saharan Africa. Additionally, an outbreak of a strain that was not infective in humans occurred in Reston, Virginia, just outside of Washington, DC, in 1989. This outbreak became widely recognized following the publication of Richard Preston's book, *The Hot Zone,* and reminded scientists that globalization had removed the natural barriers for dangerous pathogens, giving them the opportunity to readily travel across oceans and continents.

In 2007, Andrew Speaker, an Atlanta lawyer, was diagnosed with a drug-resistant strain of tuberculosis. While infected, he knowingly boarded a plane from Atlanta to Europe for his wedding and honeymoon. During his trip, Speaker visited Italy and Greece in addition to other European destinations. After being warned by US officials not to return to the United States due to the risk to other travelers, Speaker flew to Canada and, despite US Department of Homeland Security warnings, was allowed to return through the Champlain, New York, border crossing. During his trip, Speaker risked infecting hundreds of travelers. By ignoring US and international travel restrictions regarding tuberculosis-infected patients, Speaker may have provided a blueprint for future terrorist attacks, giving adversaries a view of potential vulnerabilities.

Emerging Infectious Diseases

Infectious diseases have always been a component of man's environment. However, over the last 150 years, man has gained a greater understanding of the pathogens that have long plagued societies, allowing science to nearly eliminate several of the greatest known killers, including Variola virus major/minor (smallpox), Yellow fever virus (yellow fever), poliomyelitis (polio), and Yersinia pestis (plague).

Although many of these traditional threats are now little more than footnotes in history, new diseases have begun to emerge with the potential to replace them. Since 1973, at least 30 previously undiscovered disease-causing organisms have been identified. Deadly new pathogens such as SARS-associated coronavirus (SARS), HIV and AIDS, Lassa virus (lassa fever), Marburg virus (Marburg hemorrhagic fever), and Ebola viruses (Ebola hemorrhagic fever) have demonstrated tremendous killing potential. Most of these pathogens have not proven capable of sustaining human-to-human transmission, although each has the potential for adaptation. This means that the potential for a mutation resulting in increased severity and transmissibility is well within the realm of possibility.

Re-emerging Threats

As noted earlier, the increased understanding of disease-causing organisms has allowed the developed world to largely—but not completely—eliminate many traditional threats. The downside to the decreased incidence of many of these pathogens, however, is that worldwide agent-specific vaccination programs have atrophied, creating the potential for the re-emergence of these pathogens.

Other factors combine to provide a fertile environment should such a re-emergence occur. Continued worldwide urbanization and globalization have removed many natural barriers to disease spread. Cities in the developing world suffer from overcrowding and often lack the sanitation infrastructure to support massive populations. Air travel allows rapid spread of diseases across oceans and continents, providing new pools of unprotected populations to infect. Similar to the Native American populations that were once decimated by smallpox and yellow fever during European expansion, today we have lost much of our developed immunity to these diseases, leaving us with no natural protection.

Concurrent with our decreased immunity, many pathogens have become resistant to existing antiviral and antibiotic treatments. Today, re-emerging threats, whether naturally occurring (e.g., extensively drug-resistant tuberculosis) or accidentally or intentionally released (e.g., smallpox), pose a threat to the United States, its allies, and its interests.

The Biological Weapons Threat: Challenges in Control

The 20th century was an age of global warfare. For the first time in modern history, nations devoted vast resources in peacetime to maintain large standing armies. To achieve an advantage, nation-states attempted to leverage technological advances. Despite treaty regimes, such as the 1899 Hague Convention, prohibiting the use of gas and biological warfare, some nations developed chemical and biological warfare plans.

In World War I, Germany infected draft animals being shipped to the Allied powers with anthrax and glanders. Although their attempts to affect Allied supply efforts by killing the animals were largely ineffective, this was just the beginning of a biological arms race that would involve much of the modern world and increase the risk to future generations as the global environment evolved. By the time the Biological Weapons Convention (BWC) went into force in 1975, more than a dozen nations had begun biological warfare research and development. Although the BWC has increased barriers to biological

weapons development, advances in the life sciences have increased the view of biological weapons as the "poor man's" nuke and increased the risk of their proliferation and use globally.

Terrorism and Globalization: Foreshadowing the Threat Evolution

Suicide bombers have become a reality of modern warfare. Although conventional suicide bombers use explosives to inflict casualties, the potential exists for a new type of suicide killer to emerge—one who is focused on the intentional spread of naturally occurring diseases in an attempt to effect a severe outbreak.

Although cooperative threat reduction efforts have helped to raise barriers to terrorist acquisition of biological weapons, the possibility remains that terrorists may attempt to use global travel patterns to begin a mass epidemic that could inflict a significant human and financial toll on the United States. Despite increased emphasis in the 2005 International Health Regulations, infectious disease surveillance efforts remain under-resourced, and reporting remains inconsistent. These factors along with the measures taken by governments to delay or contain outbreaks (closing borders, banning imports, etc.) contribute to the likelihood that terrorists may one day intentionally spread a pathogen as a means of attacking the United States and our global partners.

The response to natural outbreaks and terrorist attacks are not mutually exclusive, and a coordinated strategy as needed to reduce the impact of biological events on the United States and its interests. Ongoing efforts have substantially increased the security of our nation's most sensitive biological materials and helped to raise barriers to terrorist acquisition of pathogens. The United States must continue to champion these efforts and push for increased coordination so that the international community is capable of identifying; containing, where possible; mitigating; and rapidly recovering from infectious disease outbreaks.

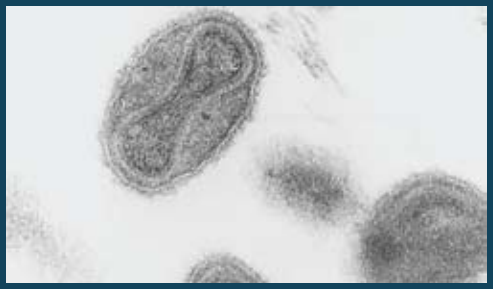
Countering the Threat

Infectious diseases occupy a unique place within the threat lexicon. Whether naturally occurring or intentionally released, an outbreak of any highly transmissible pathogen will be difficult—if not impossible—to contain. Commanders must develop plans that support prevention, protection, response to, and recovery from disease outbreaks, whether naturally occurring or accidentally or intentionally released. This is accomplished through comprehensive planning that supports hazard mitigation at the local, regional, and global levels.

Planning for infectious disease response must be accomplished at every level through the lens of ensuring

SMALLPOX — RE-EMERGING THREAT

In 1980, the World Health Organization (WHO) officially announced that its smallpox eradication efforts had eliminated the disease from the natural environment. In the 21st century alone, prior to the WHO's worldwide vaccination efforts, smallpox killed more than 300 million people worldwide. The last natural case of smallpox was reported in Somalia in 1977.



The "dumbbell-shaped" structure inside the smallpox virion is the viral core, which contains the viral DNA. This DNA acts as the blueprint by which the virus replicates itself once it is released into the host cell. (Public Domain: Dr. Fred Murphy & Sylvia Whitfield, HHS/CDC)

The WHO's efforts were supported by three characteristics that have thus far proven unique to the smallpox eradication effort:

- There is only one form of smallpox, unlike the influenza virus, which comes in multiple types, subtypes, and strains. These differences force the creation of unique vaccines. Conversely, smallpox requires only one vaccine.
- Smallpox has no natural reservoir beyond humans. The inability of the virus to seek out other hosts within the animal kingdom to perpetuate its existence allowed for a surge in worldwide vaccination to eliminate the virus with little risk of re-emergence.
- Unlike bacteria, there are no asymptomatic smallpox carriers. Eradicable viruses usually cause symptomatic disease and do not result in asymptomatic infectious-carrier states that serve as a reservoir for infecting others. This allows vaccination efforts to focus on limiting the spread of the virus. Similar to the use of fire-breaks to limit the spread of wildfires, vaccination efforts strive to achieve herd immunity, thus allowing the virus to "burn itself out."
- WHO vaccination efforts achieved almost universal support from the international community. Through the development of herd immunity, the virus was unable to find sufficient hosts in which to perpetuate itself and thus died out.

Today, smallpox is only known to exist in state laboratories in the United States and Russia, although there has never been a means of confirming this fact. With the cessation of worldwide vaccination programs, the herd immunity that led to the virus' eradication is largely gone. Whether through an act of nature, negligence, or terrorism, the potential re-emergence of smallpox stands as a threat to unprotected populations around the world.

DOD force health protection and maintaining mission assurance. Additionally, commanders must recognize the potential for disease outbreaks to adversely impact the social, political, economic, and security stability of a region. Some factors operational planners should consider when planning for infectious disease threats include:

- **Adopt an Integrated Plans Construct.** Infectious disease threats are not a medical problem—they are an operational challenge. At every level, commanders must coordinate the efforts of the operations, intelligence, and medical plans and policy communities reaching across the medical and conventional weapons management and disposal functions. Executable plans focused on reducing the risk to warfighters must account for disease outbreaks which are a part of the operational environment. Increased resilience of the DOD community to disease outbreaks will sustain DOD's ability to execute its assigned missions.

- **Maintain Situational Awareness.** Intelligence and surveillance are critical to providing commanders with the information necessary to make informed decisions. Commanders must endeavor to "operationalize" medical intelligence and bio-surveillance capabilities. Due to the nature of infectious diseases, where the threat is an unseen micro-organism, these capabilities are necessary to provide the indicators and warnings that will aid commanders in adequately mitigating disease effects.

- **Establish Enduring Communications Programs.** Preparation begins with an informed network of stakeholders. Operational planners must plan for communications with both internal organizations and external partners during all periods of preparation, response, and recovery. Disease outbreaks crosscut other operational issues to create a complex, dynamic operating environment. To remain flexible and responsive, commanders must emphasize preparation and decisive action, empowering leaders at every level to take the necessary measures to limit the impact to the DOD force. Additionally, planners must account for the stability of a region in a pandemic or epidemic environment and the impact on DOD operations.

- **Build Partner Capacity.** It is likely that in any outbreak, DOD forces would be affected at a rate comparable to our civilian counterparts. This means any requirement to support additional missions would compete for degraded resources with currently assigned missions. To minimize the operational risk, commanders must focus on building the capacity of international partners to identify and mitigate the effects of an outbreak.

Following these guidelines should mitigate the threat of infectious disease.

Conclusion

The danger posed by infectious diseases is unique within the threat lexicon due to the variation in hazards, the ability of disease to spread across the battlespace, and the fact that diseases are a component of the operating environment and not an enemy to be defeated. Although technology has provided the potential to counter the infectious disease threat, the same technology provides our adversaries with the capability to inflict an immense financial and human toll on us. Additionally, diseases have proven both resilient and adaptive, increasing the likelihood that we will face far greater emerging threats in the future. To effectively mitigate the risk created by these threats, commanders and planners must develop adaptive, responsive plans that set the conditions to prevent, protect, respond to, and recover from outbreaks. Through preparation and decisive action at the local, regional, and global levels, DOD will limit the impact of these threats and continue to prosecute our national security strategy unimpeded.

MAJ James Harwell is currently a Weapons of Mass Destruction (WMD) Plans and Operations Officer assigned to the Deputy Director for Antiterrorism/Homeland Defense (J-34), Operations Directorate (J-3), Joint Staff and is pursuing a doctorate in biodefense at George Mason University. He is an Army Chemical Officer with 11 years of experience in CBRNE operations supporting the Iraqi theater of operations. He commanded a CBRNE Joint Response Team comprised of both chemical specialists and explosive ordnance disposal technicians while assigned to the Combined Joint Task Force – TROY.

Bibliography

Associated Press. "Border Agent Ignored Warning for TB Traveler." MSNBC, May 31, 2007. Retrieved November 19, 2009, from http://www.msnbc.msn.com/id/18960857/

Centers for Disease Control and Prevention. (2007). "Smallpox: 30th Anniversary of Global Eradication." Updated October 1, 2007. Retrieved November 19, 2009, from http://www.cdc.gov/Features/SmallpoxEradication/

Flight, C. (2005). "Smallpox: Eradicating the Scourge." BBC, November 5, 2009. Retrieved November 19, 2009, from http://www.bbc.co.uk/history/british/empire_seapower/smallpox_01.shtml

Garrett, L. *The Coming Plague: Newly Emerging Diseases in a World Out of Balance*. New York: Penguin Books, 1994.

Karlen, A. *Man and Microbes*. New York: Simon and Schuster, 1995.

National Science and Technology Council. "Emerging Infectious Diseases." Available at http://www.fas.org/irp/offdocs/pdd/pdd-nstc-7.pdf

Oldstone, M. *Viruses, Plagues and History*. New York: Oxford Press, 2010.

Strategic Event Assessment

EVENT: Supreme Court of the United States – *Holder v. Humanitarian Law Project*

First Amendment, Constitution of the United States: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

Patriot Act: a federal crime to "knowingly provide material support or resources to a foreign terrorist organization."

Secretary of State: the authority to designate an entity a "foreign terrorist organization" subject to judicial review.

Foreign Terrorist Organizations (FTO) List

Designation as a FTO impacts travel related to terrorist organizations, makes it a crime to provide material support to terrorist organizations, and freezes the financial accounts of terrorist organizations in U.S. financial institutions

State Department Official Designation Numbers
Foreign Terrorist Organizations: 45
State Sponsors of Terrorism: 4

STRATEGIC SIGNIFICANCE:

WASHINGTON, DC – On June 21, 2010, the US Supreme Court upheld provisions of the Patriot act that made it a federal crime to "knowingly provide material support or resources" to a FTO. (The term defined in 18 U.S.C. § 2339A(b)(1) as "any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals to include oneself), and transportation, except medicine or religious materials."

The Supreme Court ruled 6-3 that the First Amendment does not prevent Congress from barring actions taken to aid terrorist groups simply because the actions may have an expressive component, when it does so based on a reasonable conclusion that the actions are likely to promote the groups' terrorist goals. The Court held that aid provided for a terrorist group's humanitarian activities can free up resources which can be re-allocated to terrorist activities.1

This decision could increase the Department of Justice's ability to prosecute US citizens or groups suspected of contact that provides support to foreign entities designated a terrorist organization. The decision specifically does not apply to domestic organizations. The Preamble of the Constitution notes that a key purpose of government is to "provide for the common defense."

QUOTES:

It is unlawful for a person in the United States or subject to the jurisdiction of the United States to knowingly provide "material support or resources" to a designated FTO.

18 U.S.C. § 2339A(b)(2) provides that for these purposes "the term 'training' means instruction or teaching designed to impart a specific skill, as opposed to general knowledge."

18 U.S.C. § 2339A(b)(3) further provides that for these purposes the term "expert advice or assistance" means "advice or assistance derived from scientific, technical or other specialized knowledge.''

— U.S. Department of State, Office of the Coordinator for Counterterrorism, Legal Ramifications of Designation"

"As Madison explained, 'security against foreign danger is… an avowed and essential object of the American Union.'"

— Chief Justice Roberts Opinion of the Court – Holder v. Humanitarian Law Project

Not even the "serious and deadly problem" of international terrorism can require automatic forfeiture of First Amendment rights.

— Justice Breyer dissenting - Holder v. Humanitarian Law Project

"Held: The material-support statute, §2339B, is constitutional as applied to the particular forms of support that plaintiffs seek to provide to foreign terrorist organizations."

— United States Supreme Court
Holder vs Humanitarian Law Project
21 June 2010

[1] Washington Legal Foundation: http://www.wlf.org/litigating/case_detail.asp?id=425

EVENT: Homegrown Islamist Terrorism in 2009

Since Sept 11, 2001, the US Department of Justice has secured 160 convictions for terrorism offenses and 240 convictions for terrorism-related crimes.[1] In 2009, the United States experienced a spike in terrorist-related incidents involving the homeland or US citizens:

- 139 Muslim Americans were linked to terrorism violence between 2001 and 2009—most incidents occurred abroad.
- 41 Muslim Americans were involved in terrorism in 2009.
- 12 of 32 domestic terrorism events occurred in 2009.[2]

The following US citizens or residents were accused of attacks resulting in fatalities:

- Abdulhakim Muhammad (military-recruiting station, Little Rock, Arkansas: 1 dead)
- Major Nidal Hasan (predeployment processing center, Fort Hood, Texas: 32 dead)
- Shirwa Ahmed (first American suicide bomber, Somalia: 30 dead)

US citizens or residents accused of plotting attacks in 2009 include Bryant Neal Vinas (targeting a train in New York City's Penn Station), Michael Finton (targeting a federal building in Illinois), Najibullah Zazi and four other suspects (multiple bombing targets in New York City), David Coleman Headley (targeting a Danish newspaper and supported Mumbai terrorist attack), and Hosam Smadi (targeting a skyscraper in Dallas).

STRATEGIC SIGNIFICANCE:

Homegrown terrorists are those living in the US who radicalize and initiate attacks with guidance or inspiration from foreign terrorist organizations such as al Shabaab, al Qaeda, or Tehrik-i-Taliban Pakistan. The July 2005 bombings in London, perpetrated by Muslims born in the United Kingdom, brought the concerns of homegrown terrorism to the forefront in the US. Since 2001, 12 of approximately 32 domestic terrorist events occurred in 2009, with a corresponding spike in US citizens or residents charged with participating in terrorist activity. This spike includes five Americans accused of joining al Shabaab in Somalia and five others from the Washington, DC, area charged in Pakistan with seeking to join jihadis in their fight against Americans in Afghanistan.

The radicalization process begins with the "jihadi-Salafi interpretation of Islam and an increasing activist-like commitment to solve global political grievances through violence." This politico-religious ideology can be effectively espoused via social media by English-speaking, American radicals, such as Anwar al-Awlaki and Adam Ghadani. These inspirational extremist messages attract and encourage Americans who are radicalized. Some have traveled abroad and received training from terrorist groups, returning home to conduct attacks in the homeland. Successful acts of homegrown terrorism and overreaction in combating terror at home both produce more homegrown terrorism—essentially a cycle feeding itself through under- or overreaction.

Given the limited number of attempts, fears of a low-level terrorist insurgency at home are exaggerated.[3] The small number of disaffected radicals have not found the Muslim American target audience as receptive as Muslim minority communities in Europe, which has had difficulty integrating these large Muslim minorities. These terrorists are often poorly led, subpar operatives who receive little training and limited guidance or support from terrorist organizations. Often they are turned in before they can conclude their plots.[4] Less than a third of the cases involving Americans in recent years have been successful, suggesting that intelligence, information sharing, local law enforcement, and community relationship-building efforts to detect and disrupt threats are working.

QUOTES:

"We are now moving beyond traditional distinctions between homeland and national security. National security draws on the strength and resilience of our citizens, communities, and economy. This includes a determination to prevent terrorist attacks against the American people by fully coordinating the actions that we take abroad with the actions and precautions that we take at home."

— President Barack Obama
National Security Strategy
May 2010

"Particularly troubling [is] this whole notion of radicalization, of Americans leaving this country and going to different parts of the world and then coming back [and] doing harm to the American people."

— Attorney General Eric Holder
ABC News Interview
July 2010

[1] Holder, Eric. Senate Testimony, April 2010
[2] Schanzer, David, Kurzman, Charles, and Moosa, Ebrahim. *Anti-Terror Lessons of Muslim Americans [white paper]*. 6 January 2010.
[3] Ibid.
[4] Byman, Daniel, & Fair, Christine. "The Case for Calling Them Nitwits." *Atlantic Monthly,* July/August 2010.

DD AT/HD
Joint Staff, J-3 Operations Directorate
Pentagon
Room MB917
Washington, DC 20318-3000

Note: If your copy of the Guardian has been damaged in shipping or is unreadable, please contact us at guardian@js.pentagon.mil. We will send out an electronic pdf to replace it.