

Strategic Insight

Countering the al-Qaeda WMD Threat

by Jack Boureston and Charles Mahaffey

Jack Boureston is Managing Director of [FirstWatch International](#), a private WMD proliferation research group. Charles Mahaffey is a graduate student pursuing a degree in International Policy Studies and Nonproliferation at the Monterey Institute of International Studies. Strategic Insights are published monthly by the Center for Contemporary Conflict (CCC). The CCC is the research arm of the [National Security Affairs Department](#) at the [Naval Postgraduate School](#) in Monterey, California. The views expressed here are those of the authors and do not necessarily represent the views of the Naval Postgraduate School, the Department of Defense, or the U.S. Government.

November 3, 2003

The threat of al-Qaeda's use of weapons of mass destruction is real. During the 1990s, al-Qaeda used its significant financial resources and global support network to pursue the acquisition of nuclear, biological, chemical and radiological weapons. As the terrible events of September 11, 2001 demonstrated, the group is unrestrained by moral proscriptions against devastating, indiscriminate violence against civilians. The attacks on New York and Washington DC also reveal the group's ability to use the infrastructure of the target country as a weapon. Earlier analysis has shown that the critical infrastructure of the United States, including its nuclear and chemical facilities, as well as its shipping and transport networks, contain glaring vulnerabilities, which, if exploited in an al-Qaeda attack, could result in casualties even beyond what the world witnessed on September 11, with or without weapons of mass destruction.^[1]

Countering the Threat: Homeland Security

What is the United States doing to counter al-Qaeda's elusive and amorphous threat of mass destruction? Shortly after 9/11, the United States began seeking ways to protect itself against the terrorist threat. The Department of Homeland Security (DHS) is one result. DHS endeavors to coordinate the activities of previously disparate domestic agencies into one department to protect the nation against threats to the homeland. The DHS has developed its strategy around increasing its internal security, global presence, and international intelligence efforts. The United States has also organized a global coalition to fight terrorism on five fronts: diplomatic, intelligence, law enforcement, financial, and military.

Diplomatic. The United States has built a truly global coalition, developing new counterterrorism partnerships with Russia, China, India, Pakistan, Central Asian republics, and others. The United States also is collaborating to combat terrorism with such nations as Algeria, Bahrain, Egypt, Morocco, Tunisia, and the United Arab Emirates. The extent to which the March 2003 U.S. invasion and occupation of Iraq has impacted these latter relationships, however, remains to be seen.

Intelligence. The United States and its allies have expanded intelligence sharing and cooperation to effectively preempt and combat terrorism all over the world. Intelligence gathered from captured enemy combatants and imprisoned terrorists is being exploited to thwart future activities and expose terrorist safe havens.

Law Enforcement. Law enforcement agencies are taking extra measures to track down and arrest al-Qaeda members. Recently, FBI Director Robert Mueller visited Saudi Arabia, Yemen, Pakistan, and Afghanistan to discuss how to more actively pursue al-Qaeda members. For example, Mueller discussed how the United States and Pakistan could collaborate more closely to capture Taliban and al-Qaeda operatives hiding in the tribal zone along the border of Afghanistan and Pakistan.^[2] International cooperation among law enforcement agencies has resulted in the capture and detention of over 3000 al-

Qaeda operatives in over 100 countries. In Pakistan alone, approximately 500 al-Qaeda suspects were arrested, with 346 of them handed over to the United States. On June 12, French police arrested suspected al-Qaeda leader Christian Ganczarski for his alleged involvement in the 2002 attack on a Tunisian synagogue. Ganczarski, an electronics and telecommunications expert, is thought to have been in contact with Osama bin-Laden and may have been involved in the 9/11 attacks.[\[3\]](#)

The DHS is also attempting to prevent terrorists from using cargo containers to smuggle chemical, biological or nuclear weapons into the United States. It has placed teams of U.S. inspectors at major seaports in Middle Eastern nations and at other smaller, strategically located ports. The inspectors have radiation monitors, chemical detectors, and other equipment to inspect what might be considered "high-risk" containers. This is part of a two-phase program, the first of which began shortly after 9/11 and focused on twenty large container ports in Europe and Asia. Currently, there are over 130 inspectors working overseas and another 170 more are in training to join them. The second phase will see teams placed in Dubai, Malaysia, Turkey, and other nations with large Muslim populations.[\[4\]](#)

Recently, the DHS has opened a new office to deal with potential hand-held missile threats to the aircraft outside of the United States. Acting on intelligence reports, DHS agents have inspected airports in Iraq, Greece, Turkey, and the Philippines. So far the results of these activities have not been published.

Financial. UN Security Council Resolution 1373 obligates nations to freeze the assets of terrorists and to prohibit anyone in the country from providing financial or other material assistance to terrorists or their supporters. So far over 166 countries have issued orders freezing more than \$121 million in terrorist-related financial assets. The 29-nation Financial Action Task Force is establishing legal and regulatory standards and policies to combat money laundering and deny terrorists access to the world financial system.

Military. Most visible to the public is the military action undertaken by U.S. forces in Afghanistan, in Iraq, and in other countries. The United States has waged this war on terrorism using its own military forces and in cooperation with other countries.

Domestically, the DHS has improved U.S. structural integrity by increasing security in the air, at sea, along its borders, and overseas. An example of this is the new DHS-sponsored and administered U.S. VISIT program. VISIT is a new border security and enforcement tool under development to capture point of entry and exit information by visitors to the United States. This system will be capable of using information, coupled with biometric identifiers, such as photographs and fingerprints to create an electronic check-in/check-out system for people who come to the United States to work, study or visit. VISIT will also provide a useful tool to law enforcement to find those visitors who overstay or otherwise violate the terms of their visas. The DHS also sponsors numerous exercises to determine the preparedness of first responders. These exercises provide valuable lessons concerning the vulnerabilities and requirements for preparing authorities for worst-case scenarios.

Lastly, the DHS is working to improve its intelligence capability and enlist experienced analysts to work within its offices. Intelligence is key to DHS and its ability to warn against potential attack. According to DHS's intelligence chief, "Information analysis and infrastructure protection is the center of gravity of this entire department."[\[5\]](#) However, much of the relevant intelligence work occurs outside of DHS. DHS officials have developed an arrangement in which the CIA, the FBI and the new Terrorist Threat Information Center (TTIC) will pass on intelligence reports about possible terrorist threats. Through the Directorate of Information Analysis and Infrastructure Protection (IAIP), the DHS can then identify and assess current and future threats to the homeland, map those threats against U.S. vulnerabilities, issue timely warnings, and take preventive and protective action.

As good as the above process sounds, it may not be enough to predict future terrorist attacks. New and innovative methods must be considered to identify possible terrorist plots and prevent possible attacks. As Dr. Joshua Sinai of ANSER wrote, "Failing to anticipate the attacks of 11 September represented

more than a failure of intelligence—it was a failure of imagination."^[6] Sinai has developed a risk assessment methodology that is based on seven attack warning indicators: previous terrorist attacks, failed attacks or plots not yet executed that serve as blueprints for intentions and future targeting; a terrorist group's modus operandi, particularly tactics; use of particular types of weaponry and devices that a terrorist group perceives will achieve its objectives; the objectives of a group's state sponsor; the location of a group's adversary and the group's logistical capability to reach, conduct surveillance on and attack a target; historical dates of particular significance to terrorist groups; and triggers that propel a group to launch attacks in a revenge mode as quickly as possible as a result of sudden developments such as a severe military setback.^[7]

Conclusions

The events of September 11, 2001 have forced policymakers in the United States to see what others around the world already knew: terrorism is a constant threat and is not going away any time soon. Since 9/11 much has changed for the United States and for the world. A U.S.-built coalition against terrorism has led to numerous arrests of key members of al-Qaeda. Intelligence-sharing has allowed the coalition to thwart several planned attacks. But what we know about terrorism, and in particular about al-Qaeda, is that it is asymmetric. Al-Qaeda is vast in its membership and resources, and can readily adapt to the environment surrounding an intended target. And we know that al-Qaeda has studied methods of developing biological, chemical, nuclear, and radiological weapons. Al-Qaeda remains a real enemy that must be dealt with in the United States and overseas. The enemy is not attempting to attack in the overt conventional fashion to which Americans have grown accustomed. This enemy is subtler, more staggered, and perhaps more strategically calculating. "Al-Qaeda is not only trying to beat the United States," a senior intelligence official said, "it is trying to create a lasting legacy of international insurgencies by supporting conflicts in Philippines, Kashmir, Pakistan, Chechnya, inside Iraq, Malaysia, Indonesia—everywhere on earth where there is an Islamic insurgency." The organization's strong point is not its overall military strength, but its ability to "change its operational system at will in response to the methods needed to approach and attack a new target."^[8]

Another lesson learned after 9/11 is that many components of our critical infrastructure are vulnerable to attack and in desperate need of improvement. Our ports, power supplies, hospitals, and nuclear plants are all vulnerable to some extent to terrorist attack. The Department of Homeland Security was established to coordinate the efforts of federal agencies charged with managing the potential threats coming from land, sea, and air. DHS is primarily focused on protecting assets in the United States; but it also responsible for nullifying enemies abroad that may threaten American interests overseas. DHS is charged with collecting and analyzing information that may lead to terrorist activity, as well as with providing actionable intelligence to state and local authorities to better prepare first responders. DHS analysts would do well to consult with Dr. Sinai's methodology, which offers innovative concepts for assessing potential adversary's activities. Potential targets or events that are not necessarily high value, but have perceived importance to a terrorist's view of the United States also should be considered when performing threat analyses. The nexus between Dr. Sinai's warning indicators and U.S. vulnerabilities may be the point that requires further scrutiny and additional security as protection from future attacks.

No matter how much work goes into making an area more secure, it can never be made invulnerable. The sheer volume of radioactive, biological, and chemical material transported and stored in the United States alone makes it nearly impossible to ensure the security of such shipments at all times. Therefore, timely intelligence to foresee possible attacks must be produced. Greater emphasis must be made on improving intelligence collection and analysis. Some analysts have suggested that improving HUMINT is the key. No doubt, infiltrating a terrorist group would be helpful to obtain a deeper understanding of its intentions. What is required is constant tracking and profiling of terrorist groups. According to Dr. Sinai, "We need to begin thinking like the enemy—always anticipating and preparing to counteract new types of attacks and targeting."^[9] And this can only be done through greater intelligence, analysis, preemption, and protection.

For more topical analysis from the CCC, see our [Strategic Insights](#) section. For related links, see our [Homeland Security](#), [WMD Proliferation](#), [Middle East](#), and [South Asia](#) Resources.

References

1. Jack Boureston and Charles Mahaffey, "[Al-Qaeda and Mass Casualty Terrorism: Assessing the Threat](#)," *Strategic Insight*, October 1, 2003.
2. For background, see Peter R. Lavoy, "Fighting Terrorism and Avoiding War in South Asia: The Indo-Pakistani Situation," *Joint Forces Quarterly*, no. 32 (Autumn 2002): 27-34.
3. "French Say Suspect is Qaeda Big," *CBSNews.com*, June 12, 2003.
4. Phillip Shennon, "U.S. Inspectors To Be Placed At Muslim Ports," *International Herald Tribune*, June 13, 2003.
5. John Mintz, "At Homeland Security, Doubts Arise Over Intelligence," *Washington Post*, July 21, 2003.
- 6, 7. Joshua Sinai, "[How to Forecast and Preempt al-Qaeda's Catastrophic Terrorist Warfare](#)," *The Journal of Homeland Security*, August 2003.
8. Montgomery C. Meigs, "Unorthodox Thought about Asymmetric Warfare," *Parameters*, Summer 2003, pp. 4-18.
9. Sinai, op.cit.