# Obama's National Security Vision

## Confronting Transnational Threats with Global Cooperation

Matthew Levitt, Editor

Policy Focus #107 | October 2010

THE WASHINGTON INSTITUTE *for Near East Policy*

# Obama's National Security Vision

## Confronting Transnational Threats with Global Cooperation

Matthew Levitt, Editor

Policy Focus #107 | October 2010

THE WASHINGTON INSTITUTE *for Near East Policy*

Published in 2010 in the United States of America by the Washington Institute for Near East Policy,
1828 L Street NW, Suite 1050, Washington, DC 20036.

Design by Daniel Kohan, Sensical Design and Communication
Front cover: President Barack Obama addresses a United Nations summit, September 2010. (AP photo/Richard Drew)

# Contents

# Contributors

**Daniel Benjamin** is the State Department's coordinator for counterterrorism. Prior to his appointment, Ambassador Benjamin was a senior fellow in foreign policy studies and director of the Center on the United States and Europe at the Brookings Institution. A former senior fellow in the International Security Program at the Center for Strategic and International Studies, the ambassador has also served on the National Security Council and as director for counterterrorism in the Office of Transnational Threats. He is the coauthor, most recently, of *The Age of Sacred Terror*, a New York Times Notable Book of 2002 and winner of the Arthur Ross Book Award.

**David Cohen** is the assistant treasury secretary for terrorist financing. In this role, he is responsible for formulating and coordinating the Treasury Department's counterterrorism financing and anti-money-laundering efforts. A key member of the Obama administration's national security team, Mr. Cohen focuses on developing strategies to combat the financial support networks behind a wide range of threats, including terrorist groups, organized criminal enterprises, and weapons-of-mass-destruction proliferation.

**David T. Johnson** is the assistant secretary of state for the Bureau of International Narcotics and Law Enforcement Affairs. In this position, Ambassador Johnson advises the president, secretary of state, related State Department bureaus, and other relevant government agencies on international narcotics and crime. In addition, he has served as deputy chief of mission for the U.S. embassy in London and as U.S. ambassador to the Organization for Security and Cooperation in Europe.

**Matthew Levitt**, director of The Washington Institute's Stein Program on Counterterrorism and Intelligence, is a former U.S. deputy assistant treasury secretary for intelligence and analysis (2005–2007); in this capacity he coordinated efforts to protect the U.S. financial system from abuse by terrorists, weapons proliferators, and other rogue actors. He writes and comments frequently on Iranian proliferation of weapons to terrorists and on the effectiveness of sanctions to halt Iran's nuclear program. Previously, Dr. Levitt provided tactical

and strategic analytical support for counterterrorism operations at the FBI, including the ongoing terrorist threat surrounding the September 11 attacks. Serving as an expert witness for the Justice Department in many terrorism cases, he is a professorial lecturer in international relations and strategic studies at Johns Hopkins University's SAIS. Dr. Levitt is the coauthor, most recently, of the 2010 Strategic Report *Fighting the Ideological Battle: The Missing Link in U.S. Strategy to Counter Violent Extremism*.

**John T. Morton** is the assistant secretary of the Department of Homeland Security (DHS) and director of U.S. Immigration and Customs Enforcement. In this role he leads the principal investigative component of DHS and the second largest investigative agency in the federal government. Mr. Morton has held a variety of positions within the Department of Justice, including as a trial attorney and special assistant to the general counsel in the former Immigration and Naturalization Service, and as counsel to the deputy attorney general.

**Steven Pelak** is the Justice Department's first national coordinator for export enforcement, a position he has held since October 2007. In this capacity, and as deputy chief of the department's Counterespionage Section, he supervises investigations and prosecutions of export-control and embargo violations across the United States, along with espionage and other national security cases. Previously, he served for more than eighteen years as an assistant U.S. attorney in the District of Columbia.

**Todd M. Rosenblum** is deputy undersecretary with the Department of Homeland Security's Office of Intelligence and Analysis. He has served on the national security cluster for the Obama presidential transition team, the Senate Intelligence Committee, and the Office of Near Eastern Affairs in the CIA's Directorate of Intelligence. Mr. Rosenblum has also held various management and advisory positions at the State Department and the U.S. Arms Control and Disarmament Agency.

# Acknowledgments

MANY THANKS to the leadership and staff of The Washington Institute for Near East Policy for helping to make both this publication, and the lecture series on which it is based, possible. Institute executive director Dr. Robert Satloff and deputy director for research Dr Patrick Clawson are unflagging in their support of the Stein Program on Counterterrorism and Intelligence in general, and this series in particular.

Neither the lecture series nor this edited volume would have been possible without the assistance of the Institute's communications, administrative, and research staff. Special thanks go to our managing editor Mary Kalbach Horan and to the Stein Program's able research assistants and interns, present and former, Ben Freedman, Stephanie Papa, Sam Cutler, David Bagby, and Jordan Gerstler-Holton. And to Michael Jacobson, who was a senior fellow in the Stein Program from the inception of this speaker series through much of this last set of lectures and who has since returned to U.S. government service, heartfelt thanks for helping to get this extremely successful speaker series up and running.

Finally, I want to extend my sincere thanks and appreciation to the many generous donors to the Stein Program: you make all our work possible.

Matthew Levitt
*October 2010*

# Introduction

*Matthew Levitt*

In January 2010, The Washington Institute's Stein Program on Counterterrorism and Intelligence began the fourth series of its highly regarded lectures on counterterrorism.

As of this writing, the Stein Program has hosted twenty-seven officials from the White House, the Departments of Defense, State, Justice, and Homeland Security, federal and local law enforcement, the U.S. military and intelligence communities, and elsewhere.

This volume, the fourth compilation of these lectures,[1] tracks the development of counterterrorism and counterproliferation policy in the Obama administration's first year, during which it debated, developed, and rolled out its new National Security Strategy (NSS). Indeed, one week after the NSS's May 2010 release, a senior administration official stood at the Institute's podium explaining the new strategy in the context of America's current threat environment.

Together, these lectures provide much-needed insight regarding the Obama administration's approach to national security, with particular emphasis on combating terrorism, proliferation, and threats to homeland security. This volume features presentations by six senior officials responsible for leading that fight:

- John T. Morton, assistant secretary of homeland security and director of Immigration and Customs Enforcement
- Todd M. Rosenblum, deputy undersecretary of homeland security
- Daniel Benjamin, the State Department's counterterrorism coordinator
- David Cohen, assistant secretary of the Treasury
- Steven Pelak, national coordinator for export enforcement at the Justice Department
- David T. Johnson, assistant secretary of state for international narcotics and law enforcement affairs

■ *Matthew Levitt, director, Stein Program on Counterterrorism and Intelligence, The Washington Institute*

1. The first three volumes include *Terrorist Threat and U.S. Response: A Changing Landscape* (Policy Focus no. 89, September 2008); *Countering Transnational Threats: Terrorism, Narco-Trafficking, and WMD Proliferation* (Policy Focus no. 92, February 2009); and *Continuity and Change: Reshaping the Fight against Terrorism* (Policy Focus no. 103, April 2010).

## Obama's National Security Strategy

The 2010 NSS laid out the administration's strategic vision for U.S. security, one that draws from all elements of national power to secure American interests, including a multilateral approach aimed at engaging foreign partners. According to that document, America's global leadership will be used to pursue a long list of U.S. interests, at the top of which are countering terrorism and defending the homeland: "We will disrupt, dismantle, and defeat al-Qaeda and its affiliates through a comprehensive strategy that denies them safe haven, strengthens frontline partners, secures our homeland, pursues justice through durable legal approaches, and counters a bankrupt agenda of extremism and murder with an agenda of hope and opportunity."[2]

The 2010 NSS was also the first to integrate homeland and national security intelligence. Todd Rosenblum addressed the challenges raised by this approach, noting that "the emergent field of homeland security" and the task of "providing it with intelligence support" represent a complex undertaking that "differs significantly from foreign intelligence, law enforcement, and traditional national security." Whereas national security is the federal government's responsibility, homeland security requires tremendous coordination among federal, state, and local governments as well as the private sector, with each serving as an equal partner. For example, to improve integration between homeland and national security agencies, agents from the Immigration and Customs Enforcement's Homeland Security Investigations branch are now stationed in every state and in forty-four other countries.

The 2010 National Security Strategy was the first to integrate homeland and national security intelligence.

In this environment, effective and timely information sharing along the local-state-federal pipeline is especially critical. Local and state authorities are best situated to recognize suspicious activity in their communities, while federal authorities are ideally equipped to place that information into the larger context of lessons learned through foreign diplomatic engagement and intelligence collection related to terrorist groups' intentions and capabilities. Contending with other high-priority threats, such as disrupting Iran's illicit procurement efforts, also requires close interagency cooperation. For example, Steven Pelak noted that sharing information and resources helps create reciprocal relationships that facilitate prosecutions of procurement networks.

But as Daniel Benjamin pointed out, today's security challenges demand not only continual improvements in our own intelligence and homeland security apparatus, but also collaboration in a variety of multilateral forums. Similarly, David Johnson highlighted the need for "dynamic threat mitigation" via cooperation with international partners in order to address transnational threats. By working with the United Nations, G-8, European Union, Interpol, Financial Action Task Force, and other international and regional bodies, Washington and its allies are "fighting networks with networks." David Cohen's address focused on the Treasury Department's significant achievements in working through "key international mechanisms" as a means of "coordinating global efforts against terrorist financiers and facilitators." "We say it often," he emphasized,

2. U.S. National Security Strategy 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

"but it bears repeating: our national security interests are best advanced when a broad coalition of nations works together to fight against those who engage in terrorist activity."

## The Evolving Threat

Since the Stein Program's lecture series began, speakers have taken the opportunity to comment on the current state of an ever-evolving terrorist threat. The latest lectures reflected a growing consensus that although al-Qaeda faces significant pressure, both it and its affiliates remain willing and able to carry out attacks. What remains to be seen is whether the dispersion of the global jihadist threat from the heart of the Middle East to South Asia and Africa foreshadows organizational decline or revival for al-Qaeda itself and the radical ideology it espouses. How governments and civil society organize to contend with the changing threat will be central to determining the outcome.

The latest lectures reflected a growing consensus that although al-Qaeda faces significant pressure, both it and its affiliates remain willing and able to carry out attacks.

In the meantime, improved offensive counterterrorism efforts have taken the fight to al-Qaeda along the Afghan-Pakistan border, reduced its ability to carry out spectacular attacks in the West, and limited affiliates' capabilities as well. According to Benjamin, senior U.S. intelligence figures have noted that al-Qaeda remains "under pressure in Pakistan," where it has suffered "a number of leadership losses" and is finding it more difficult to operate and plan attacks. Indeed, counterterrorism officials are far more skilled at collecting intelligence on the group than they were eight years ago, and both human sources and technical coverage have improved dramatically.

Fewer terrorist masterminds mean less-capable operatives attempting simpler and smaller—but likely more frequent—attacks. Speaking in June 2010, Rosenblum pointed out that "the number and pace of attempted attacks against the United States over the past nine months have surpassed the number of attempts during any other previous one-year period." Such attempts, he warned, are likely to increase.

In short, the terrorist threat has not diminished so much as it has expanded to include attacks by less-coordinated, more-dispersed franchises and homegrown terrorists. Although the speakers acknowledged that the al-Qaeda core remains "a highly capable, highly innovative, and very determined group," they also pointed to a "more widely distributed and more geographically and ethnically diversified" threat from affiliates "and those inspired by the al-Qaeda message." For example, citing the case of Umar Farouq Abdulmutallab, the Nigerian suicide bomber dispatched by al-Qaeda in the Arabian Peninsula (AQAP) to attack a U.S. airliner, Benjamin warned, "We have every expectation that we will hear more from AQAP."

At the same time, one of the greatest concerns facing U.S. counterterrorism officials is the growing number of radicalized U.S. citizens and residents, some of whom have traveled abroad to join the global jihad. Consider the Somali Americans who have fought with the Somali terrorist group al-Shabab, as well as other Americans who have traveled to Pakistan and Afghanistan for similar purposes. And some individuals have derived inspiration, direction, or training from abroad to plan attacks at home, such as Fort Hood shooter Nidal Malik

Hasan, Times Square plotter Faisal Shahzad, and Najibullah Zazi, who planned to bomb the New York subway system. Several Americans have also risen to prominence as al-Qaeda leaders, such as Adam Gadahn, a spokesman for the group's core leadership, and regional boosters Omar Hammami (Somalia) and Anwar al-Awlaki (Yemen). According to U.S. officials, al-Awlaki has "moved up the terrorist supply chain" by virtue of his success as a talent scout and radical ideologue.[3]

Meanwhile, Iran's illicit procurements present still another pressing threat to U.S. interests and global security. As John Morton highlighted, the regime is aggressively seeking nuclear capabilities that would drastically change the balance of power in the Middle East. Despite being conducted by a network of international brokers, these efforts are very much directed by Tehran. Fortunately, they have been significantly impaired by aggressive targeted actions—part of a sustained and calculated campaign by the United States and the international community to enforce export controls. "The threat of Iran's procurement networks is clear," Pelak noted, pointing out that a "foreign agent can acquire weapons parts from a U.S. company, illegally transport them overseas through a third country to Iran, and pass them on to an operative in Iraq, who can then use them to create an improvised explosive device that kills American soldiers." As Morton concluded after cataloguing the administration's strong domestic and international collaboration, "[T]he magnitude and scope of the threats facing our country have never been greater than today."

Indeed, terrorist groups adapt and evolve partly in response to the countermeasures taken against them.

## Combating Transnational Threat Financing

Likewise, the financial underpinnings of terrorist activity are far from static. As Cohen asserted, al-Qaeda may now be "in the worst financial shape it has been in for years," but the group "is not disabled, nor is it bankrupt, and our progress in degrading its financial strength will not be lasting without continued, vigorous efforts." And unlike al-Qaeda, he reported, "the Taliban is not experiencing much financial stress."

Indeed, terrorist groups adapt and evolve partly in response to the countermeasures taken against them. As the threat has shifted, the means by which terrorist groups raise, store, and move funds have also changed, often hindering government efforts to thwart terrorist activities. Studies show that such groups learn from one another, exchange information on new technologies, and share innovations. This adaptability is particularly evident today as more terrorist groups turn to crime for both monetary and popular gains. "Reacting to the financial state of [the] al-Qaeda core," Cohen pointed out, "al-Qaeda affiliates in Africa and the Arabian Peninsula have come to rely less on support from the al-Qaeda network as they plan and mount terrorist attacks. These al-Qaeda affiliates instead have taken up independent fundraising activities to sustain themselves—including drug trafficking, kidnapping for ransom, and extortion."

3. "Officials: 'Credible Intelligence' on Terror Attack Planning against U.S.," FoxNews.com, January 14, 2010, http://www.foxnews.com/politics/2010/01/14/officials-credible-intelligence-collected-terror-attack-planning.

It may seem hypocritical for supposedly religious terrorists to pursue criminal activity—in fact, many of these groups acknowledge the contradiction and attempt to justify their actions. Johnson noted the case of a convicted Taliban member who cited the overarching goal of turning "all the infidels into corpses," whether "by opium or by shooting."

Although this trend is certainly a dangerous one from the U.S. perspective, it also presents opportunities for policymakers. As the nexus of terrorism and crime grows busier, targeting terrorists' criminal activities will become an increasingly effective strategy. Terrorist networks are more transnational than ever, and a key challenge in confronting them is to increase international cooperation. By taking action against criminal and terrorist groups as they converge, governments can use existing strategies of international cooperation and diplomatic engagement on both fronts to gain broader support for their efforts.

This convergence is likely to increase even more in the coming years, given terrorists' marked turn to drug trafficking. As former U.S. Drug Enforcement Administration operations chief Michael Braun explained in a July 2008 Washington Institute speech, terrorist organizations and drug cartels "often rely on the same money launderers" and shadow networks.[4] Targeting the full range of launderers, traffickers, document forgers, and other criminals could prove instrumental in combating today's terrorist threat.

Meanwhile, Iran remains the world's most prominent state sponsor of terrorism and is aggressively seeking to procure sensitive technologies for its military and nuclear programs. Mirroring the Iranian banking sector's deceptive financial practices, various procurement agents, businesses, and transporters in Iran have developed a network of front companies and willing partners aimed at acquiring controlled military and dual-use technologies. Many of these items come from the United States. According to Morton, in fiscal year 2009, his agency initiated 1,313 criminal investigations of possible illegal exports, the majority focusing on the flow of key U.S. technology to Iran. But the Islamic Republic's procurement efforts go well beyond the United States. Consider the 2009 annual report of the Czech Security Information Service, which found that Iran had used front companies in the Czech Republic to obtain items that could facilitate the production of weapons of mass destruction.[5]

In sum, the threat posed by adversary networks—whether terrorists or proliferators—greatly depends on their ability to raise funds. As Cohen warned, our success against such networks is largely contingent "on the extent to which we are able to engage our international partners in a cooperative effort" against their finances.

The threat posed by adversary networks—whether terrorists or proliferators—greatly depends on their ability to raise funds.

## Countering Violent Extremism

According to Benjamin, one area demanding greater innovation is Washington's effort to address "the political, economic, and social factors that terrorist

4. See Michael Braun, "Drug Trafficking and Middle Eastern Terrorist Groups: A Growing Nexus?" PolicyWatch no. 1392 (The Washington Institute for Near East Policy, July 25, 2008), http://www.washingtoninstitute.org/templateC05.php?CID=2914.
5. The report is available online at http://www.bis.cz/ar2009en.pdf.

organizations exploit," as well as "the ideology that is their key instrument in pushing vulnerable individuals down the path toward violence." Confronting this ideology has proven an uncomfortable task for the administration thus far.

The 2010 National Security Strategy accurately described Afghanistan and Pakistan as "the frontline" of a war "against a far-reaching network of hatred and violence." But it did not specifically address threats from other terrorist groups employing violence in support of similarly hateful ideology. Indeed, much of the discussion that followed Rosenblum's lecture focused on the administration's contention that America should not describe such enemies as "jihadists" or "Islamists." To be sure, we must be careful not to employ language that could be interpreted as an attack on Islam as a religion. But if the administration fails to clearly articulate the threat posed by the ideology of Islamist extremism, its broader whole-of-government efforts will lack strategic focus and overlook the varied root causes of domestic and foreign radicalization. Voicing this threat without denigrating the Islamic religion in any way is an achievable goal.

For all the tactical counterterrorism successes documented in these lectures, strategic counterterrorism success remains elusive.

Indeed, for all the tactical counterterrorism successes documented in these lectures, strategic counterterrorism success remains elusive. Despite losing safe havens and facing financial difficulties, al-Qaeda, its affiliates, and its followers remain capable of recruiting foot soldiers and executing attacks. Yet specific policies and programs aimed squarely at countering the radical narrative remain few and far between, even amid a sharp increase in terrorist plots and homegrown radicalization cases. It is axiomatic that the United States cannot simply capture and kill its way out of the problem; it must find a way to take on the extremist ideology directly. "Quite simply," Benjamin concluded, "we need to do a better job to reduce the recruitment of terrorists."

## Conclusion

As the speakers in the Stein Program lecture series and other senior U.S. national security officials continue to work tirelessly to protect Americans and American interests from very real threats, the administration's new National Security Strategy will serve as their guide. Its focus on international cooperation and interagency information sharing bodes well for continued counterterrorism and counterproliferation success, especially in the tactical areas in which the government tends to excel. What remains to be seen is whether the administration's strategic vision will translate into strategic success. Given the emergence of several critical threats—including Iran's nuclear program and terrorist groups that have been able to recruit operatives both at home and abroad—the challenge is considerable. The NSS's goal of reshaping the current strategic environment is formidable, but as these lectures and those in preceding volumes make clear, American leadership remains up to the task. Timely analysis and creative ideas are critical as U.S. officials strive to keep up with our adversaries' ever-changing tactics. Toward that end, the insights in the presentations that follow are especially welcome.

# Combating Export Violations to Iran: The Role of ICE Homeland Security Investigations

*John T. Morton*

September 2, 2010
Prepared Remarks

Good afternoon. I am honored to be here to talk to you today about the role of ICE Homeland Security Investigations (HSI) in the U.S. government's counterterrorism and counterproliferation efforts.

This topic is especially poignant, as next week marks the ninth anniversary of the 9/11 attacks on the United States. Back then, I was serving as an assistant U.S. attorney in the Eastern District of Virginia, first in the Major Crimes Unit and later in the Terrorism and National Security Unit. In fact, one of the cases I prosecuted was the case against a man who helped two of the 9/11 hijackers fraudulently obtain Virginia identification cards. As I look back, it is hard to believe nearly a decade has passed since that terrible day—a day we lost so many lives in the World Trade Center, the Pentagon, and on United Airlines Flight 93.

That day also changed the landscape of the U.S. government. One of the most far-reaching steps taken to protect America was the creation of the Department of Homeland Security. DHS, which began operations in early 2003, took twenty-two different federal agencies and brought all or parts of them under one organization. This was the largest reorganization of the federal government since 1947, when the Department of Defense was created.

One of the new agencies created in DHS was the agency I have the honor to lead. ICE brought together resources and personnel from the U.S. Customs Service and the Immigration and Naturalization Service, along with the Federal Protective Service, so it could carry out its mission of enforcing more than four hundred individual immigration and customs statues.

■ *John T. Morton, assistant secretary of Homeland Security for U.S. Immigration and Customs Enforcement (ICE)*

## What Is ICE HSI?

Today, ICE is the principal criminal investigative arm of the Department of Homeland Security and one of the three department components charged with the civil enforcement of the nation's immigration laws. But ICE is not just an immigration-focused agency.

HSI agents are stationed in every state of the union and forty-four countries overseas. We investigate a wide array of federal crimes: child pornography and sex tourism; gang violence; document fraud; border smuggling of all kinds—including drugs, money, people, and guns; counterfeit goods; intellectual property theft; and international art theft. HSI is the only federal law-enforcement

entity with full statutory authority to investigate and enforce criminal violations of all U.S. export laws related to military items, controlled dual-use commodities, and sanctioned or embargoed countries.

## Export Enforcement Authorities

Our mission to combat terrorism is multifaceted:

- to prevent terrorists from reaching or remaining in the United States
- to disrupt terrorist plots and bring to justice those who attempt to do harm
- to protect the American public from the introduction of weapons of mass destruction (WMD) and other instruments of terror into the United States
- to prevent illegal exporters, targeted foreign countries, terrorist groups, and international crime organizations from trafficking in WMD and their components; obtaining and illegally exporting licensable commodities, technologies, conventional munitions, and firearms; or engaging in financial transactions that support these activities or violate U.S. sanctions or embargoes

These tasks are, I believe, among the most critical aspects of HSI's role as part of the Department of Homeland Security. Through its Visa Security Program, ICE seeks to ensure that those who receive permission to come to the United States are not bent on doing harm. In enforcing the nation's immigration laws, ICE targets individuals who violate those laws and pose national security threats through its terrorist removal and visa overstay programs.

Our technology is a critical asset to U.S. national security and could be an instrument of intimidation or destruction in the wrong hands.

The other critical component of ICE's national security and antiterrorism efforts is the leadership role the agency has traditionally played in the realm of export controls. Bottom line: enforcing export control laws keeps military products and sensitive technology out of the hands of terrorist groups and hostile nations.

Combined with the investigative efforts of our predecessor, the U.S. Customs Service, we have led law enforcement efforts in export enforcement for approximately thirty-five years. In fact, our export authorities are the broadest within the U.S. government.

It is not difficult to understand why export enforcement is so important. Our technology is a critical asset to U.S. national security and could be an instrument of intimidation or destruction in the wrong hands. America produces some of the most advanced technology in the world, and as such has become a primary target of other countries, criminal groups, and terrorist organizations seeking to advance their own technological capabilities. Anyone—in the private sector or military—who is involved in any aspect of high-technology research, development, production, or sales is a potential acquisition target. Even a seemingly insignificant product could easily be the necessary component of a major technological development or dangerous weapon for those who seek to do us harm.

The People's Republic of China operates a robust North American procurement program obtaining military technology and equipment that not only supports the People's Liberation Army but is also provided to prohibited countries around the world.

Iran, as we all know, is aggressively seeking nuclear capabilities that would forever change the balance of power in the Middle East. We now see an alarming response by Iran's neighbors, who now feel compelled to develop nuclear capabilities themselves.

Nuclear weapons are not the only threat; small arms and light weapons and other conventional weapons move illegally from Western industrialized countries to areas of civil unrest, resulting in hundreds of thousands of innocent civilian deaths in countries least able to protect their borders and citizens.

Over the years, illicitly acquired U.S. munitions and technology have assisted our adversaries in jeopardizing our soldiers, our citizens, and our interests. They have also harmed our allies. Today, nearly nine years after the 9/11 attacks, nuclear, chemical, and biological weapons and their components are more widely available to terrorists and rogue nations than ever before. Despite treaties and sanctions, countries like Iran continue to work around the system in an effort to obtain restricted technology. That is why export enforcement is more important than ever.

## How HSI Fulfills This Mission

This [export enforcement] is an area of enormous sensitivity and importance to protecting our national security, and HSI has a number of mechanisms in place to carry out our mission to combat terrorism. One way is through our Counter-Proliferation Investigations Unit. This team is responsible for overseeing a broad range of investigative activities. The Counter-Proliferation Investigations Unit's priority programs address trafficking in WMD components and materials, sensitive dual-use commodities, and technologies sought by rogue nations and terrorist groups. Our programs address illegal exports of military equipment and spare parts to embargoed countries, significant financial and business transactions with proscribed countries and groups, and export enforcement training for private industry as well as state, local, and foreign agencies.

Another way HSI carries out this mission is through initiatives such as Project Shield America, which began in 2001 under the U.S. Customs Service. Through this program, HSI special agents reach out to U.S. manufacturers and exporters of arms and sensitive technology to educate them about export laws and to solicit their assistance in preventing illegal foreign acquisition of their products.

Let us be clear, though: Project Shield America is not intended to restrict or discourage legitimate U.S. exports. According to statistics released in July by the International Trade Administration, the United States exported $739.5 billion in goods and services during the first five months of 2010. Obviously, exports are a vital part of our economy and we certainly do not want to stifle that in any way. But we are charged with protecting the technical accomplishments resulting from American ingenuity and labor, and preventing our adversaries from achieving technological parity or gaining a military advantage through illegal acquisition of U.S. technology. That is a task we take very seriously. We must weigh the benefits of trade against the need for enforcement, and we have worked hard to strike the proper balance.

We must weigh the benefits of trade against the need for enforcement, and we have worked hard to strike the proper balance.

Project Shield America works in concert with the three-pronged approach of HSI's Export Enforcement Program: inspection and interdiction; investigations; and international cooperation.

The first aspect, inspection and interdiction, utilizes specially trained U.S. Customs and Border Protection field officers stationed at high-threat ports to selectively inspect suspicious export shipments. The investigations phase involves HSI special agents deployed throughout the country who pursue the arrest and eventual prosecution of offenders of the Export Administration Regulations; the Arms Export Control Act and the International Traffic in Arms Regulations; the Trading with the Enemy Act; the International Emergency Economic Powers Act; and other relevant statutes. Our focus is on working *proactively* to detect and disrupt illegal exports before they can cause damage to the national security interests of the United States. Finally, our attaché offices around the globe enlist the cooperation of their host nations in an effort to initiate new investigative leads and to develop information in support of ongoing investigations.

And then there is the National Export Enforcement Coordination Network (NEECN), established in 2007 by the Counter-Proliferation Investigations Unit to coordinate efforts by numerous agencies within the law-enforcement and intelligence communities to prevent foreign adversaries and illicit procurement networks from illegally obtaining U.S. munitions and critical dual-use technology. The NEECN fulfills this mission by:

Inspection and interdiction utilize specially trained U.S. Customs and Border Protection field officers stationed at high-threat ports to selectively inspect suspicious export shipments.

- deconflicting law-enforcement efforts
- supporting criminal investigations in the field
- coordinating with export-licensing agencies and commodity and technology experts
- coordinating with the intelligence community to identify proliferation trends and identify ways to neutralize those threats
- disseminating investigative leads to field offices for action

These combined efforts are supported by the Exodus Command Center, located in Washington, D.C. This facility is the principal administrative and operational center that coordinates with external export regulatory agencies to seek clarification or rulings in support of export enforcement investigations.

## A Record of Success

Since it was formed under the U.S. Customs Service, our Export Enforcement Program has been responsible for major seizures of controlled technology, including laser guidance devices, military equipment, sophisticated computer systems, and other items critical to allied defense and U.S. industry. These seizures have also included high-technology items designed primarily for civilian use but that are still subject to export controls to certain destinations because of their potential military application. Recognizing this success, other countries

have initiated their own export control programs, often through training provided by ICE personnel.

In November 2009, the president initiated an export control reform process that established an interagency task force under the National Security Council and the National Economic Council. As part of this reform process, National Security Council principals charged ICE HSI with creating and leading a national export enforcement fusion center in order to synchronize U.S. government efforts. This responsibility was given to ICE because of its long history and statutory authority in leading this important national security mission.

Over the last year, HSI has been the lead investigative agency for approximately 75 percent of the significant export prosecutions identified by the U.S. Department of Justice. In fiscal year 2009, HSI initiated 1,313 criminal investigations of possible illegal exports; made 708 criminal arrests, 218 of which were for sensitive commodities and technologies; secured 194 indictments; and obtained 190 convictions. A majority of these national security cases have been focused on stemming the flow of sensitive U.S. technology to Iran.

Over the last year, HSI has been the lead investigative agency for approximately 75 percent of the significant export prosecutions identified by the U.S. Department of Justice.

For success like this to continue, we depend on the cooperation of the export community. HSI recommends that our industry partners implement an export management system consisting of several elements that will facilitate export control—including a *strict* policy of reporting suspicious orders or inquiries to ICE.

## Noteworthy Cases

For obvious reasons, much of what we do in this area we cannot discuss publicly, but I would like to tell you a bit about some of our latest notable cases.

**Amir Ardebili—Iran.** Beginning in 2002, Iranian citizen Amir Ardebili functioned as an intermediary for the Iran Electronics Institute, which directly supplied Iran's military and served as a mechanism for Iran to illegally acquire sensitive U.S. technology and munitions. He was involved in the acquisition of a wide range of components, including military-aircraft parts, night-vision devices, and communications equipment. Specifically, he sought items that he believed would be used in an Iranian air-defense phased-array radar system and in advanced military avionics. Ardebili acquired thousands of components for the government of Iran—approximately $1 million worth of components each year. He told our undercover agents these technologies were to be utilized to enhance Iranian military capabilities in the event of conflict with the United States.

During a meeting with an undercover agent, Ardebili accepted delivery of a thousand microchip phase shifters and two quartz rate-sensor gyro-chips. During other meetings, he outlined the Iranian military defense procurement system and described the money-laundering techniques used to shield the identity of Iranian funds in internatinal transactions.

He established front companies in the United Arab Emirates and used European bank accounts to further his technology-acquisition efforts. On October 2, 2007, he was arrested in the Republic of Georgia after negotiating with undercover agents to acquire and export phase-shifter microchips and a digital air-data recorder to Iran. It should also be noted that the phase-shifter microchips

are used in phased-array radar and the digital air-data recorder is a computer that is fitted specifically for F-4 military aircraft.

On May 19, 2008, Ardebili pleaded guilty to fourteen counts related to violations of U.S. export control laws. On December 14, 2009, he was sentenced to sixty months in prison.

**Mahmoud Yadegari—Iran.** On July 29, 2010, Mahmoud Yadegari was sentenced in the Ontario Court of Justice in Canada to twenty months in jail after being convicted of violating the United Nations Act and Canadian criminal laws. This was in addition to fifteen and a half months he served in presentencing custody. The arrest, execution of multiple search warrants, and conviction were the direct result of a joint investigation initiated by our Special Agent in Charge (SAC) office in Boston along with the U.S. Department of Commerce, ICE assistant attaché–Toronto, the Royal Canadian Mounted Police (RCMP) Customs and Excise Section, and the Canada Border Services Agency. The investigation centered on the illegal transshipment of U.S.-origin, dual-use nuclear technology to Iran.

In February 2009, along with Department of Commerce agents, we conducted an industry outreach visit to Pfeiffer Vacuum Inc. in Nashua, New Hampshire. While there, details of a suspicious order emerged regarding the sale of twenty pressure transducers to a new customer, Mahmoud Yadegari of N&N Express Inc. in Ontario. Through coordination with ICE assistant attaché–Toronto, the Royal Canadian Mounted Police and Canada Border Services Agency initiated a joint investigation into Yadegari and his company.

The arrest... and conviction of Mahmound Yadegari were the direct result of a joint investigation initiated by our Special Agent in Charge office in Boston.

The Canada Border Services Agency detained a shipment made by Yadegari that was destined for the United Arab Emirates. It contained two pressure transducers; subsequent investigation revealed that they were manufactured by Setra Systems in Boxborough, Massachusetts. They were controlled for export by the Department of Commerce for reasons of nuclear nonproliferation. These items were also controlled for export under Canadian law.

During March and April 2009, our agents in Boston assisted the Royal Canadian Mounted Police with the execution of search warrants in Canada that were associated with Yadegari's email accounts, financial records, telephone accounts, and residence. The RCMP seized eight additional Setra Systems pressure transducers from his home; additional evidence revealed that all the items were destined for Iran. He was arrested on April 16, 2009, and charged in Canada with violating the United Nations Act, the Customs Act, and the Export and Import Permits Act.

**Chi Tong Kuok—China.** In December 2006, an individual later identified as Chi Tong Kuok contacted a British representative of the U.S.-based company ViaSat. The case was referred to our SAC office in San Diego, and undercover communications with Kuok began shortly thereafter. Initially, Kuok presented an extensive list of high-tech communications devices he was seeking. The items on the list were collectively worth millions. The list consisted almost entirely of communications devices that utilized National Security Agency (NSA)–developed encryption, including the AN/CYZ-10—a "fill" device used to store, transfer, or receive encrypted data. Over the course of the investigation, Kuok finally agreed to meet an undercover agent in Panama to purchase two AN/

PRC-148 handheld radios and a Defense Advanced GPS Receiver. Both items use NSA encryption, and are heavily used by the U.S. military.

Kuok was arrested in Atlanta on June 27, 2009, en route to Panama. When he was interviewed, Kuok admitted he was attempting to obtain all of the devices for the Chinese government. Kuok is scheduled to be sentenced on September 13.

**Jacques Monsieur, "The Field Marshal"—Iran.** In January 2009, a confidential informant contacted our Assistant SAC office in Mobile, Alabama, regarding a man identified as Jacques Monsieur, otherwise known as " The Field Marshal." The informant indicated that Monsieur was known throughout the world as an illegal "gray market" arms dealer, as well as a procurer of military-related items for embargoed countries. The informant advised agents that Monsieur was seeking parts and engines for the F-5 fighter jet employed by Iran. The informant subsequently offered Monsieur information about contacts in the United States who could potentially acquire these items. In February 2009, Monsieur made initial contact with an undercover agent in an attempt to purchase F-5 fighter-jet engines and parts, which were ultimately intended for illegal export from the United States to Iran.

In May 2009, an undercover agent met with Monsieur in London, where Monsieur introduced business associate Dara Fatouhi. Together they discussed the illegal acquisition and export of F-5 fighter-jet engines and parts. Monsieur and Fatouhi asked the undercover agent if they could obtain U.S. shipping or export-authorization documents that falsely indicated the end-user of the items would be located in Colombia rather than Iran.

In June 2009, Monsieur sent the undercover agent a purchase order from a front company located in Kyrgyzstan. He later wired approximately $110,000 from Dubai to a bank account located in Alabama as payment for the parts and subsequent transshipment.

On August 28, 2009, our agents arrested Monsieur upon his arrival in New York City based on an arrest warrant issued in the U.S. District Court in the Southern District of Alabama. On November 23, 2009, he entered a guilty plea for conspiracy to export merchandise from the United States. A sentencing date has yet to be determined. His associate, Fatouhi, is still at large and an Interpol Red Notice has been issued for his arrest.

## Conclusion

These are just a few examples of the work we have been doing, together with our law-enforcement partners and prosecutors. As you can see, in each of these instances the blatant disregard for the law had potentially grave national security implications. Time after time, our export-enforcement investigations have helped prevent the illegal acquisition of resources and helped maintain military, political, and economic stability throughout the world. We will not allow U.S. national security to be held hostage by rogue nations or sold to the highest bidder. HSI is committed to working closely with our partners at every level of law enforcement to ensure this does not happen. While we have had success for many years as the nation's leading law-enforcement agency investigating violations of export-control laws, the magnitude and scope of the threats facing our country have never been greater than today.

Time after time, our export enforcement investigations have helped prevent the illegal acquisition of resources and helped maintain military, political, and economic stability throughout the world.

# Defining Homeland Security Intelligence

*Todd M. Rosenblum*

June 4, 2010
Prepared Remarks

■ *Todd M. Rosenblum, deputy undersecretary of Homeland Security*

Good afternoon and thank you.

Ever since the early 1990s, when I would come here from the State Department to hear from some of the nation's, and indeed the world's, leading experts on national security and the Middle East, I have been a great fan of the Institute. So, it is with great pleasure, and a significant amount of humility, that I appear before you today.

As someone who has been working for more than twenty years in the fields of national security, intelligence, and politics, I can say with certainty that I did not think my first appearance before this distinguished audience would be for the purpose of discussing homeland security. There are logical synergies and ties between the fields of homeland and traditional national security, but the tools for success in one are not necessarily the same tools for success in the other. Put another way, how we provide physical protection of the homeland and how we promote and defend our interests overseas are not the same.

My hope this afternoon is to give you a sense of what has come to be known as the field of homeland security. I will provide you with some thoughts on the changing threat environment, the great strides we are making in building a true homeland security enterprise, as well as on the challenges associated with meeting the homeland security intelligence needs of this new enterprise.

Most fundamentally, I will make the case that the emergent field of homeland security, and providing it with intelligence support, is both complex and differs significantly from foreign intelligence, law enforcement, and traditional national security. Success in each domain is reliant on success in the others, even as the actors, lexicon, and operating environment ... are often distinct.

## The New National Security Strategy

As you know, President Obama released his first National Security Strategy framework last week. It is premised on the fact that national security and homeland security are integrated, and that our government has no greater priority than the safety and security of the American people. This is the primary mission of the Department of Homeland Security. It is the primary mission of the DHS Office of Intelligence and Analysis (I&A), in which I am honored to serve.

The president makes clear that success relies on our facing the world as it is, that great advances have been made, but that those advances have been accompanied by persistent problems. Our country will continue to underwrite global security, and we will do so through our commitments to allies, partners, and institutions. The president's new National Security Strategy speaks in no uncertain terms to the new way ahead:

> We will disrupt, dismantle, and defeat al-Qaeda and its affiliates through a comprehensive strategy that denies them safe haven, strengthens frontline partners, secures our homeland, pursues justice through durable legal approaches, and counters a bankrupt agenda of extremism and murder with an agenda of hope and opportunity. (page 4) . . . Our intelligence and homeland security efforts must be integrated with our national security policies, and those of our allies and partners. (page 5)

John Brennan, the president's assistant for homeland security and counterterrorism, spoke to a public audience on May 26, one day before the release of the new National Security Strategy. It is worth noting here some key elements from Mr. Brennan's remarks:

- First, the security of the United States, its citizens, and U.S. allies and partners is, and always will be, paramount.
- Second, our enemy is not "terrorism," because terrorism is a tactic. . . . Nor do we describe our enemy as "jihadists" or "Islamists." We never have been and never will be at war with Islam. Islam, like so many faiths, is part of America.
- Third, our enemy is al-Qaeda and its terrorist affiliates; we are at war against al-Qaeda and its terrorist affiliates. The United States will disrupt, dismantle, and ensure a lasting defeat of al-Qaeda and violent extremist affiliates.
- Fourth, we will continue the never-ending work of strengthening our defenses here at home. Since 9/11, we have made enormous progress in securing the homeland. We have built upon the work of the previous administration and have accelerated efforts in many areas. We have strengthened intelligence, information sharing, and cooperation at all levels—federal, state, local, and the private sector—and timely analysis of threat information. Today, our defenses are stronger and the United States presents a much less hospitable environment for terrorists to carry out their cowardly attacks than ever before.
- Fifth, this is the first National Security Strategy of any president that integrates homeland security as part of a broader security strategy. The White House has already merged the staffs of the National Security Council, Homeland Security Council, and parts of the National Economic Council into a single, integrated National Security Staff that encompass new offices, including cybersecurity.

Finally, no nation, despite how powerful, can prevent every threat. Instead of simply building defensive walls, we must bolster our ability at all levels—federal, state, local, and the private sector—to withstand disruptions, maintain operations, and recover quickly.

We have never been and will never be at war with Islam. Like so many faiths, Islam is part of America.

## Current Threat Environment

Having tried to paint a picture of the president's overarching strategy, I now would like to give you some perspective on how we at the Department of Homeland Security's Office of Intelligence and Analysis view the terrorist threat to the homeland.

In our view, we are facing a more diversified threat than ever before. We have gone from a centralized, cellular al-Qaeda threat to loosely networked franchises, and now to radicalized individuals inspired by, but not necessarily tied to, al-Qaeda and its terrorist affiliates.

As John Brennan noted one week ago, "This is a new phase of the terrorist threat—no longer limited to coordinated, sophisticated 9/11-style attacks, but expanding to single individuals attempting to carry out relatively unsophisticated attacks."

The number and pace of attempted attacks against the United States over the past nine months have surpassed the number of attempts during any other previous one-year period, and we believe al-Qaeda, its terrorist affiliates, and radicalized individuals will try to conduct operations in the United States with increased frequency.

Particularly disturbing is the significant increase in al-Qaeda and its affiliates' ability to use operatives who have access to and familiarity with the United States.

Particularly disturbing is the significant increase in al-Qaeda and its affiliates' ability to use operatives who have access to and familiarity with the United States.

Secretary of Homeland Security Janet Napolitano spoke to this in her remarks at the National Press Club on April 15.

> This is ... really a change that I have seen in my fourteen or fifteen months as the secretary of Homeland Security. And that is the increase in the number of U.S. citizens who themselves are radicalized to the point where they may travel to the Federally Administered Tribal Areas of Pakistan (FATA) or to Yemen ... be in a camp, learn the tradecraft of a terrorist, and then return ... or learn much of it simply via the internet, among other things.

Najibullah Zazi, who pleaded guilty to plotting to attack the New York City subway system last year, is a lawful permanent [U.S.] resident, and Faisal Shahzad, now charged for his alleged role in the failed bombing attempt in Times Square on May 1, is a naturalized U.S. citizen. Both spent several years in the locale of their planned attacks. Accused Fort Hood shooter Nidal Hasan is a U.S. person, and Northwest Airlines Flight 253 passenger Abdulmutallab spent some time in the United States.

U.S. persons also have joined al-Qaeda in inspiring, plotting, and in some cases planning attacks in the homeland. U.S.-born al-Qaeda spokesman Adam Gadahn recently released a video titled *A Call to Arms* and publicly called for others to emulate the attack at Fort Hood. Anwar al-Awlaqi uses recorded messages to preach a violent interpretation of Islam and promote attacks against the United States.

Gadahn and al-Awlaqi are American citizens who understand our society, strengths, and vulnerabilities, and use that knowledge not only to plan attacks but also, via the internet and extremist websites, to exhort people already living in the United States to take up arms and launch terrorist attacks from within.

Al-Qaeda and its affiliates have not given up on prominent political, economic, and infrastructure targets to produce mass casualties and visually dramatic destruction. But recent events suggest a trend in which terrorists believe smaller, more achievable attacks against easily accessible targets could have dramatic effect.

Coupling softer targets with greater access to U.S. persons for planning and execution poses a heightened threat environment. Adding in what we believe to be shorter training cycles and less reliance on outside support or travel abroad means we have to operate under the premise that other operatives are in the country and could advance plotting with little or no warning.

Our bottom-line judgment is that we face an increased challenge in detecting terrorist plots under way by individuals or small groups acting quickly and independently or with only tenuous ties to foreign handlers.

## The Homeland Security Enterprise

Earlier in my remarks I indicated that there are clear distinctions between traditional national security, law enforcement, and intelligence programs, and the tools to support the homeland security enterprise. I would now like to turn to describing the core elements of the homeland security enterprise and its primary actors.

I also mentioned earlier that most of my career has been spent on the foreign side of the national security equation, and how different the operating environment is inside the homeland. I cannot overstate the criticality of not assuming the rules of one arena apply to the other but equally making necessary linkage between them.

The first and most central difference between traditional national security and homeland security is the role of the federal government. It is the federal government that speaks for the United States overseas. We operate under rules set forth by the federal government, regardless of whether [we are] acting unilaterally, bilaterally, multilaterally, or internationally with the international community. Rules governing what we say, how we say it, and where we operate are determined and executed by the federal government, or by entities acting on behalf of the federal government.

The first and most central difference between traditional national security and homeland security is the role of the federal government.

The traditional national security enterprise consists of our diplomatic, military, intelligence, and foreign-assistance communities coordinated in Washington, managed by an ambassador, and executed by a unified team.

On the other hand, the homeland security enterprise is completely different. It is a partnership between the federal government, states and localities, and the private sector. In traditional national security, the context is primarily the federal government. Inside the homeland, the federal government is one of several equally important actors.

Just last week, Secretary Napolitano summed up the importance of the federal/nonfederal partnership in homeland security when discussing the release of the president's National Security Strategy:

> DHS is working with federal, state, and local law enforcement, and with a range of community groups, to better combat the threats posed by domestic-based

> terrorism. We do this by ensuring that law enforcement at every level has access to information and intelligence about threats so they are fully equipped to confront them on the front lines.

Identifying the type of suspicious activity we are seeing today associated with attempted terrorism in the homeland almost certainly will come from outside the federal government. Our security at home depends on expanding the federal government's partnerships with states, localities, and the private sector. This partnership means the federal government provides timely and predictive information on terrorist training, techniques, and patterns of behavior to the nonfederal network. This information is intended to link what the federal government knows about terrorism plots and makes it relevant and actionable to nonfederal partners in their communities.

This partnership must be reciprocal. Nonfederal partners must know what to look out for and how to convey suspicious-activity information to the federal government.

In other words, information sharing is the key to the federal-nonfederal partnership. This is easier said than done. Information sharing between federal actors is often a matter of technology and culture. Information sharing with nonfederal partners involves mutual investment in building classified and unclassified systems for collaboration; harmonizing federal, state, local, and private-sector information-sharing rules; and establishing the trust that the federal government will share all it can but still may not always be able to share all that it knows. Of course, and most important, we are talking about information sharing inside the United States.

Information sharing is the key to the federal-nonfederal partnership.

DHS, and my home office of I&A in particular, is leading the effort to build focal points for information sharing between the federal government and nonfederal partners. This effort comes together through what we call "fusion centers." Fusion centers are owned and operated by states and localities. The federal government, primarily through DHS and DOJ, provides assistance and connectivity to recognized fusion centers. DHS also ensures a federal presence at fusion centers. This presence is intended to give reach back to Washington and for the fusion of federal and nonfederal information.

Fusion centers are neither joint terrorism task forces nor intelligence operations centers. Fusion centers are what their name implies—a vital analytic mechanism for expanding the partnership network between federal and nonfederal homeland security officials.

Secretary Napolitano has made standing up a fully operational national network of fusion centers one of her highest priorities. There are currently seventy-two fusion centers up and running across the country. Soon, all fusion centers will have classified connectivity to the federal government and at least one representative from the DHS Office of Intelligence and Analysis. The DHS Office for Civil Rights and Civil Liberties, as well as the DHS Privacy Office, provides training to federal, state, and local fusion-center personnel. This is done to ensure that all activities at fusion centers are done in accordance with our cherished privacy rights, civil rights, and civil liberties.

## Homeland Security Intelligence: Challenges and Complexities

Finally, I would like to spend just a few moments discussing some of the unique challenges in defining homeland security intelligence. This is a new and still developing discipline; we have a ways to go in our understanding of its primary mission space and operating environment.

Among the most challenging questions the broader homeland security community is wrestling with are the following:

- What is the homeland security intelligence playing field?
- What are its strategic and operational playing fields?
- What does it mean to produce strategic analysis on homeland security?
- Is it the same as producing classified national intelligence estimates on terrorism trends in the homeland?
- Is it like producing the State Department's annual, unclassified *Patterns of Global Terrorism*?
- Might homeland security intelligence be more like operational intelligence provided to warfighters?
- Is homeland security intelligence more akin to the tactical targeting and case support provided to traditional law enforcement and intelligence collectors overseas?

Answering these questions is made more difficult when taking into account the reality that a large swath of the homeland security intelligence customer set is nonfederal partners without security clearances. And even in cases where nonfederal partners have security clearances, how do we best support them in their requirement to translate the information for the vast majority of their brethren who do not have clearances?

Another evolving element in defining homeland security intelligence is how this field is integrated with the traditional law enforcement and intelligence communities. Traditional law enforcement activities, like the investigative work done by the Federal Bureau of Investigation, and foreign intelligence collection done overseas, are conducted in a different context. Law enforcement investigations must have a predicate. Likewise, in a society committed to the preservation of both security and liberty, information on our citizens must not be collected solely for the purpose of monitoring religious, political, or other protected activities. Even when assessing demographic trends and detecting patterns of behavior, we must pay careful attention to ensuring that we do not somehow stifle people's willingness to participate in our democratic society. In a globalized world where there is a decreasing distinction between terrorist plots conceived, planned, and executed overseas from those inside the homeland, striking the right balance between identifying and sorting potentially key bits of information necessary for homeland security intelligence has become one of our greatest and [most] important challenges.

Striking the right balance between identifying and sorting potentially key bits of information necessary for homeland security intelligence has become one of our greatest and [most] important challenges.

Finally, there is a range of obstacles [faced when] integrating homeland security intelligence information with that of the larger national intelligence community. My home office, the DHS Office of Intelligence and Analysis, works in both worlds. It is a statutory member of the national intelligence community—the national intelligence community that understandably has a predominantly foreign focus, rarely engages with nonfederal partners, and has few requirements for information associated with U.S. persons inside the homeland. My office not only views the homeland as its primary playing field, but most often attempts to provide terrorism-related information at the unclassified level to those outside the federal government who often are unfamiliar with the scope and limitations of intelligence collection and analysis.

## Conclusion

President Obama has issued his first National Security Strategy. He has said we must eliminate the increasingly frayed distinction between foreign- and homeland-based terror threats. Al-Qaeda and its affiliates make no distinction, and neither should we. Our warfighters, law-enforcement officials, and intelligence operators overseas must continue to be successful in degrading and denying safe haven to al-Qaeda and its affiliates.

Those of us with responsibilities for counterterrorism at home must work through what it means to provide homeland security intelligence.

President Obama has said we must eliminate the increasingly frayed distinction between foreign- and homeland-based terror threats.

We know that securing the homeland from al-Qaeda and its affiliates requires seamless connectivity between the federal government and our state, local, tribal, territorial, and private sector partners. There are more than 750,000 state and local law-enforcement and first responders in the homeland. They know their communities far better than we in Washington. We can provide them guidance and current information on threat trends and patterns. But it is a reciprocal relationship, in which we are dependent on the information provided by them.

In closing, I would like to return to where I began. The terror threat to the homeland is real and it is evolving. We must continue to evolve too. The president, federal national-security community, and homeland security enterprise—comprised of state, local, tribal, and private sectors—are doing all that we can to identify and disrupt threats. This means deepening the partnerships between all elements of homeland security national power. We all have a role in this enterprise.

# Confronting a Resilient al-Qaeda: The U.S. Strategic Response

*Daniel Benjamin*

May 21, 2010
Prepared Remarks

Good afternoon. It is a great pleasure to be back at The Washington Institute and see so many familiar faces in the room. Thanks to Matt Levitt for inviting me. A few weeks ago Matt and I shared a panel at the Anti-Defamation League. For twenty-five years now, The Washington Institute has been putting out quality scholarship on the Middle East—work that I read regularly when I was in the think-tank world, but is perhaps even more valuable for me now as a senior U.S. government policymaker. Rob Satloff's fascinating book and the follow-on documentary on the Muslims in North Africa who helped save Jews during the Holocaust shed new light on the events of that era, and have relevance for today as well.

I am also pleased to be participating in The Washington Institute's counterterrorism lecture series, which my predecessor, Ambassador Dell Dailey, kicked off in December 2007, and I know you have had at least twenty of the U.S. government's top counterterrorism officials. I am particularly glad to have the chance to be here today because, as I think most people in this room recognize, there have been some important changes in the nature of the threat in recent months. So I want to discuss with you what those changes are and how the Obama administration is adapting and reshaping the way the United States combats terrorism both in the short and in the long term.

■ *Daniel Benjamin, coordinator for counterterrorism, State Department*

Let me begin with the baseline: over the last year, al-Qaeda has suffered a number of important setbacks. As you have heard from the leaders of our intelligence community recently, the group remained under pressure in Pakistan due to Pakistani military operations aimed at eliminating militant strongholds in the Federally Administered Tribal Areas (FATA). It has had a number of leadership losses and is finding it more difficult to raise money, train recruits, and plan attacks outside of the region. As my friend and colleague Treasury assistant secretary David Cohen noted here last month, al-Qaeda (AQ) is now in the "worst financial shape it has been in for years."

Of course, this by no means suggests that we can signal the all-clear on conspiracies driven by al-Qaeda's senior leadership—we know full well that they are still a highly capable, highly innovative, and very determined group. But even outside the FATA, the environment is becoming more challenging. Al-Qaeda has also suffered from popular Muslim disaffection due to recent and

past indiscriminate targeting of Muslims by its operatives and allies in Algeria, Iraq, Saudi Arabia, Pakistan, Indonesia, and any number of other countries. The number of conservative clerics and former militants speaking out against the organization has increased, and that is very good news indeed.

Despite these setbacks to the core leadership, the broader AQ threat is becoming more widely distributed and more geographically and ethnically diversified among affiliates and among those who are inspired by the AQ message. We saw this most dramatically with the attempted December 25 bombing of a U.S. commercial airliner. This incident demonstrated that at least one affiliate—al-Qaeda in the Arabian Peninsula (AQAP)—has not just the will but also the capability to launch a strike targeting the United States at home. We have every expectation that we will hear more from AQAP.

We have learned something else important this year: the assumption that Americans have some special immunity to al-Qaeda's ideology has been dispelled. While our overall domestic radicalization problem remains significantly less serious than in many Western nations, several high-profile cases demonstrate that we must remain vigilant. As you all know, five Americans from nearby Virginia were arrested in Pakistan on suspicion of terrorist ties. We also have seen Americans traveling to Somalia, ones who ultimately ended up joining al-Shabab.

The assumption that Americans have some special immunity to al-Qaeda's ideology has been dispelled.

We have seen U.S. citizens rise in prominence as proponents of violent extremism. The native Californian Adam Gadahn has become an AQ spokesman, enabling the group to increasingly target its propaganda to Western audiences. Another individual, Omar Hammami, an American citizen who grew up in Alabama, has become an important al-Shabab voice on the internet. The most notable is Yemeni-American Anwar al-Awlaqi, who has become the most influential voice of Islamist radicalism among English-speaking extremists and has catalyzed a pool of potential recruits that others had failed to reach. The alleged Fort Hood attacker, Nidal Malik Hasan, sought him out for guidance, and the December 25 bomber, Umar Farouq Abdulmutallab, visited him at least twice in Yemen. We should make no mistake about the nature of al-Awlaqi: as his recent video declaration of allegiance to al-Qaeda suggests, this is not just an ideologue, but someone who incites acts of mass violence against Americans and others, and someone who is at the heart of a group plotting such action.

Another domestic dimension of the changing threat: in the last few months we have seen two high-profile law-enforcement cases, individuals who appear to have been trained and handled from the FATA, operating within our borders. Najibullah Zazi, a U.S. lawful permanent resident and airport shuttle driver, trained in Pakistan and recently pleaded guilty to charges that he was planning to set off several bombs in the United States. An American citizen, David Headley, has pleaded guilty in a U.S. court to crimes relating to his role in the November 2008 Lashkar-e-Taiba attacks in Mumbai, which killed more than 160 people—including six Americans. Yes, it is important to note that we found these people and that our intelligence and law-enforcement tripwires worked. But that is not reason enough for complacency. The threat we face is dynamic and evolving.

Now we have the Times Square incident to add to the list. You have seen the public remarks from Attorney General Eric Holder about Faisal Shahzad and

his links to the Pakistan Taliban, and reports of search warrants that have been executed in several locations in the Northeast in connection with this investigation. Because this is an ongoing investigation, I cannot say more, but what I can say is that the significance of this case cannot be ignored.

Obviously, these changes that we have seen in the threat challenge us in important ways. A Nigerian suicide bomber—someone with virtually no prior record of involvement in terrorism who can be effectively launched at us from Yemen: this presents a real intelligence and security challenge, and so, too, does the appearance of operatives in the United States who are legal residents or citizens but are connected with AQ or another radical group in South Asia.

Clearly, there is a requirement to improve our intelligence, and without going into details here, I can assure you that the intelligence community is working hard on this. And there are challenges for our defenses—especially our aviation security, since aviation remains at the top of the list of al-Qaeda's targets—as it has demonstrated recently through both successful and unsuccessful plots directed at aircraft. The United States has taken steps, both on its own and with international partners, to bolster aviation security in the wake of the failed bombing on Christmas Day.

Under Secretary Janet Napolitano's leadership, we have been working closely with the International Civil Aviation Organization, the G-8, and other multilateral forums to lead a global initiative to strengthen the international aviation system against the evolving threats posed by terrorists. Over the past several months, the U.S. government has signed joint declarations with numerous foreign partners on improving information sharing, strengthening aviation-security measures and standards, and working together to develop and deploy new security technologies to airports around the world. We have also strengthened the watch-listing system and developed new, more flexible security protocols based on real-time, threat-based intelligence. These measures consist of multiple layers of security, seen and unseen, which are tailored to intelligence about potential threats.

Defenses, of course, are an essential part of the equation. But another equally vital part of the equation is engaging with the other countries that are being used as platforms by terrorists and working with them to contain, reduce, and eliminate these threats. Given what we have seen over the last year and the years before, Pakistan and Yemen are today the countries of greatest concern. So let me turn to our efforts with them.

Given what we have seen over the last year and the years before, Pakistan and Yemen are today the countries of greatest concern.

First, Pakistan: Pakistan, we should all remember, is a frontline partner in fighting extremists. We provide a spectrum of assistance to Pakistani counterterrorism campaigns, which ranges from police training to anti-money-laundering efforts. Undoubtedly, the hundreds of millions of dollars directed to Pakistani counterterrorism efforts have saved American lives, and we should not forget that Pakistan has put out of business more al-Qaeda operatives than any other country.

Over the past year, the U.S. government has seen very encouraging signs that Pakistan not only recognizes the severity of the threat from violent extremists but is actively working to counter and constrain it. Pakistani military operations in Swat and Waziristan have eliminated militant strongholds and damaged

the operational abilities of extremist groups. Moreover, we are seeing increasing cross-border cooperation with Afghanistan and the International Security Assistance Force, which is instrumental in the reduction of key militant safe havens. And in the wake of the operation in Swat, we have seen public opinion turn more decisively against the militants.

In late March, with the beginning of the Strategic Dialogue with Pakistan, we started a new phase in our partnership, with a new focus and a renewed commitment to work together to achieve the goals we share: stability, prosperity, and opportunity for the people of both Pakistan and the United States. While this was not the first strategic dialogue between our countries, it was the first at the ministerial level, and it reflects the administration's commitment to its success. Under the Kerry-Lugar legislation, we will be providing Pakistan with $1.5 billion a year—for five years—to address key developmental issues.

The discussions in the Strategic Dialogue generated new momentum and mutual trust to jointly tackle the extremist groups that threaten both Pakistan's security and U.S. security. And I should mention that under this new dialogue, I will travel to Islamabad for the second time in three months with an interagency team in June to discuss terrorism with the Pakistanis. During the trip, both countries will discuss how to better use nonmilitary capabilities to fight extremism.

We have seen tangible evidence of Pakistan's commitment to clamping down on extremist networks operating within its borders. As you know, several top Afghan Taliban leaders—including Mullah Abdul Ghani Baradar—have been apprehended, and we are grateful to the Pakistani authorities for this.

We have seen tangible evidence of Pakistan's commitment to clamping down on extremist networks operating within its borders.

Immediately after the Times Square incident, we also began working closely with the government of Pakistan on the investigation, and it has been cooperative in assisting our efforts. We will continue to work with Islamabad on this important prosecution.

Let me turn to Yemen. It is important to remember that Yemen did not turn into an al-Qaeda safe haven overnight. In fact, Yemen was arguably the very first front, since the December 1992 al-Qaeda attempt to bomb U.S. troops was probably the first genuine al-Qaeda attack in Aden. Those troops, you may recall, were en route to Somalia to support the UN mission there—almost eight years before the USS *Cole* attack in 2000. Al-Qaeda has had a foothold in Yemen since the organization's earliest days, and this has always been a major concern for the United States.

When the Obama administration came into office, it was clear that the government of Yemen was distracted by other domestic security concerns, and our bilateral cooperation had experienced real setbacks and al-Qaeda was on the rise. In the spring of 2009, the administration initiated a full-scale review of our Yemen policy. The review has led to a new, whole-of-government approach to Yemen.

To advance this strategy, we have engaged consistently and intensively with our Yemeni counterparts. Senior administration civilian and military officials—including Deputy National Security Advisor John Brennan, Assistant Secretary of State for Near Eastern Affairs Jeffrey Feltman, Gen. David Petraeus, and myself—visited Yemen to discuss how we can jointly confront the

threat of al-Qaeda. The result has been a significant—and we hope enduring—turn by the government in taking on al-Qaeda consistently. Those actions, it is important to emphasize, began before the December 25 plot, and have continued ever since.

Now, Yemen has conducted multiple operations designed to disrupt AQAP's operational planning and to deprive its leadership of safe haven within Yemeni territory.

We recognize that al-Qaeda has taken advantage of insecurity in various regions of Yemen that have been worsened by internal conflicts. We also know that Yemen is grappling with serious poverty—it is the poorest country in the Arab world. This lack of resources inhibits good governance, the delivery of services, and the effectiveness of the security that is needed to deal with terrorism. So to have any chance of success, U.S. counterterrorism policy has to be conceived in strategic, and not merely tactical, terms and time lines. That is why the administration has adopted a two-pronged strategy for Yemen—helping the government confront the immediate security concern of al-Qaeda and mitigating the serious political, economic, and governance issues that the country faces over the long term. Not only are we working to constrict the space in which al-Qaeda can operate in Yemen by building up the Yemeni capacity to deal with the security threats within its borders, we are also working to develop government capacity to deliver basic services and economic growth.

We recognize that al-Qaeda has taken advantage of insecurity in various regions of Yemen that have been worsened by internal conflicts.

This dual strategy will help Yemen confront the immediate security concern of al-Qaeda, but also mitigate the serious political and economic issues that the country faces in the longer term. It is a strategy that requires full Yemeni partnership. It is a strategy that requires working closely with regional partners and allies. It is a strategy that requires hard work and American resources. The challenges are great, and they are many; but the risk of doing nothing is far too grave.

What we are doing in Yemen, what we are doing in Pakistan, is what we are doing in many other countries—building capacity. Consistent diplomatic engagement with counterparts and senior leaders helps build political will for common counterterrorism objectives. When there is that political will, we can address the nuts-and-bolts aspect of capacity building. We are working to make the training of police, prosecutors, border officials, and members of the judiciary more systematic, more innovative, and more far-reaching. Capacity building also includes counterterrorism finance training; it represents a whole-of-government approach. This is both good counterterrorism and good statecraft. We are addressing the state insufficiencies that terrorism thrives on, and we are helping invest our partners more effectively in confronting the threat—rather than have them look thousands of miles away for help or simply look away altogether.

I have focused on some of the diplomat's traditional tools—engagement, building political will, and capacity building. I think we are deploying these tools well. But the diversification of the threat I have described means that we cannot stop there. We need to both use all of the tools in our toolbox and to innovate and create new ones—to continue to stay ahead of the threat and to maintain and strengthen our defenses.

For example, we need to advance our agenda of building international security cooperation against the terrorist threat. Our allies in Europe have become central partners in the counterterrorism arena, as a number of the plots in recent years illustrate dramatically just how intertwined U.S. and European security interests have grown.

With American and European fates so closely linked, it is essential that we work together even more closely to prevent al-Qaeda and its affiliates from carrying out a successful attack. The Treasury Department's Terrorist Finance Tracking Program and the DHS's Passenger Name Record program are both critically important tools in this effort, and have proven instrumental in protecting the security of Americans and Europeans alike.

Given the importance of these programs to both U.S. and European security, we and the Europeans have a longstanding partnership to protect both the security of our citizens *and* their personal data. We know our two approaches to protecting privacy have more in common than what divides them, and we both share a strong commitment to protecting human rights. The challenge is to reach agreement on the proper balance between security and privacy without impeding the operation of vital programs and creating security gaps that have the potential to harm not only American citizens but individuals from Europe and beyond as well.

We need to advance our agenda of building international security cooperation against the terrorist threat.

There is one more key area in which we need to innovate. In the past eight years, the United States has made great strides in what might be called tactical counterterrorism—taking individual terrorists off the street, and disrupting cells and their operations. But an effective counterterrorism strategy must go beyond efforts to thwart those who seek to harm the United States and its citizens, allies, and interests. Military power, intelligence operations, and law-enforcement efforts alone will not solve the long-term challenge that we face—the threat of violent extremism. Instead, we must look as well to the political, economic, and social factors that terrorist organizations exploit and to the ideology that is their key instrument in pushing vulnerable individuals down the path toward violence. As President Obama succinctly put it, "A campaign against extremism will not succeed with bullets or bombs alone."

Quite simply, we need to do a better job to reduce the recruitment of terrorists. To combat terrorism successfully, we have to isolate violent extremists from the people they pretend to serve. In the government, we refer to this as countering violent extremism, or CVE. Many have attempted CVE efforts over a number of years from a number of different agencies but without sufficient focus. Now we have an administration that is committed to cutting down on radicalization and recruitment.

The indiscriminate targeting of Muslim civilians by violent extremists that I mentioned before in Iraq, Pakistan, and elsewhere has alienated populations, led to a decline in support for al-Qaeda's political program, and outraged influential clerics and former allies—who in many cases have spoken publicly against terrorism. But we cannot count on al-Qaeda to put itself out of business. So we are also focusing our efforts on undermining the narrative and preventing the radicalization of vulnerable or alienated individuals.

We are working to develop a better understanding of the dynamics of the communities in which violent extremism has taken root. Every at-risk community possesses unique political, economic, and social factors that contribute to the radicalization process. For this reason, we know that one-size-fits-all programs have limited appeal. Instead, programs need to be tailored to fit the characteristics of the audience. "Microstrategies" need to be customized for specific communities—and even neighborhoods—and they will have a better chance of succeeding and enduring.

We also know that credible local voices have to take the lead in their own communities. They are the ones best placed to convey counternarratives capable of discrediting violent extremism. The U.S. government is simply not going to be the most credible interlocutor in this conversation, so we are working to identify reliable partners and amplify legitimate voices. The United States can help empower these local actors through programmatic assistance, funding, or by simply providing them with space—physical or electronic—to challenge violent extremist views. Nontraditional actors such as NGOs, foundations, public-private partnerships, and private businesses are some of the most capable and credible partners in local communities. The U.S. government and partner nations are also seeking to develop greater understanding of the linkages between diaspora communities and ancestral homelands. Through familial and business networks, events that affect one community have an impact on the other.

With the aid of credible messengers, the United States is trying to make the use of terrorist violence taboo and to trump the radical narrative, and also to offer something more hopeful. President Obama's effort to create partnerships with Muslim communities on the basis of mutual interest and mutual respect, as he outlined in speeches in Ankara and Cairo, provides an opportunity to promote a more positive story than the negative one promulgated by al-Qaeda.

Obama's effort to create partnerships with Muslim communities on the basis of mutual interest and mutual respect provides an opportunity to promote a more positive story than the negative one promulgated by al-Qaeda.

Clearly, we have not figured it all out. Al-Qaeda is a nimble adversary, and we have a never-ending race to protect our country and stay one step ahead. Because of the flatness of their organization, a high level of inspiration, and ingenuity, we need to be on top of our game all the time. We need to keep in mind the words of the 9-11 Commission Report, which in this respect got it precisely right: "It is crucial," the investigators wrote, "to find ways of routinizing and even bureaucratizing the exercise of the imagination." This is really the paramount and enduring challenge we face. Staying sharp, innovating our defensive systems, and maintaining our intellectual edge—these are all essential.

Well, I know a speech at The Washington Institute would be incomplete without some discussion of the other side of the terrorism coin—the state sponsors of terrorism. And they are among the U.S. government's highest priorities as well. Together with Matt Levitt, I spoke at length on this exact subject recently at the ADL conference, and I would refer you to my remarks from that event, which are posted on the State Department website.

It is important not to forget that Iran remains the foremost state sponsor of terrorism, supporting Hizballah, Hamas, and other terrorist Palestinian groups. And Syria has also provided political and material support to Hizballah in Lebanon and allowed Iran to resupply it with weapons. In early April, we

reiterated our grave concerns and alarm to the Syrians over reports that they may have provided Scud missiles to Hizballah.

We have spoken out forcefully about the grave dangers of Syria's transfer of weapons to that group. We condemn this in the strongest possible terms and have expressed our concerns directly to the Syrian government. Transferring weapons to Hizballah—especially longer-range missiles—poses a serious threat to the security of Israel. It would have a profoundly destabilizing effect on the region. And if such weapons cross into Lebanon, it would absolutely violate UN Security Council Resolution 1701, which bans the unauthorized importation of any weapons into Lebanon.

We have spoken out forcefully about the grave dangers of Syria's transfer of weapons to Hizballah.

We do not accept such provocative and destabilizing behavior—nor should the international community. President Bashar al-Asad is making decisions that could mean war or peace for the region. We know he is hearing from Iran, Hizballah, and Hamas. It is crucial that he also hear from us directly, so that the potential consequences of his actions are clear. That is why we are sending an ambassador back to Syria. There should be no mistake, either in Damascus or anywhere else: the United States is not reengaging with Syria as a reward or as a concession. Engagement is a tool that can give us added leverage and insight, and a greater ability to convey strong and unmistakably clear messages aimed at Syria's leadership.

Thank you for the opportunity to speak today. I look forward to your questions.

# Enhancing International Cooperation against Terrorism Financing

*David Cohen*

April 7, 2010
Prepared Remarks

Good afternoon. I want to thank the Washington Institute for Near East Policy for inviting me to speak today. It is a great privilege to have the opportunity to offer my voice to the exchange of views fostered by this distinguished institution.

Before I begin, I want to offer my special thanks to Matt Levitt and Mike Jacobson for facilitating this event. As many of you know, Matt and Mike each spent several years doing outstanding work in Treasury's Office of Intelligence and Analysis. We at Treasury remain grateful for their service, and The Washington Institute has been fortunate to benefit these past few years from their insightful and innovative scholarship on critical issues relating to terrorism and terrorist financing.

■ *David Cohen, assistant secretary for terrorist financing, Treasury Department*

As you know, the Treasury Department's Office of Terrorism and Financial Intelligence (TFI) plays a unique role in U.S. national security. As I stand before you today, TFI is contributing to work on a new, robust set of sanctions against the government of Iran; ensuring compliance with the letter and spirit of UN Security Council resolutions regarding North Korea's nuclear program; assisting the courageous [administration of Felipe] Calderon in targeting the financial networks of violent drug-trafficking organizations in Mexico; and committing substantial resources to combating illicit finance in Afghanistan and Pakistan, as we work to disrupt the money flows that support al-Qaeda, the Taliban, and other extremist groups.

In short, we are active on many fronts—here at home and around the world—to foster a well-regulated, transparent, and secure financial system, one that is inhospitable to money laundering, terrorist financing, and other forms of illicit finance.

Today, I'd like to focus on TFI's work to disrupt and dismantle terrorist-financing networks. In particular, I will discuss the importance of strong and enduring mechanisms of international collaboration in the ongoing effort to combat terrorist financing.

We say it often, but it bears repeating: our national-security interests are best advanced when a broad coalition of nations works together to fight against those who engage in terrorist activity. There is no question that we can do a great deal to combat terrorist financing simply through the exercise of

our national authorities—and Treasury has made great progress against terrorist financing and facilitation through designations under our counterterrorism executive order.

But in today's global environment, where terrorists have no regard for national boundaries, and money rockets around the globe, effective and empowered multilateral forums and mechanisms significantly amplify our own efforts and provide some of the most powerful defenses against terrorist threats.

I want to begin by briefly addressing some of the very real terrorist threats we face—threats that powerfully demonstrate the need for coordinated international action. As you are well aware, often these threats are associated with terrorist networks linked to the Middle East, whose avowed goal is to disrupt any and all efforts at achieving peace in that troubled region.

First and foremost, there is al-Qaeda, which is now in the worst financial shape it has been in for years. But al-Qaeda is not disabled, nor is it bankrupt, and our progress in degrading its financial strength will not be lasting without continued, vigorous efforts.

Reacting to the financial state of the al-Qaeda core, al-Qaeda affiliates in Africa and the Arabian Peninsula have come to rely less on support from the al-Qaeda network as they plan and mount terrorist attacks. These al-Qaeda affiliates instead have taken up independent fundraising activities to sustain themselves—including drug trafficking, kidnapping for ransom, and extortion.

Al-Qaeda is not disabled, nor is it bankrupt, and our progress in degrading its financial strength will not be lasting without continued, vigorous efforts.

Unlike al-Qaeda, the Taliban is not experiencing much financial stress, and it has sufficient resources to sustain its recruiting and training infrastructure, conduct devastating attacks on Afghan civilians, and present substantial resistance to our troops. Working with the Afghan government, we have achieved some key successes against the Taliban's finances, and we are confident that there are many more successes to come. But the Taliban still has the funding necessary to hold territory, buy allegiance, and fundamentally challenge our core national-security objective of bringing peace and stability to Afghanistan.

In the Middle East, Hamas—which ignores demands from the international community to renounce violence—receives substantial support from the government of Iran, as well as contributions from donors and nongovernmental organizations (NGOs) in the Gulf states and in Europe. The Palestinian Authority, which understands the threat that Hamas poses to peace in the region, has taken important steps to limit Hamas's influence by supervising both the Palestinian banking system and the charitable sector in the West Bank and Gaza. Working closely with the Palestinian Authority, last month we designated the Islamic National Bank of Gaza for providing financial services to Hamas.

Even more than Hamas, Hizballah receives support from Iran, which is supplemented by expatriate sympathizers, NGOs, and a variety of revenue-generating commercial enterprises. This financial backing helps fund Hizballah's communications, security, weapons systems, and terrorist operations. Suffice it to say, we are keenly focused on the threat that Hizballah poses to destabilize the region.

The ability of any of these terrorist organizations to function—including their ability to raise, move, and expend funds in support of their violent

activities—represents a clear threat to our national security. We are hard at work combating this activity. But make no mistake: our success depends in significant part on the extent to which we are able to engage our international partners in a cooperative effort to combat terrorist financing.

Against this backdrop, I want to highlight three key international mechanisms for coordinating global efforts against terrorist financiers and facilitators: first, the terrorist designation program under UN Security Council Resolution (UNSCR) 1267 and its counterterrorist-financing companion, UN Security Council Resolution 1373; second, the recent work by the Financial Action Task Force to identify jurisdictions with strategic deficiencies in their anti-money-laundering and counterterrorist-financing laws; and finally, Treasury's Terrorist Finance Tracking Program, a key tool in our counterterrorism arsenal. Each of these mechanisms can be highly effective in protecting our national and international security—and even more so when the international community as a whole embraces and supports them.

## The UN Counterterrorist-Financing Regime

The core of the UN Security Council's efforts against the financing of terrorism is UNSCR 1267 (its al-Qaeda and Taliban sanctions regime) and UNSCR 1373 (which requires every UN member state to adopt laws preventing and suppressing the financing of terrorism).

UNSCR 1373 requires each UN member state to adopt laws preventing and suppressing the financing of terrorism.

Without question, these resolutions are among the most effective international coordination mechanisms we have in combating terrorist financing. Yet because of some unfounded concerns about the fairness of the UNSCR 1267 designation process, and because of limited compliance with UNSCR 1373's requirements, one of the international community's most powerful counterterrorist-financing mechanisms is not operating as effectively as it could or should.

Now more than a decade old, the 1267 designation process has been quite effective in disrupting and disabling terrorist activity. Indeed, al-Qaeda's weakened financial state today is traceable, at least in part, to designations of al-Qaeda financiers under UNSCR 1267.

But in the past few years, the 1267 regime has come under attack, particularly in Europe, for not providing adequate procedural protections for those designated. Some listed individuals and entities have brought their complaints to courts in Europe, asserting that the designation process violates EU guarantees of fundamental human rights. These critiques and court cases have led some to doubt the long-term viability of the UN designation process.

These challenges are misplaced, largely because they do not take into account improvements that have been introduced over the last few years in two successor resolutions, UNSCR 1822 and UNSCR 1904, that have markedly enhanced the procedural protections for those who are designated.

UNSCR 1822, adopted in June 2008, requires the posting on the 1267 committee's website of narrative summaries explaining the bases for each designation. It also calls for a comprehensive review of every person and entity that appears on the 1267 list. This comprehensive review, which is to be completed by June of this year, is to be followed by periodic reviews of all listings in the future. These reviews involve an extremely thorough and detailed

analysis of the facts around each designation to determine whether a sufficient basis continues to exist to maintain a designation or, alternatively, that a designee should be delisted.

Bear in mind that a delisting may be warranted for a variety of reasons—including, most important, [...] evidence that the designee has taken affirmative steps to disassociate from al-Qaeda or the Taliban. After all, a key goal of a designation is to encourage a change in behavior—to persuade someone who is affiliated with al-Qaeda or the Taliban to renounce terrorism and rejoin the legitimate political process. Altogether, fifty-eight names have been taken off the 1267 list since the 1822 review process began.

UNSCR 1904, adopted last December, expands the protections for designees. Most important, it created an "ombudsperson" to receive delisting requests from designees and to assist the committee in considering these requests by conducting research, engaging in dialogue with relevant parties, and drafting a report on the delisting petition for committee review.

These procedural enhancements, among others, go a long way to resolving concerns about the fundamental fairness of the 1267 designation process. But regardless of whether some of the criticisms of the original 1267 regime had validity, the UN designation process as it operates today—with its emphasis on transparency, accuracy, and redress—is worthy of broad international support.

UNSCR 1373 obligates each member state to adopt laws that would allow it to apply targeted financial measures against terrorists and their support networks.

But that is not enough. The other key component of the UN's counterterrorist financing program is UNSCR 1373, which obligates each member state to adopt laws that would allow it to apply targeted financial measures against terrorists and their support networks. Each member state is required to criminalize terrorist financing, forbid providing financial support to terrorists, and freeze the assets of those who commit or support terrorist acts.

Unfortunately, compliance with UNSCR 1373 is quite spotty. In fact, my colleagues and I spend a good deal of time traveling the globe to encourage states to come into compliance with this resolution.

We do not do this because we fancy ourselves the UNSCR 1373 compliance police. We do this because, when a country criminalizes terrorist financing and develops the legal basis to apply target[ed] financial sanctions, it sends a powerful message to its citizens that terrorist financing is wrong. And when a country demonstrates its commitment by taking action against terrorist financiers, it also amplifies the effectiveness of global efforts to combat terrorist financing, including the UN 1267 designation process.

Which brings me back to my key point: when the community of nations works together in a coordinated and cohesive fashion to combat terrorist financing, we all benefit.

## Financial Action Task Force

The second international counterterrorism mechanism I would like to address is the Financial Action Task Force (FATF), and in particular the recent work by the FATF to publicly identify jurisdictions that pose substantial threats to the international financial system due to significant, unresolved deficiencies in their anti-money-laundering and counterterrorist-financing legal regimes.

I imagine that many of you are familiar with the FATF, the premier international standard-setting body for regulating anti-money-laundering and counterterrorist-financing regimes. Its forty recommendations for legal and regulatory structures to protect against money laundering and its nine special recommendations against terrorist financing represent the unquestioned gold standard in the international effort to combat illicit finance, having been recognized as authoritative by the UN Security Council and the G-20.

It is instructive to compare how the FATF and the UN Security Council go about their work against terrorist financing. Unlike the UN Security Council, whose efforts are targeted at individuals and entities engaged in terrorism or terrorist financing and whose actions have the force of international law behind them, the FATF focuses on systemic issues and relies on voluntary compliance to achieve its goals. But much like the Security Council's 1267 designation process, the FATF's success in combating terrorism and terrorist financing depends in large part on the extent to which countries around the world join in the effort. The FATF elicits cooperation not through the force of law or the threat of compulsion—it has neither at its disposal—but through a combination of unquestioned expertise, widespread acknowledgment of the validity of its technical judgments, and a strong dose of peer pressure.

The FATF's success in combating terrorism and terrorist financing depends in large part on the extent to which countries around the world join in the effort.

Over the past decade, working with the International Monetary Fund, the World Bank, and FATF-style regional bodies, the FATF has assessed virtually every country against its standards. These mutual assessments produce lengthy reports detailing each country's compliance, in law and in practice. Although addressing highly charged issues, these mutual assessments have been enormously successful in improving the worldwide anti-money-laundering (AML) and counterterrorist-financing (CFT) regime, in large part because the mutual assessments are understood to be objective reviews against technical standards, where accuracy and impartiality are the overriding concerns. Because of this, many countries have chosen to remedy the deficiencies noted in their mutual assessments by modifying their AML/CFT legal structures and following through to implement effective AML/CFT controls.

Nonetheless, some countries have refused to bring their AML/CFT regime into line with the FATF's standards, or have failed to translate adequate laws into real action. As a result, in 2006 the FATF upped the ante. It established a new initiative to publicly identify those uncooperative jurisdictions that have gone through the mutual evaluation process, whose AML/CFT regimes have been found to be deficient, and that have failed to take corrective action.

One notable result of this process has been the FATF's actions to highlight the serious threat to the international financial system posed by Iran's lack of comprehensive AML/CFT controls. The FATF publicly identified Iran's AML/CFT deficiencies in October 2007, and three more times in 2008. Each time, the FATF called for its members to advise their financial institutions to take the risk arising from Iran's deficiencies into account if they engaged in or facilitated transactions with Iran.

Then, in February 2009, after Iran still failed to meaningfully address its AML/CFT deficiencies, the FATF called for its members to apply countermeasures to protect their financial sectors from the risks emanating from Iran. The

FATF has reiterated its call for countermeasures against Iran three times, most recently in February of this year.

In April 2009, the G-20 asked the FATF to reinvigorate its review process and publicly identify high-risk jurisdictions for terrorist financing and money laundering. The FATF responded and in February 2010 publicly identified twenty-eight countries—in addition to Iran—with strategic deficiencies in their AML/CFT controls.

The apprehension generated by the G-20's request that the FATF identify AML/CFT laggards was itself a powerful motivating force. By the time the FATF issued its report in February of this year, most of the countries that were publicly identified as having strategic AML/CFT deficiencies had made clear, high-level political commitments to work with the FATF to remedy their problems. In its February statement, the FATF welcomed these commitments.

But a few countries—Angola, Ecuador, Ethiopia, and North Korea—failed to engage constructively with the FATF and commit to improving their AML/CFT regimes. The FATF responded by calling on its members to consider the money-laundering and terrorist-financing risks arising from these countries. Heeding this call, several countries, including the United States, issued advisories to their financial institutions highlighting these countries' lack of commitment to AML/CFT reform and instructing their institutions to apply enhanced due diligence in conducting transactions with banks in these countries.

Clearly, the FATF's effectiveness comes from the broad-based, international consensus—which it has carefully nurtured and promoted over the past two decades—that money laundering and terrorist financing represent a serious risk to our mutual security. It is critical that the international community continue to respect the FATF's judgments, respond to its calls for due diligence and countermeasures, and support its continued work to protect the international financial system.

The Treasury Department's Terrorist Finance Tracking Program is a crucial international mechanism in countering illicit finance and transnational terrorism.

## Terrorist Finance Tracking Program

Finally, I would like to turn to the Treasury Department's Terrorist Finance Tracking Program (TFTP), a crucial international mechanism in countering illicit finance and transnational terrorism.

As I am sure many of you know, recently the European Parliament voted down an agreement between the United States and the European Union that was designed to continue the flow of critical data to the TFTP, on an interim basis, while a long-term agreement was negotiated. This very disappointing development has created a gap in our ability to track the financial transactions of terrorist suspects around the world. Since the beginning of this year, we have not been able to use the TFTP to its full potential to protect our citizens here in the United States and in Europe because we no longer receive information that is now stored only in Europe.

I would like to describe the program's origins, operations, robust privacy protections, and exceptional value as a counterterrorism tool, because I have seen that when we "demystify" the TFTP, we assuage concerns—whether in Europe or here at home—about the value and necessity of this program, and the effectiveness of its privacy safeguards.

In the aftermath of the terrorist attacks on September 11, 2001, the Treasury Department determined it was critical to make use of the financial information left behind when terrorists and their financial supporters conduct international funds transfers, and to add this financial data to the overall mix of information collected to help identify terrorist threats.

The result was the Terrorist Finance Tracking Program. Under the TFTP, the Treasury Department obtains, by administrative subpoena, a limited set of international funds transfer message data from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), an international bank-to-bank payment messaging system. Over the years, the Treasury Department has refined and narrowed the scope of its request, ensuring that the subpoena is focused as narrowly as possible on information necessary to combat terrorism.

From the outset, we recognized that even with a narrowly tailored subpoena, it was important to put procedures and safeguards in place to ensure the data obtained was being accessed only for counterterrorism purposes and that its confidentiality was maintained.

Privacy protections in the program specify that the data in the TFTP may only be searched in connection with a specific counterterrorism investigation, and not for any other law enforcement, national security, or other purpose. In fact, the TFTP data can be searched only if an independent basis exists to believe that the subject of a search is connected to terrorism or its financing. This independent evidentiary predicate must exist—and must be recorded—before any search in the TFTP data is conducted.

Privacy protections in the program specify that the data in the TFTP may only be searched in connection with a specific counterterrorism investigation, and not for any other law enforcement, national security, or other purpose.

The TFTP cannot be used for data mining. This point is critically important. No data mining of any kind has ever been permitted in the TFTP. There is no algorithmic or automated profiling. And there is absolutely no use of the TFTP for commercial or competitive purposes. It is—and always has been—purely and exclusively a counterterrorism tool.

To verify the TFTP's robust safeguards, an independent auditor reviews the program's physical security, ensures proper procedures are implemented, and confirms that no data mining occurs.

The privacy protections already embedded in the TFTP were enhanced even further when the Treasury Department, in late 2006, made a series of public commitments to the European Union concerning the processing of personal data in the TFTP. In these commitments, we reiterated that the TFTP would be used only for fighting terrorism and that no data mining of any kind would ever occur. These commitments further ensured that European citizens' personal financial data was protected, while at the same time preserving the utility of the TFTP in combating terrorism.

To provide further comfort to the Europeans, the United States also permitted a noted French counterterrorism expert, Judge Jean-Louis Bruguière, to review the TFTP on behalf of the EU, and offered him unprecedented access to the program.

In late 2008, Judge Bruguière issued a report in which he reached two critical conclusions. First, he found that the Treasury Department had implemented significant and effective controls and safeguards that ensure the protection of

personal data. Second, he reported that the TFTP generated significant value, in particular for countries in the EU, where over 1,300 TFTP-derived leads concerning specific terrorist threats had been shared with member states. Judge Bruguière reiterated both of these conclusions in a second report on the TFTP, which he issued in early 2010.

Judge Bruguière conclusion that the TFTP is an extremely effective counterterrorism investigative tool—not only for the United States but for Europe as well—is emphatically true. TFTP-generated leads have aided thousands of investigations, here and abroad, by providing law-enforcement and counterterrorism officials with information that helps them follow the money to the violent extremists who are dead set on doing us harm. This is the stuff of everyday, nose-to-the-grindstone work that protects our mutual security in often imperceptible, but nonetheless consequential, ways.

Let me offer some examples: TFTP-generated leads have assisted in the investigations of the 2002 Bali bombings; the Van Gogh murder in the Netherlands in 2004; the plan to attack John F. Kennedy Airport in 2007; the Islamic Jihad Union plot to attack Germany that same year; the Mumbai attacks in 2008; and the Jakarta hotel attacks in 2009.

Information gleaned from the TFTP has been used productively in investigations of several al-Qaeda-linked terrorist attacks, including the 2004 Madrid train bombings and the 2005 bombings in the London Underground.

As of today, we have shared over 1,550 TFTP-generated reports with our European colleagues.

Results from searches of TFTP data have also aided investigations that have disrupted several planned al-Qaeda plots. For example, we passed results from TFTP searches to European governments during their 2006 investigation into the al-Qaeda-directed plot to attack transatlantic airline flights between the UK and the United States. The plot was foiled, and in mid-September 2009, three individuals were convicted for their involvement; each was sentenced to at least thirty years in prison.

To take another example, in October 2008, eight individuals were arrested in Spain for their suspected involvement with al-Qaeda. European partners provided us information outlining these individuals' suspected connection to terrorism, and TFTP information clarified connections between the targets and other individuals in Spain, Morocco, and the Netherlands. Many of those arrested are now serving jail time.

As of today, we have shared over 1,550 TFTP-generated reports with our European colleagues. But despite the enormous value of this program, and the robust data-privacy protections built into it, the continued operation of the TFTP is in doubt.

In early 2010, SWIFT moved a large portion of data critical to the program to a new storage location in Europe. In anticipation of this change in the SWIFT network's architecture, in mid-2009 the Treasury Department and the European Commission started negotiations to ensure that the United States would continue to have access to the full scope of SWIFT data for the TFTP.

We reached an interim agreement in late November 2009, and the agreement was put before the European Parliament for ratification. The debate was quite vigorous, and despite our efforts to allay concerns over both process and

substance, in early February, the European Parliament voted not to give its consent to the interim agreement.

We now find ourselves in a worrisome situation. The interim agreement would have ensured our continued access to SWIFT data that is now stored only in Europe. Because the interim agreement was rejected, however, this critical data has not been provided to us since the beginning of this year. Each day we go without it, we run the very real risk that information crucial to preventing an attack—the kind of information the TFTP produces—is not available to U.S. and EU authorities.

Notwithstanding the European Parliament's action earlier this year, we are hopeful that we will be able to negotiate a long-term agreement with the European Union that both we and the European Parliament will find acceptable. As we work to address the issues and concerns that have been voiced in Europe, it is crucial that the core functionality of the TFTP be maintained. We are confident that this can be achieved. Indeed, press reports indicate that just a few days ago, the European Commission proposed a negotiating mandate for a long-term agreement that will provide European negotiators with sufficient negotiating flexibility.

For our part, the United States stands ready to negotiate an agreement that ensures the long-term operation of this crucial tool that has provided valuable, actionable information not only for the United States but for jurisdictions around the globe as we seek to identify, disrupt, and prevent terrorist activity. As our European counterparts understand, this is a security responsibility we owe to every citizen—in the United States, in Europe, and around the world.

There is, of course, much we can do through the exercise of our own authorities to combat terrorism and terrorist financing, and we at TFI will continue to aggressively employ our own tools against al-Qaeda, the Taliban, Hamas, Hizballah, and other violent extremists that threaten our security.

Nonetheless, we also recognize that our efforts to combat terrorism and terrorist financing are substantially augmented by effective international mechanisms, including the UNSCR 1267 terrorist-designation process, the FATF's campaign to enhance global AML/CFT compliance, and the Terrorist Finance Tracking Program. For these mechanisms to operate as effectively as possible, it is crucial that we obtain the collaboration and cooperation of a broad array of international actors. We at the Treasury Department, along with our colleagues across the national security community, work daily to foster this cooperation and, in doing so, help protect Americans, as well as others around the world, from the threat of terrorist attacks. It is tremendously rewarding work, and I appreciate the opportunity to describe it to you this afternoon.

Thank you.

But despite the enormous value of this program, and the robust data-privacy protections built into it, the continued operation of the TFTP is in doubt.

# Disrupting Iran's Illicit Activities

*Steven Pelak*

March 23, 2010
Rapporteur's Summary


■ *Steven Pelak, national coordinator for export enforcement, Justice Department*

In recent weeks, calls for additional sanctions against Iran and increased prosecutions of violators have highlighted the need for effective enforcement mechanisms. Although enhanced sanctions may be valuable, they will have little effect if there is no penalty for violations. As part of its effort to reinforce sanctions regulations and ensure that U.S. national-security interests are preserved, the Justice Department has sought to disable Iranian procurement networks that may involve U.S. companies, citizens, or goods.

## The Threat

The threat posed by Iran's procurement networks is clear: for example, a foreign agent can acquire weapons parts from a U.S. company, illegally transport them overseas through a third country to Iran, and pass them on to an operative in Iraq, who can then use them to create an improvised explosive device (IED) that kills American soldiers. The Justice Department has the authority to prosecute participants in such networks when American entities or goods are involved, even though large portions of these networks are located outside the United States. In many cases, prosecutors target individuals who cause an American company to be involved (at times unwittingly) in an illicit transaction. Some have accused the United States of acting extraterritorially in these types of cases, but this criticism lacks merit—there is a U.S. angle in every prosecution because they all involve American citizens, goods, or both.

Many individuals involved in procurement networks are motivated not by a specific political allegiance or ideology, but by money. For example, Asher Karni, an Israeli national working in South Africa, procured hundreds of triggered spark gaps for Pakistan. These high-energy power switches are dual-use goods, playing an integral role in both medical devices and nuclear weapons. Yet even as he worked for the Pakistanis, Karni also helped India obtain weapons testing equipment. He later pleaded guilty to these charges after being arrested during a skiing vacation in the United States.

In another case, Amir Hossein Ardebili conspired to procure radar and fighter-aircraft components for Iran in clear violation of U.S. export-control laws. He pleaded guilty after being extradited to the United States from Georgia,

where he was caught in a sting operation. It has since become clear that Ardebili was motivated more by greed than by any ideological allegiances.

## Export-Control Initiative

The Justice Department's Export-Control Initiative has helped increase the government's focus on enforcement. Under this measure, the department works closely in targeting illicit procurement networks with a number of agencies, such as the Federal Bureau of Investigation, the Bureau of Industry and Security, Immigration and Customs Enforcement, the Defense and Naval Criminal Investigative Services, and the Air Force Office of Special Investigations.

The initiative also includes an education and training program for prosecutors and investigators throughout the country. More than a thousand federal officers have already received such training, along with numerous federal prosecutors and analysts. In addition, the department provides advice and counsel to other agencies, departments, and local law-enforcement offices that request it. Overall, the initiative has improved coordination among such agencies as well as cooperation with the intelligence community.

Regarding prosecutions, the initiative has paid major dividends, resulting in an approximate 30 percent increase in successful cases. The variety of cases has also widened, though prosecutions involving Iran and China remain the top priority.

Other countries have improved their export-control laws as well. For example, the United Arab Emirates enacted new legislation on this front in 2007, and the United States continues to work with authorities there to ensure effective implementation. Similarly, Malaysia will be enacting such legislation in the near future. The number of export-control-related international task forces has also increased—a sign that additional countries are taking the issue seriously.

## Disrupting and Prosecuting Iranian Procurement

A number of agencies are involved in enforcing sanctions against Iran, each playing a different role. While the Justice Department takes the lead on prosecutions, for example, the Treasury Department handles licensing decisions. The intelligence community plays a critical part as well, of course. Disrupting procurement activity requires coordination with intelligence agencies in order to identify the individuals and broader networks involved. Intelligence can also help law enforcement agencies interdict illegal exports before they leave the United States, lure targets to locations for arrest, and subsequently exploit these targets' communications.

Foreign law-enforcement and intelligence agencies can help U.S. authorities identify and disrupt illicit procurement networks as well. For example, they helped uncover illegal exports by Aviation Services International (ASI), a small Dutch company that ordered goods from multiple American companies, shipped them through third countries, and ultimately transported them to Iran for military purposes. Foreign law enforcement provided the U.S. government with evidence that ASI, under the direction of Robert Kraaipoel, had shipped military-aircraft parts and unmanned-aerial-vehicle components to Iran for more than ten years. Foreign officers subsequently detained

Many individuals involved in procurement networks are motivated not by a specific political allegiance or ideology, but by money.

shipments and requested statements of proof regarding their destination. ASI provided false documentation and was ultimately indicted (originally under seal) in 2007.

When the charge was unsealed, no bank would hold Kraaipoel's money other than Iran's Bank Melli (now designated by the United States for its role in Tehran's weapons-of-mass-destruction activities). In addition, the U.S. Department of Commerce added him to its "denied party" list, which barred him from obtaining any goods with U.S. components. Within forty-eight hours of the charge becoming public, Kraaipoel had agreed to plead guilty to conspiracy under the U.S. International Emergency Economic Powers Act. Even more important, he provided a Rolodex of his customers' names, leading to numerous other investigations and enabling U.S. authorities to more effectively target the broader network.

Ironically, America's strong rule of law actually encourages Iranian procurement networks to seek out U.S. goods despite the risk of detection.

## Conclusion

For the foreseeable future, U.S. export-control enforcement will continue to focus on Iran and China, devoting extra attention to banks and other components of procurement networks such as freight forwarders. Interagency cooperation and a strong system of relevant U.S. law are the two most valuable resources at the Justice Department's disposal. Sharing information and resources with agencies to create reciprocal relationships allows for more successful prosecutions of violators. And the department's efforts in this arena ensure that sanctions against Iran and other countries are enforced and ultimately support U.S. national-security efforts.

Ironically, America's strong rule of law actually encourages Iranian procurement networks to seek out U.S. goods despite the risk of detection. That is, American goods tend to be higher quality because manufacturers know that they will be held accountable for defects and other problems. In turn, Iranian operatives know that if they purchase an electronic component for an IED from the United States, it will be more likely to work. By identifying and disrupting such procurement efforts, the Justice Department is helping the United States and its warfighters gain an important edge on the battlefield and beyond.

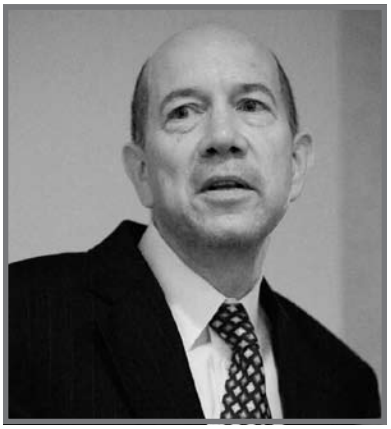
# The Escalating Ties between Middle East Terrorist Groups and Criminal Activity

*David T. Johnson*

January 19, 2010
Prepared Remarks

Good afternoon. I want to thank Dr. Robert Satloff for his invitation to speak to you today.

It is a pleasure to be here with this distinguished group, and to contribute to The Washington Institute's series on these important issues. I would also like to applaud the Stein Program on Counterterrorism and Intelligence for advancing our understanding of the links between crime and terrorism and the risks those links can pose to America's national security interests.



■ *David T. Johnson, assistant secretary of state, Bureau of International Narcotics and Law Enforcement Affairs*

## Dangerous Alliances in the Crime-Terror Continuum

While our discussion today will focus on Middle East terrorist groups' links to criminal activity, it is important to bear in mind that the threat of terror and the origins of terrorist groups span beyond any single region. Moreover, terrorist groups' links to criminal activity are not new phenomena. In the 1970s and 1980s, for example, groups like the Red Army Faction, the Red Brigades, and the domestic Symbionese Liberation Army financed violent terrorism with violent crimes like bank robbery.

In recent years, many of these groups have focused almost exclusively on using narcotics as a means to finance their activities. As the international community clamped down on state-sponsored terrorism and pressured governments from financially supporting terrorist organizations, many groups resorted to drug trafficking and other illicit activities as sources of revenue. According to the U.S. Drug Enforcement Administration, nineteen of the forty-four groups that the U.S. government has designated as Foreign Terrorist Organizations (FTOs) participate in the illegal drug trade and many also engage in financial and other forms of crime.

Today, we look at organizations as diverse as Hizballah, al-Qaeda, the Revolutionary Armed Forces of Colombia (FARC), the Taliban in Afghanistan, the Kurdistan Workers Party (PKK), and the Liberation Tigers of Tamil Eelam (Sri Lanka), all of which engage or have engaged in criminal activities as a vehicle to finance their terrorist (or violent political) activities.

In places like West Africa, we now see how increased drug flows from Latin America, kidnappings, and other crimes produce opportunities for criminal groups that might sympathize with al-Qaeda to tap into the wealth generated

by narcotics trafficking and other illicit activities to fund their operations. Last month, for example, U.S. prosecutors in the Southern District of New York charged three men who claimed to be al-Qaeda associates with conspiracy to smuggle cocaine through Africa. In Afghanistan, we have long known that among the Taliban's funding sources were informal taxes on heroin traffickers. Two years ago, U.S. and Colombian investigators were able to dismantle an international cocaine-smuggling and money-laundering gang that funneled some of its profits to Hizballah, a U.S.-designated Foreign Terrorist Organization. In the Horn of Africa, we are seeing illicit routes established by criminal groups to smuggle immigrants, arms, narcotics, and other contraband, and know these illicit activities will create opportunities for terrorist groups to exploit.

We also remain concerned about the crime-terror links in an increasing number of ungoverned or insufficiently governed spaces, such as Yemen and the Sahel belt, where insecurity and other destabilizing factors provide opportunities for illicit networks to thrive and find safe haven—and as possible staging platforms to project their terror campaigns abroad. For example, in the Tri-Border Area, along the loosely controlled region that borders Paraguay, Brazil, and Argentina, individuals with apparent connections to radical Islamic groups have been active in drug trafficking, money laundering, intellectual-property-rights piracy, alien smuggling, and arms trafficking.

These are very serious issues, but you may ask why these issues are becoming national security priorities for the United States now.

Violent criminal and terrorist networks threaten the security, economic health, and social fabric of all nations.

## Threats to U.S. National Security

Violent criminal and terrorist networks threaten the security, economic health, and social fabric of all nations. These transnational threat networks imperil public trust and core democratic and market values, especially in the midst of the most serious global economic and financial crisis in decades. Criminal entrepreneurs who smuggle billions of dollars of illegal goods across borders—drugs, arms, humans, natural resources and endangered wildlife parts, counterfeit medicines, and pirated software, as well as embezzled public funds—create insecurity, cost our economies jobs and tax revenue, endanger the welfare and safety of our families and communities, and overwhelm law enforcement countermeasures. Similarly, terrorist groups create great insecurity by the acts of cowardice and the killing of thousands of innocent people to advance their political and ideological objectives. They do not respect traditional borders or nation-states, and they exploit ungoverned and undergoverned areas as places for safe haven—as places to rest, to recruit, to train, and to plan their operations. In many places, these networks become the de facto government.

## Corruption, Crime, and Terrorism: The Unholy Trinity

Poor governance and corrupt officials in many parts of the world enable criminals, insurgents, and terrorists to operate with impunity. Criminal syndicates have long supported terrorist groups—for both ideological and economic reasons—by facilitating their transborder movements, weapons smuggling, and providing forged documents. At the same time, terrorist groups also resort to organized crime to finance their activities, including through drug dealing.

Such terrorist-criminal cooperation is of particular concern, especially because some of these criminal syndicates have the organizational and financial wherewithal that could potentially allow them to acquire and sell radioactive materials, chemical and biological weapons, or technologies used for weapons of mass destruction. This financial strength makes it much more difficult for governments to shut off the spigot used to finance terrorism, at least through traditional means that focus on deterring exploitation of the formal banking system. As terrorist groups move toward mimicking the tactics of organized crime, our international response will need to incorporate more creative law-enforcement tools that go well beyond effective regulation of financial transactions.

The question is frequently raised as to why criminals would want to assist terrorist groups. While it is possible that criminals may not want the extra attention from states' national security institutions that will come from associating with terrorists, some may nevertheless find the financial temptation too great. Others may not care with whom they conspire, as long as they are paid for the increased risk of detection they assume when cooperating with known terrorist groups. For example, reports indicate that some charge extra for dealing with certain nationalities and others more for "special services." And some criminals may have no idea who their clients really are. These people are undoubtedly clever, but they may nevertheless be more greedy than smart.

A convergence of crime and corruption can also pave the road for terrorist organizations to finance their [acts of] terror, as was the case in Bali, Madrid, and Mumbai. In particular, terrorist financiers are not only concealing their financing assets through complex transactions in the formal banking system but also harnessing centuries-old money-laundering tactics. They exploit informal value-transfer mechanisms such as *hawala* (or *hundi*) and trade-based money laundering, and use illegal cash couriers as bulk-cash smugglers, particularly in countries with nonexistent or weak anti-money-laundering enforcement practices.

A convergence of crime and corruption can also pave the road for terrorist organizations to finance their acts of terror, as was the case in Bali, Madrid, and Mumbai.

## Smart Power and International Cooperation

So what is the U.S. Department of State doing to combat these transnational threat networks? The State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL), which I lead, is responsible for international counternarcotics and countercrime issues. We lead diplomatic efforts to raise awareness of the destabilizing impact of transnational organized crime and illicit activities, and we strengthen global efforts to combat these threats, including through enhanced law-enforcement cooperation, where organized crime and terrorism intersect. We are enhancing international cooperation to dismantle criminal networks and combat the threats that they pose—not only through law enforcement efforts but also by building up governance capacity, supporting committed reformers, and strengthening the ability of citizens to monitor public functions and hold leaders accountable for providing safety, effective public services, and efficient use of public resources.

In the Middle East and other parts of the world, the United States is working with partner governments to develop effective, democratic, civilian-led and

skilled law-enforcement and justice-sector institutions. Hamas and Hizballah continue to finance their terrorist activities mostly through the state sponsors of terrorism, Iran and Syria, and through various fundraising networks in Europe, the United States, and the Middle East. The funds channeled to these organizations frequently pass through major international financial capitals, such as Dubai, Bahrain, Hong Kong, Zurich, London, or New York. Hizballah also continues to profit from the drug-trafficking groups in the Beqa Valley of Lebanon.

In response, the United States is helping to strengthen the anti-money-laundering and counterterrorist-finance programs of partner countries that aim to detect, disrupt, and dismantle these illicit activities. In Palestine, and Gaza, besides being responsible for hundreds of rocket, mortar, and small-arms attacks into Israel, Hamas and other armed groups have engaged in tunneling activity and smuggled weapons, cash, and other contraband into Gaza. In the West Bank, the United States helps to support the Palestinian Authority (PA) security forces to establish law and order and fight terrorist cells by helping to build capacity to administer criminal justice institutions. The United States has also helped train thousands of members of the Palestinian security forces at Jordan's International Police Training Center, who can then be deployed by the PA to protect peace and stability in the West Bank. In Lebanon, a place I visited last week, we are partnering with the Lebanese government, and specifically with its Ministry of Interior, in an initiative to train the next generation of Internal Security Forces officers. Our objective is clear: to support the development of professional institutions under the Ministry of Interior that can provide security and vital services to the Lebanese people.

In Iraq, criminal insurgencies have profited from the illicit trade of siphoned oil.

In Iraq, criminal insurgencies have profited from the illicit trade of siphoned oil. The United States is working to target and dismantle these illicit networks as part of our broader counterinsurgency effort. We continue to support reconstruction and stabilization by helping to develop an Iraqi criminal justice system that is sufficiently fair and effective that the Iraqi people have confidence in that system and turn to it rather than extrajudicial groups and militias to resolve disputes and seek justice. We also support rule-of-law programs that focus on judicial security, capacity building for judges, prosecutors, investigators, and court administrators, and integration of the various components of the justice system. We are also working with Iraq on legislation to reform its criminal codes, and continue to support the FBI-led Major Crimes Task Force.

In Afghanistan, where we have long focused on combating narcotics trafficking and the revenue stream that creates for the Taliban, we are also working with our military colleagues to develop criminal justice institutions by giving Afghans the necessary training, equipment, infrastructure, institutional capacity, and organizational structure to provide the rule of law and combat crime.

In Yemen, we recently completed a judicial and law-enforcement assessment. Based on that, we aim to undertake targeted assistance to the government of Yemen to strengthen its capacity to control the movement of people and goods through Yemen and across its borders.

In West Africa, over the next three years, INL aims to strengthen criminal justice institutions such as the police, prosecutors, and the courts to successfully

investigate, prosecute, and incarcerate transnational criminals, networks, and organizations. Right now, we are considering how best to support Kenya and other partner nations in the Horn of Africa to prosecute and incarcerate those apprehended for piracy. At the same time, though, we and others at the State Department are focused on the longer-term solution to the piracy question—political stability, restoring the rule of law, and supporting economic opportunity in the Horn of Africa.

In Indonesia, INL has worked closely and successfully with the National Police for many years, and our investment is paying off. The first police units that responded to the July 2009 attacks on the Marriott and Ritz-Carlton hotels in Jakarta were trained through INL programs. The unit that ultimately brought down the mastermind behind those bombings, Noordin Top, was also trained and worked closely with us for many years. Noordin had ties to Jemah Islamiyah as well as to al-Qaeda.

In Indonesia, INL has worked closely and successfully with the National Police for many years, and our investment is paying off.

The United States is also committed to working with others to strengthen law-enforcement cooperation in combating transnational threats, including dismantling illicit networks and prosecuting high-level corrupt officials to disrupt the convergence of various threat networks. On numerous occasions, President Barack Obama and Secretary of State Hillary Clinton have highlighted the threat of high-level corruption, and we are working to strengthen the tools we have to combat and deter corruption and to use those tools more effectively.

International legal and political cooperation is essential to prevent, investigate, prosecute, and punish serious crimes as well as to break up terrorist networks, to eliminate safe havens, and to disrupt those activities that support terrorist organizations. Our efforts are aimed not only at the murderous acts terrorists perpetrate but also at their funding, their travel, their communications, their recruitment, and their intelligence and information collection.

With our international partners, we encourage others to implement the UN Convention against Transnational Organized Crime (and its protocols) and the UN Convention against Corruption. These international instruments, built on the foundation of the three UN counterdrug conventions, create a broad legal framework for mutual legal assistance, extradition, and law-enforcement cooperation. Additionally, the United States supports implementation of UN Security Council (UNSC) Resolution 1373, and other UNSC resolutions and UN legal instruments, to combat terrorism.

## Fighting Networks with Networks

Beyond the United Nations, my colleagues and I in the Bureau of International Narcotics and Law Enforcement Affairs also work through the G-8, the European Union, Interpol, and the Financial Action Task Force, along with its regional subgroups—APEC [Asia-Pacific Economic Cooperation] as well as other regional forums. Through these groups, we set international counterdrug and anticrime standards, take steps that close off safe havens to criminal and terrorist groups, pool skills and resources, and improve cross-border cooperation. For example, at last year's G-8 summit in L'Aquila, Italy, leaders expressed concern about the converging threats of terrorism, drugs, and organized crime, and

Our enemies will continue to use all available means to sustain their agenda.

agreed to strengthen international cooperation and capacities to prevent international criminal networks, kleptocrats, and terrorists from corrupting public institutions to advance their goals. Additionally, the United States is working with Interpol and other multilateral partners to strengthen interregional law-enforcement efforts to combat transnational threats in a coordinated manner across the Pacific and Atlantic.

As the world witnessed this past Christmas Day when a terrorist attempted to blow up a commercial airliner, al-Qaeda remains keen to harm Americans and others around the world. Our enemies will continue to use all available means to sustain their agenda. As already noted, in places such as Afghanistan, Southeast Asia, West Africa, Somalia, and Yemen, illicit networks, trafficking in everything from weapons to drugs, are making it easier for al-Qaeda and other terrorist groups to fund their campaigns. As a recently captured Taliban [operative] underscored: "Whether it is by opium or by shooting, this is our common goal [to harm all infidels as part of jihad]."

Faced with these challenges, we must continue to take more effective steps to understand our adversaries and to strengthen our capabilities to deter, disrupt, and dismantle transnational threat networks—not only at the end of their efforts, when they carry out acts of violence, but at every step along the way.

# The Washington Institute

*Board of Directors and Advisors*

THE
WASHINGTON INSTITUTE
*for Near East Policy*

1828 L Street NW, Suite 1050 ■ Washington, DC 20036 ■ www.washingtoninstitute.org