

THE CONVERGENCE OF
CRIME AND TERROR:
Law Enforcement
Opportunities and Perils

Daveed Gartenstein-Ross
Senior Fellow
Foundation for Defense of Democracies

Kyle Dabruzzi
Terrorism Analyst
Gartenstein-Ross Group



The Convergence of Crime and Terror: Law Enforcement Opportunities and Perils provides an analysis of the increasingly important link between traditional criminal activities and terrorism. By cataloging a number of relevant cases, the authors have illustrated that terrorists routinely resort to “traditional” crimes, from drug trafficking to financial scams, to further their objectives.

As a result, terror prosecutions must find inspiration from historical government efforts to arrest, prosecute, and incarcerate notorious violent criminals such as Al Capone on relatively minor charges such as tax evasion. The aggressive prosecution of such relatively minor offenses can serve to disrupt grander malevolent schemes.

As the authors suggest, the rise of terrorism means that the traditional, reactive law enforcement model must change. We cannot afford to wait until after a successful terrorist attack occurs to investigate and prosecute. The examples from Europe included in this paper provide a sobering explanation for why that is so. Law enforcement officials must consider disruptive investigations and prosecutions that may not ultimately lead to a criminal trial on terrorism charges but that will stop potential terror plots before they are put into motion.

We face a decentralized, networked, and self-sufficient enemy. Independent cells are increasingly purchasing that self-sufficiency with the proceeds of criminal enterprises. This hard reality provides yet another justification for transforming state and local first responders into first *preventers* of crime and terror.

The Center for Policing Terrorism thanks Daveed Gartenstein-Ross and Kyle Dabruzzi for making the case in this paper for prevention-oriented, intelligence-led policing.

Timothy P. Connors
Director, Center for Policing Terrorism
tconnors@manhattan-institute.org

ABOUT THE AUTHORS

DAVEED GARTENSTEIN-ROSS is a senior fellow at the Foundation for Defense of Democracies and director of its Project on Religion, Politics, and Radicalism. Gartenstein-Ross also consults for a number of clients on issues of terrorism and Islamic extremism, including the Manhattan Institute's Center for Policing Terrorism, the Christian Broadcasting Network, and law enforcement.

Born into a Jewish family, Gartenstein-Ross converted to Islam in his early twenties and worked for the head U.S. office of the Al Haramain Islamic Foundation, an international Wahhabi charity that was a major al-Qaeda financier. Prior to 9/11, Gartenstein-Ross left the Islamic faith for Christianity. By the time the FBI raided the Al Haramain offices where he had worked, he was ready to assist the investigation. This experience is detailed in his book *My Year Inside Radical Islam*.

Gartenstein-Ross has testified before the U.S. Senate's Homeland Security and Governmental Affairs Committee, discussing religious radicalization in prisons. He frequently writes on the global war on terror, including for such publications as *Reader's Digest*, the *Wall Street Journal Europe*, *The Middle East Quarterly*, *Commentary*, *The Weekly Standard*, the *Washington Times*, and the *Dallas Morning News*. He also frequently appears as an analyst to discuss these issues on national television and talk radio.

Previous positions that Gartenstein-Ross has held include commercial litigator at Boies, Schiller & Flexner and law clerk on the United States Court of Appeals for the D.C. Circuit. He received a law degree from the New York University School of Law and a B.A. from Wake Forest University.

KYLE DABRUZZI is a terrorism analyst at the Gartenstein-Ross Group. His contributions to the firm's projects include producing training PowerPoints for law enforcement and providing analysis to the firm's clients. He has written for such publications as *The Middle East Quarterly* and *The Daily Standard*, and he is coauthor of two forthcoming book chapters. Dabruzzo is also a frequent contributor to ThreatsWatch, a web-based publication of the Center for Threat Awareness.

Dabruzzo received a B.A. in political science with a minor in Middle East and South Asian politics from Wake Forest University in 2006. While at Wake Forest, he conducted research for a former FBI hostage negotiator on the communicative aspects of threats made during hostage crises.

CONTENTS

- 1 **Introduction**
- 2 **Drug Trafficking**
 - Hizballah
 - Al-Qaeda
 - The Madrid Cell
- 5 **Financial Scams**
 - Identity Theft
 - Bank Fraud
 - Cigarette Smuggling
 - Counterfeiting
- 8 **Cyber-Crime**
- 9 **Illegal Money Transfers**
 - Benevolence International Foundation
 - The Holy Land Foundation
 - Al Haramain Islamic Foundation
 - Hizballah
- 12 **Immigration Violations**
 - Document Fraud
 - Sham Marriages
- 14 **Implications of the Al Capone Model**
 - The British Experience
 - Critics of the Al Capone Model
- 16 **Conclusion**
- 18 **Endnotes**

THE CONVERGENCE OF CRIME AND TERROR: LAW ENFORCEMENT OPPORTUNITIES AND PERILS

Daveed Gartenstein-Ross & Kyle Dabruzzi

INTRODUCTION

The Soviet Union was a major terrorist sponsor during the Cold War. When the USSR collapsed, terrorist groups were forced to look elsewhere financially, and many turned to criminal activities. Some fifteen years later, terrorist groups that are not state-sponsored pose the greatest threat to the United States.¹ Consistent with post-Cold War trends, these groups have become heavily involved in criminal activities. (While this paper discusses a number of federal criminal statutes, state criminal laws also are applicable; we use federal law as a vehicle for discourse as a matter of convenience.)

Terrorist involvement in criminal activity has two strategically significant aspects. First, it allows terrorists to gain financially while at the same time damaging the societies they target. Terrorists, always on the lookout for new ways to fund their violent activities, find important sources of revenue in criminal enterprises. Close scrutiny of jihadist terrorism since 9/11 demonstrates that these groups are often funded through the drug trade, money-laundering schemes, and a variety of financial scams that range from the simple to the highly complex. Terrorists also use other illegal activities, such as document fraud and sham marriages, to facilitate their operational objectives.

A second strategic aspect is that law enforcement can derive some advantage from the crime-terrorism nexus. A comprehensive law

enforcement model for counterterrorism has echoes of the approach used to fight the mob in the early to mid-twentieth century. This approach was typified by the prosecution of Al Capone, who in 1931 was the country's first celebrity criminal.² Everybody knew what Capone was up to: his litany of offenses included murder, bribery, and running illegal breweries. But the government would have had trouble proving Capone's guilt beyond a reasonable doubt for his most notorious activities. Instead, he was charged with tax evasion, prompting the incredulous mobster to say, "The government can't collect legal taxes from illegal money."³ Capone proved to be wrong, and he entered an Atlanta prison on May 5, 1932.

Shortly after 9/11, then-attorney general John Ashcroft recommended that a similar disruptive approach be used against suspected terrorists:

Attorney General [Robert] Kennedy made no apologies for using all of the available resources in the law to disrupt and dismantle organized crime networks. Very often, prosecutors were aggressive, using obscure statutes to arrest and detain suspected mobsters. One racketeer and his father were indicted for lying on a federal home loan application. A former gunman for the Capone mob was brought to court on a violation of the Migratory Bird Act. Agents found 563 game birds in his freezer—a mere 539 birds over the limit. . . .

The American people face a serious, immediate and ongoing threat from terrorism. At this moment, American service men and women are risking their lives to battle the enemy overseas. It falls to the men and women of justice and law enforcement to engage terrorism at home. History's judgment will be harsh—and the people's judgment will be sure—if we fail to use every available resource to prevent future terrorist attacks.

Robert Kennedy's Justice Department, it is said, would arrest mobsters for "spitting on the sidewalk" if it would help in the battle against organized crime. It has been and will be the policy of this Department of Justice to use the same aggressive arrest and detention tactics in the war on terror.

Let the terrorists among us be warned: If you overstay your visa—even by one day—we will arrest you. If you violate a local law, you will be put in jail and kept in custody as long as possible. We will use every available statute. We will seek every prosecutorial advantage. We will use all our weapons within the law and under the Constitution to protect life and enhance security for America.⁴

The Al Capone/mob model for combating suspected terrorists is not without its critics,⁵ but it is a sensible response to the threat that the country faces. Terrorists have killed more innocent Americans than the mob ever did,⁶ and if the next terrorist attack employs weapons of mass destruction, it could be even more devastating than 9/11.⁷

As with the mob, prosecutors often have difficulty proving involvement in terrorist acts beyond a reasonable doubt. But also as with the mob, as the government investigates an individual who is strongly suspected of terrorist ties, it often uncovers evidence of other crimes. As Ashcroft suggested, prosecutors have not hesitated to "use every available statute" against suspected terrorists.

The growing post-Cold War terrorist involvement in criminal enterprises has provided more opportunity for the government to prosecute suspected terrorists. From a law enforcement perspective, it is critical to minimize the advantage that terrorists gain from involvement in criminal activity and maximize the opportunity to prosecute them for the full range of illegal activities in which they engage. With this paradigm in mind, this paper explores five areas of criminal enterprise where there has been known terrorist involvement: drug trafficking, financial scams, cyber-crime, illegal money transfers, and immigration violations.

DRUG TRAFFICKING

Terrorist groups have derived a great deal of profit from the illegal drug trade. As U.S. *News & World Report* has stated, "Nearly half of the 41 groups on the government's list of terrorist organizations are tied to narcotics trafficking, according to DEA [Drug Enforcement Agency] statistics."⁸

Terrorist involvement in drug trafficking began with the collapse of the Soviet Union, as groups that lost their major state sponsor were forced to look for alternative funding sources. One such source proved to be the drug trade. Moreover, the fall of the Soviet Union coincided with the rise of globalization, which is characterized by instantaneous connectivity. This connectivity has helped to facilitate terrorist involvement in drug trafficking, as explained by Steven W. Casteel, the DEA's assistant administrator for intelligence:

Globalization has dramatically changed the face of both legitimate and illegitimate enterprise. Criminals, by exploiting advances in technology, finance, communications, and transportation in pursuit of their illegal endeavors, have become criminal entrepreneurs. Perhaps the most alarming aspect of this "entrepreneurial" style of crime is the intricate manner in which drugs and terrorism may be intermingled. Not only is the proliferation of illegal drugs perceived as a danger, but the proceeds from the sale of drugs provides a ready source for funding of other criminal activities, including terrorism.⁹

The term "narco-terrorism"—which has acquired at least a dozen definitions over the years¹⁰—attempts to characterize the use of drug shipments as a means of financing terrorist organizations. The DEA defines a narco-terrorist organization as "an organized group that is complicit in the activities of drug trafficking in order to further, or fund, premeditated, politically motivated violence perpetrated against non-combatant targets with the intention to influence [that is, influence a government or a group of people]."¹¹ While some other definitions of narco-terrorism focus more on the actions of the drug traffickers themselves,¹² the DEA's definition perfectly fits the activities described in this section. Islamic terror groups that have been involved in the drug trade include Hizballah, al-Qaeda, and the cell responsible for the 3/11 train bombings in Madrid, Spain.

■ Hizballah

Hizballah is a Shia terrorist group that first reached the public's attention in October 1983 with a suicide

bombing attack against a Marine barracks in Beirut, Lebanon, that killed 241 American servicemen.¹³ With this single attack, Hizballah killed more Americans than any other terrorist group did until 9/11. Although it is unclear how much money Hizballah derives from drug trafficking, there are at least three known cases of proceeds from the U.S. drug trade being sent to this group.¹⁴

In January 2002, the federal investigation dubbed "Operation Mountain Express III" culminated in a series of raids that took place on a single day in Chicago, Cleveland, Detroit, Fresno, Las Vegas, Los Angeles, Phoenix, Riverside, San Diego, and Carlsbad.¹⁵ The raids resulted in charges against 136 people and the seizure of "nearly 36 tons of pseudoephedrine, 179 pounds of methamphetamine, \$4.5 million in cash, eight real estate properties and 160 cars used by drug gangs."¹⁶ These raids were directed at a drug ring that had been smuggling pseudoephedrine tablets from Canada to such midwestern cities as Chicago and Detroit. (Pseudoephedrine is a key methamphetamine ingredient commonly found in allergy and cold medicines.) After being routed through these cities, the tablets were resold to Mexican-based traffickers.

Men of Middle Eastern descent ran this drug ring. In the wake of the operation, Asa Hutchinson, then the DEA's director, revealed that "[a] significant portion of some of the sales are sent to the Middle East to benefit terrorist organizations."¹⁷ Hutchinson specifically fingered Hizballah as one group that had benefited from pseudoephedrine trafficking,¹⁸ but DEA officials were quick to say that they didn't know exactly how much money had reached Hizballah or other terrorist groups.

Around the same time as Mountain Express III, federal investigators were also engaged in Operation Green Quest, "a multi-agency task force on terrorist financing designed to bring the Treasury's expertise to bear in 'identifying, disrupting, and dismantling the financial infrastructures and sources of terrorist funding.'"¹⁹ Green Quest likewise exposed instances of drug money being laundered in support of Hizballah.²⁰

A third case of Hizballah benefiting financially from the U.S. drug trade is centered on Ohio resident Mohammad Shabib. Steven Emerson, the executive director

of the Washington-based Investigative Project on Terrorism, summarized Shabib's case:

Beginning in the early 1990s, Shabib hauled about three tons of pseudoephedrine from Canada to California, where his colleagues sold the medicine to Mexican gangs that would turn it into the street drug methamphetamine. It is unclear exactly how much of this money went to finance terrorism, but Shabib's drug trade did contribute to Hizballah's financing.²¹

■ Al-Qaeda

Although there aren't many known instances of profits from the U.S. drug trade financing al-Qaeda, the U.S. market is only one part of the broader international drug trade. A large amount of drug trafficking occurs outside U.S. borders, and al-Qaeda is in an ideal position to benefit from the international drug trade because of its strong presence in Pakistan's North-West Frontier Province, which is adjacent to Afghanistan. Afghanistan lies at the center of the Golden Crescent, which is "a Central Asian version of Southeast Asia's infamous drug-supplying Golden Triangle."²² The country boasts a large number of poppy fields, and often these poppies are converted into opium or heroin.

Although drugs are forbidden within Islam and are particularly taboo in the puritanical strain of the faith that Osama bin Laden and al-Qaeda promote, the ends justify the means when it comes to the drug trade. One defense official told the *Washington Times*: "Bin Laden does not mind trafficking in drugs, even though it's against the teaching of Islam, because it's being used to kill Westerners."²³

An August 2004 article in *Time Asia* titled "Terrorism's Harvest" outlined al-Qaeda's involvement in the opium and heroin trade.²⁴ This involvement stretches back to the days when the Taliban ruled Afghanistan. A Western antinarcotics official told *Time Asia* that early in 2001, al-Qaeda's financial experts teamed up with top Afghan drug traffickers to persuade Taliban leader Mullah Omar to ban opium cultivation. Although this move initially appeared to combat the drug trade, it was actually self-serving: opium prices soared from \$30

a kilogram to almost \$650 after the ban, thus benefiting al-Qaeda and its trafficker allies who already had large stockpiles.

Reportedly, neither the Taliban nor al-Qaeda is involved in growing poppies. Instead, "[t]heir involvement is higher up the drug chain, where profits are fatter and so is their cut of the deal."²⁵ *Time Asia* reported on recent evidence of al-Qaeda's involvement:

[Mirwais] Yasini, the Afghan antidrug czar, says the terrorists receive a share of profits from heroin sales by supplying gunmen to protect labs and convoys. Recent busts have revealed evidence of al-Qaeda's ties to the trade. On New Year's Eve, a U.S. Navy vessel in the Arabian Sea stopped a small fishing boat that was carrying no fish. After a search, says a Western antinarcotics official, "they found several al-Qaeda guys sitting on a bale of drugs." In January, U.S. and Afghan agents raided a drug runner's house in Kabul and found a dozen or so satellite phones. The phones were passed to the CIA station in Kabul, which found they had been used to call numbers linked to suspected terrorists in Turkey, the Balkans and Western Europe. "It was an incredibly sophisticated network," says the official. In March U.S. troops searching a suspected terrorist hideout in Oruzgan province after a fire-fight found opium with an estimated street value of \$15 million.²⁶

Intelligence officials have stated that bin Laden profits from the drug trade because his allies regulate smuggling routes from Afghanistan into such countries as Iran, Pakistan, and Turkmenistan.²⁷ Essentially, they impose a tax on each shipment to allow it to pass. Intelligence community sources report that they don't know precisely how much money al-Qaeda derives from the drug trade, but "estimates are in the millions of dollars."²⁸

The Afghan drug trade is unlikely to abate on its own. Opium continues to fuel half of Afghanistan's economy, and there was only a 2% eradication of opium production in 2006.²⁹ Al-Qaeda will likely continue to be involved for two reasons. First, drug trafficking is seemingly a significant source of revenue. Second,

the drug trade helps to destabilize Afghan president Hamid Karzai's government. Since Karzai is unable to tax the illegal sale of drugs, the drug trade costs him money and influence.

Other terror groups allied with al-Qaeda have also been involved in the drug trade. The *Washington Times* notes, for example, that al-Qaeda's Southeast Asian ally Jemaah Islamiyah also profits from illegal narcotics trafficking.³⁰

■ The Madrid Cell

Terrorists have also benefited from the retail side of the drug business. In Madrid, ten explosions rocked four commuter trains during the height of rush hour on March 11, 2004. When the dust settled, 191 people were killed and there was also political fallout. A socialist government replaced Prime Minister Jose Maria Aznar's administration, which generally supported U.S. policies in the global war on terror. The new government promptly withdrew Spanish troops from Iraq.

One little-known aspect of the train bombings is that the Madrid cell received substantial financing from the sale of drugs, something that the cell's ideologues justified "as a weapon of jihad."³¹ Sarhane Ben Abdelmajid Fakhret, believed to be the cell's ringleader, apparently thought—perhaps because of his theological mentors—that drug trafficking was acceptable if the profits were used to advance Islam. In fact, Jamal Ahmidan, a Moroccan drug dealer who helped finance the attacks, "traded a load of hashish for the dynamite that slaughtered 191 people."³²

Ahmidan was a street thug who was transformed into a jihadist while under detention in Spain.³³ Although he was known for fanaticism at the mosque he attended, Ahmidan would also routinely go to bars and discos. The *Los Angeles Times* reported that Ahmidan's neighbors thought of him as "friendly and flashy," and they "remember him zooming by on a motorcycle with his long-haired girlfriend, a Spanish woman with a taste for revealing outfits."³⁴ The *Los Angeles Times* went on to describe how critical drug traffickers were to the 3/11 plot:

The traffickers took charge of obtaining money, weapons, phones, cars, safe houses and other infrastructure. Ahmidan rented a rickety rural cottage [on] . . . Jan. 28, turning it into a headquarters and bomb factory. He enlisted Spanish jailhouse contacts to arrange the exchange of 66 pounds of hashish for 220 pounds of dynamite stolen from a mine in the Asturias region in late February.³⁵

The Madrid cell is not the only example of Islamic terror groups in Europe funding themselves through drug trafficking. An Italian prosecutor alleged that a member of the Neapolitan Mafia converted to Islam and set up an exchange of arms for drugs with Muslim terrorists.³⁶ Overall, it's clear that—despite Islam's edicts against drugs—terrorist groups have used drug trafficking to finance their activities.

FINANCIAL SCAMS

Terrorist groups and their backers have taken part in scores of financial scams—ranging from tax evasion to credit card fraud—within the United States. This section focuses on four major financial scams that terrorists have engaged in: identity theft, bank fraud, cigarette smuggling, and counterfeiting.

■ Identity Theft

Identity theft is possibly the most lucrative enterprise in which terrorists have engaged—and they get much more than money from this crime. Dennis Lormel, the chief of the FBI's Terrorism Financial Review Group, explained in testimony before the U.S. Senate that technological advances have made it easier than ever to commit identity theft.³⁷ Advances in computer hardware and software as well as the growth of the Internet have made it easier to obtain a target's personal information and produce the counterfeit documents necessary to steal someone's identity.

One critical aspect of identity theft, according to Lormel, is the "cloak of anonymity" that it provides.³⁸ He noted that identities are often stolen in order to

carry out such violations of federal law as bank fraud, credit card fraud, wire fraud, mail fraud, bankruptcy fraud, and computer crimes. Moreover, this cloak of anonymity means that “[t]he use of a stolen identity enhances the chances of success in the commission of almost all financial crimes.”³⁹ In the context of terrorism, identity theft poses an additional danger because terrorists can use their new identities to avoid the watchful eyes of federal investigators as they plan and prepare for attacks.

The 9/11 Commission Report established that terrorists have committed identity fraud. “For terrorists,” the report noted, “travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack.”⁴⁰ The report went on to say that terrorists have used “altered and counterfeit passports and visas,” and it warned that “[f]raud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.”⁴¹

Bob Sullivan, an MSNBC technology correspondent, criticized the *9/11 Commission Report's* treatment of the identity-theft issue for not going far enough. While the report noted the issue, Sullivan consulted with experts who believed that the connection between identity theft and terrorism received short shrift in congressional hearings.⁴² Sullivan pointed out that an al-Qaeda training manual instructs trainees to have five false personas.⁴³

Information-security architect Brian Koerner has written that terrorists increasingly make use of stolen identities.⁴⁴ He outlines four major reasons that terrorists find identity theft desirable: avoiding watch lists; obscuring their whereabouts; funding terrorist activities; and gaining unauthorized access to “entry points such as airline gates, border crossings, or other facilities.”⁴⁵

Identity theft doesn't just benefit terrorists: it also harms the society against which it is directed. The FBI's *Financial Crimes Report* to the Public, released in

mid-2005, noted that identity theft hurts the monetary victims of the fraud but can also be devastating to the individual whose identity is stolen:

[T]he individual victim of the identity theft may experience a severe loss in their ability to utilize their credit and their financial identity. The loss can be short in duration, or may extend for years. It may result in the inability to cash checks, obtain credit, purchase a home or, in the most insidious cases, the arrest of the individual for crimes committed by the identity thief.⁴⁶

Identity fraud constitutes a violation of federal law. Federal code 18 U.S.C. § 1028 lists eight kinds of prohibited activity, including producing identity documents without legal authority, transferring stolen or forged identity documents, possessing such documents, or trafficking in false authentication features or false identity documents. There is also a federal statute for aggravated identity theft that covers acts of identity fraud that occur in relation to acts of terrorism transcending national boundaries.⁴⁷ However, as previously discussed, it is often difficult to prove involvement in a terrorist plot beyond a reasonable doubt; that's why Attorney General Ashcroft recommended adopting a law enforcement strategy similar to the one employed against Al Capone and the mob. Applying that model, a suspected terrorist taking part in identity theft is more likely to be convicted under the statute for simple identity fraud rather than aggravated identity theft.

■ Bank Fraud

A number of individual crimes can be considered bank fraud under federal law. But the common denominator for all offenses in this category is that they are designed to defraud financial institutions. According to the U.S. Code, the criminal penalty for bank fraud is a fine “not more than \$1,000,000 or imprison[ment] not more than 30 years, or both.”⁴⁸

The most profitable kind of bank fraud is credit card fraud. Terrorists have employed this tactic in the past, as MSNBC's Bob Sullivan writes:

The Millennium Plot terrorists, Ahmed Ressam and Mokhtar Haouari, allegedly used credit card fraud, and even made plans to buy a gas station and steal customer account numbers that way, according to a report in the Chicago Tribune. And the indictment of terrorist suspect Ali Saleh Kahlah al-Marri, who has been linked to alleged Sept. 11 paymaster Mustafa Ahmed al-Hawsawi, alleged that al-Marri was arrested with a laptop computer that had 1,000 stolen [credit card numbers] on it, along with a host of Internet bookmarks pointing to fraud and fake ID-related sites.⁴⁹

Additionally, various criminal enterprises that raise money for Hizballah have used bank fraud. A 2004 FBI report noted that “these criminal enterprises, primarily based in the Detroit area, are engaged in a wide range of offenses, including credit card fraud, bank fraud, mail fraud, mortgage fraud, wire fraud, bankruptcy fraud,” and others.⁵⁰

■ Cigarette Smuggling

Cigarette smuggling is an arbitrage scheme that has been used to raise funds for terrorist groups from within the United States. Central to such smuggling schemes is the variance in cigarette tax rates between the states. Some states, such as Virginia and North Carolina, have low cigarette taxes. Others, like New Jersey and New York, have higher cigarette taxes. In a cigarette smuggling scheme, the smugglers purchase large volumes of cigarettes in states that have low tax rates and resell them below market prices in states with high cigarette taxes. They’re able to undersell the market since the smugglers don’t pay taxes on the cigarettes they resell. Steven Emerson has explained that such schemes can yield extraordinary profits:

As a senior ATF [Bureau of Alcohol, Tobacco, Firearms and Explosives] official explained, such smuggling is quite lucrative. For example, a smuggler could buy a carton (ten packs) of cigarettes for around \$20 in Virginia (where, until September 2004, the cigarette tax was 2.5 cents per pack), and then resell it in New York City (where the tax is \$1.50 per pack) for about \$40 a carton. A

single truckload of cigarettes can yield a \$2 million profit.⁵¹

The best-known case of cigarette smuggling involved a cell in Charlotte, North Carolina, that raised money for Hizballah. Brothers Mohamad Hammoud and Chawki Youssef Hammoud would buy van loads of cigarettes in North Carolina, where the tax was 5 cents per pack, and transport them to Michigan, where the tax was 75 cents a pack. Douglas Farah has noted that “[t]he brothers could clear \$8 to \$10 per carton, and each van load netted them up to \$13,000.”⁵²

This is not the only case in which profits from cigarette smuggling were diverted to terrorist groups. By mid-2004, the ATF had more than 300 open cases of illegal cigarette trafficking, and an official reported that several of these were linked to terrorist fundraising. Assistant ATF director Michael Bouchard told the *Washington Post*: “This is a major priority for us. The deeper we dig into these cases, the more ties to terrorism we’re discovering.”⁵³

■ Counterfeiting

Counterfeit goods have become another illegal source of revenue for terrorists. Criminology professor Mark S. Hamm has written that “there is mounting evidence of terrorists’ involvement in the lucrative underworld of counterfeiting.”⁵⁴ One example he provides is the FBI’s 1996 confiscation of 100,000 counterfeit T-shirts that had both a fake Nike “swoosh” and Olympic logos. Followers of Sheikh Omar Abdel Rahman, who was sentenced to life in prison for his involvement in a 1995 plot to bomb New York City landmarks, reportedly ran that operation.⁵⁵

Moreover, multiple sources have discussed Hizballah’s involvement in the sale of counterfeit products. Summarizing the evidence on this point, Steven Emerson wrote:

Carratu International, a leading corporate investigation company, claimed in 2002 that some counterfeit products offered at Internet sites and street markets may be sold to fund terrorist organizations

like Hizballah. Fake goods range from power tools to “designer” clothes and pharmaceutical products, such as Viagra, Prozac, and Xenical. Stratfor—a leading private intelligence firm that provides corporations, governments, and individuals with geopolitical analysis and forecasts—reports that Hizballah has even supported past operations by selling knockoff designer products on New York City street corners.⁵⁶

An indictment unsealed in March 2006 provided a window into Hizballah’s counterfeiting operations. The Department of Justice explained that a Dearborn, Michigan-based ring was indicted for events that occurred between 1996 and 2004, including cigarette smuggling and the sale of counterfeit goods. These goods included “counterfeit Zig Zag rolling papers and counterfeit Viagra.”⁵⁷ Senior FBI agent Bob Clifford commented that trafficking in counterfeit Viagra made sense because the tablets are “small, they’re in high demand and they’re easily transportable. They’re the perfect medium.”⁵⁸ The profits were allegedly sent to Hizballah in Lebanon.

Intellectual property crime, a violation of federal law,⁵⁹ has been defined as “counterfeited and pirated goods, manufactured and sold for profit without the consent of the patent or trademark holder.”⁶⁰ Terrorist involvement in counterfeiting further shows how terrorists and their supporters make ingenious use of opportunities for illegal profit. From terrorist involvement in counterfeiting and cigarette smuggling, we can infer an appropriate law enforcement strategy of following up on leads when it is suspected that terrorists may derive profits from certain illegal schemes. Doing so may help law enforcement determine where to concentrate resources. For example, “a nationwide crackdown on black market tobacco” began after authorities learned that such terror groups as al-Qaeda and Hizballah were profiting from this sector of the underground economy.⁶¹

CYBER-CRIME

Cyber-crime and cyber-terrorism are emerging threats. Some kinds of cyber-crime are simply financial crimes that make use of the Internet.

For example, from December 1999 to April 2000, five Moscow-based hackers stole about 5,400 credit card numbers from Internet retailers and pocketed about \$630,000, before their arrest.⁶² As with other kinds of financial crimes, law enforcement should maintain a watchful eye for terrorist links to cyber-crime.

But there is another danger: catastrophic cyber-terrorism. So far, this threat has not been actualized. But law enforcement—as well as businesses, government agencies, and even individuals—should be aware of it. H. H. Whiteman, director general of Transport Canada’s security and emergency preparedness, wrote that “[c]yber terrorism must be considered to include the full range of threats, vulnerabilities, risks, and technological matters that anyone employing IT systems at the core and even on the periphery of their business must contend with today.”⁶³

There are many ways that a cyber-terrorist attack could damage the United States. One of the most frequently discussed is an attack on civil aviation. Seymour E. Goodman, a professor of international affairs and computing at the Georgia Institute of Technology, has written that transportation systems “are especially attractive targets for malicious or reckless attack with potentially serious casualty and economic consequences.”⁶⁴ Civil aviation is a tempting target and is “extraordinarily dependent on computer-telecommunications information systems.”⁶⁵

There is evidence that cyber-crime and cyber-terrorism are growing increasingly attractive to terrorists. Gabriel Weimann, a senior fellow at the United States Institute of Peace, has listed five major reasons for the attraction to cyber-terrorism.⁶⁶ First, it’s cost effective: all that a terrorist needs to carry out an act of cyber-terrorism is a personal computer with Internet access. Second, there is relative anonymity in cyber-terrorism. Terrorists need not be physically present at an attack and can use screen names and other cloaks of anonymity to disguise themselves from authorities. Third, there are a large number of targets. A cyber-terrorist could “target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth.”⁶⁷ Critical infrastructure such as electric power grids and emergency services would

be vulnerable. Fourth, it's easier for an organization to recruit people for cyber-terrorist attacks because their remote nature means less need for physical training and risk of mortality. Finally, cyber-terrorism can affect a larger number of people than traditional terrorist methods. This fact can be seen in the speed with which destructive computer viruses spread throughout the world.

Terrorists' increasingly sophisticated use of the Internet provides further reason for concern about the threat of cyber-terrorism. One example is a hacker called Irhabi 007, which translates as "Terrorist 007." For two years, Irhabi 007 served as an al-Qaeda conduit and had "hacked into American university computers, propagandized for the Iraq insurgents led by Abu Musab al-Zarqawi and taught other online jihadists how to wield their computers for the cause."⁶⁸ A case study produced by the SITE Institute, a Washington, D.C.-based counterterrorism research center that monitors online jihadist activity, explains that "Irhabi changed the face of the jihadi Internet world through his ability to covertly and securely disseminate violent materials including manuals of weaponry, videos of jihadist feats, such as the beheadings perpetrated by Iraqi insurgents, and other inflammatory media files."⁶⁹

When Scotland Yard officials arrested four youths suspected of taking part in a bomb plot in October 2005, one of those men, Younis Tsouli, turned out to be Irhabi 007.⁷⁰ Before his arrest, Irhabi managed to pave the way for future online jihadists. For example, in June 2005 he posted a long message on an al-Qaeda message forum titled "Seminar on Hacking Websites," which provided readers with a detailed study of hacking that was over twenty pages long.⁷¹ The example of Irhabi 007 shows not only the threat of cyber-crime and cyber-terrorism but is also indicative of the increasingly sophisticated means of propagandizing for terrorist groups.

Another sign of this increasing sophistication came in the wake of the controversy over Danish cartoons satirizing Prophet Muhammad that resulted in rioting throughout the Muslim world in February 2006. In early February 2006, the British computer magazine

Computer Shopper noted that "[g]angs of pro-Muslim computer hackers have unleashed a withering cyber attack on Danish and Western websites in the past week."⁷² Some 578 Danish websites were knocked off-line in a single week.

There are many mechanisms that terrorists could use to target the "virtual world." The U.S. Army's handbook *Cyber Operations and Cyber Terrorism* illuminates some of these tools.⁷³ Of particular concern are computer worms, which are destructive software programs containing codes capable of gaining access to a computer or network and causing harm by deleting or manipulating the data. In a worst-case scenario that policymakers fear, a worm that infects the U.S. financial sector could shut down Wall Street, or one infecting airlines' databases could result in millions of missed flights or even downed flights. Another concern is computer viruses, which are designed to infect and damage software programs.

For some time, pure cyber-terrorism has been seen as a threat that hasn't yet actualized. A 1999 report released by the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School stated that "pure cyberterrorism is a thing of the future. For the present, terrorists are much more likely to pursue cyberterror as an ancillary tool. However, as time and resources permit, groups of certain ideological types at particular growth stages will attempt to build on already existing cyberterror capabilities."⁷⁴ Eight years later, the time may fast be approaching when cyber-terror is seen as far more than an ancillary tool.

ILLEGAL MONEY TRANSFERS

This paper has already shown that terrorist groups see the United States as fertile ground for terrorist fund-raising. Another criminal act, complementary to terrorist fund-raising, is the illegal transfer of funds to terrorist groups. This process has been carried out in different ways. This section outlines four examples: the Benevolence International Foundation, the Holy Land Foundation, Al Haramain Islamic Foundation, and Hizballah.

■ Benevolence International Foundation

The Benevolence International Foundation (BIF) was an Islamic charity founded and incorporated in Palos Hills, Illinois, in March 1992.⁷⁵ At its inception, one of BIF's directors was Sheikh Adel Abdul Jalil Batterjee, who was affiliated with the "Golden Chain" group from the Persian Gulf—a group of wealthy donors who financed the mujahideen in the Afghan-Soviet war during the 1980s and went on to become major al-Qaeda backers.⁷⁶ BIF achieved tax-exempt status as a charitable organization in March 1993. Around that time, BIF replaced Batterjee and the other founding directors with new directors, one of whom was Enaam Arnaout.⁷⁷

The FBI began to investigate BIF in 1998 after a Washington, D.C., conference that an agent attended. There, the agent "learned of foreign intelligence reports indicating that Arnaout was involved in providing logistical support for jihadists."⁷⁸ Opening a full field investigation in 1999, the FBI's Chicago field office put BIF's headquarters under surveillance and even dug through its garbage.⁷⁹ Before 9/11, the FBI was unable to bring a criminal case even though agents had come across suspicious material during the search and even though the agents involved "believed BIF had substantial ties to al Qaeda, was supporting jihad, and was sending a great deal of money overseas."⁸⁰

After 9/11, more information was made available to the FBI. For example, al-Qaeda cooperators whom the FBI was allowed to interview after 9/11 revealed BIF's financial dealings with al-Qaeda in the early 1990s.⁸¹ This new information allowed the Treasury Department's Office of Foreign Assets Control to freeze BIF's assets as a specially designated terrorist organization,⁸² and the FBI finally garnered enough evidence for a criminal case. Ultimately, Arnaout pleaded guilty to one count of racketeering conspiracy for fraudulently diverting charitable donations to finance overseas combatants.⁸³

At his sentencing, Arnaout admitted to supporting various kinds of jihadist groups overseas through BIF. He admitted that BIF sent boots to mujahideen in Chechnya; boots, tents, and uniforms to soldiers in Bosnia-Herzegovina; and uniforms for a provisional,

unrecognized government in Chechnya. The court found that BIF had diverted a total of \$315,624 to overseas fighters.⁸⁴ The indictment also drew heavily from documents seized from BIF's Bosnia offices to link BIF and Arnaout to the formation of al-Qaeda.⁸⁵ However, as part of the plea agreement, the government agreed to drop charges that BIF had supported al-Qaeda and its affiliates. The plea agreement prevented the court from weighing the evidence on this point.

For a long time, BIF was able to use its tax-exempt status and reputation as a charitable organization to conceal its funding of foreign fighters. It hid this funding from authorities by lumping its donations to military operations into other donations that were devoted to legitimate charity work.

■ The Holy Land Foundation

The organization that came to be known as the Holy Land Foundation (HLF) originally assumed the name "Occupied Land Fund." It was created in about 1998 for the purpose of providing support for Hamas, which has been responsible for a large number of attacks against Israeli civilians and other targets. Originally located in California, the group moved to Richardson, Texas, where it eventually became known as the Holy Land Foundation, a tax-exempt charity whose stated objective was to provide support to the needy in the West Bank and Gaza.⁸⁶

HLF had a long-standing relationship with Hamas. During the late 1980s and into the 1990s, HLF openly provided support for Hamas, which was named a specially designated terrorist organization in 1995.⁸⁷ Shortly after its creation, HLF sent approximately \$100,000 to Abu Marzook, Hamas's future political bureau chief. HLF also sent \$725,000 to the Islamic Center of Gaza, which Hamas spiritual leader Sheikh Ahmed Yassin established to serve as a front for Hamas activity.⁸⁸ HLF sponsored a number of conferences and conventions featuring radical sheikhs and Hamas officials that were designed to help them raise funds; some events featured songs and skits depicting the killing of Jews.⁸⁹ After the Oslo Accords, which were designed to promote peace between Israel and the Palestinians, HLF's principals met

with Hamas activists in Philadelphia to try to determine how HLF could support Hamas's "opposition to the peace plan and to decide how to conceal their activities from the scrutiny of the United States government."⁹⁰ And HLF subsidized Hamas's "vital recruitment and reward efforts in the West Bank and Gaza."⁹¹ Multiple links exist between HLF and Hamas.

The Holy Land Foundation was ultimately indicted for money laundering. Money laundering refers to the metaphorical "cleansing" of money. Individuals and groups can engage in money laundering in many different ways, ranging from bulk cash smuggling to trade-based money laundering to online payment systems.⁹² There are two basic kinds of money laundering.

The first kind is designed to disguise the fact that drug dealers and others who profit from illegal ventures obtained the money illegally. Thus, the United Nations Office on Drugs and Crime defines money laundering as a "three-stage process which disguises illegal profits without compromising the criminals who wish to benefit from the proceeds. This requires: first, moving the funds from direct association with the crime; second, disguising the trail to foil pursuit; and third, making the money available to the criminal once again with the occupational and geographic origins hidden from view."⁹³

The second kind of money laundering is designed not to disguise the source of funds but rather their *destination*—in that the money in question is going to finance illegal activities overseas. U.S. law prohibits this type of money laundering as well.⁹⁴

HLF was indicted on twelve counts of money laundering and one count of conspiracy to commit money laundering.⁹⁵ The indictment charges that HLF "transmitted or caused to be transmitted approximately \$12,400,000 to various HAMAS controlled zakat committees and organizations."⁹⁶ The indictment lists seventeen wire transfers that were designed to support these organizations, as well as twelve instances in which the HLF defendants transmitted funds to the West Bank and Gaza with the intent to contribute funds, goods, and services to Hamas. These wire transfers and transmissions allegedly violate U.S. laws against money laundering.⁹⁷

Like BIF, HLF appears to have used its tax-exempt status and reputation to conceal the funding of terrorism. The criminal case against HLF is ongoing.⁹⁸

■ Al Haramain Islamic Foundation

Al Haramain Islamic Foundation was established in Riyadh, Saudi Arabia, in 1992 and quickly became one of the most important international Wahhabi charities.⁹⁹ At its peak, Al Haramain had offices in more than fifty countries and an annual budget of \$30–80 million.¹⁰⁰ Its head U.S. office was located in Ashland, Oregon. Al-Haramain was "organized as a public benefit corporation exclusively for religious, humanitarian, educational, and charitable purposes."¹⁰¹ It obtained tax-exempt status.

Al Haramain's U.S. branch and two of its directors were indicted in January 2005 for illegally moving money out of the country.¹⁰² Central to the prosecution was the requirement that anyone who transports more than \$10,000 in currency or monetary instruments in or out of the United States is required to provide details of that transaction in Form 4790, "Report of International Transportation of Currency or Monetary Instruments."¹⁰³

The actions that investigators honed in on began in February 2000, when an Egyptian man wire transferred about \$150,000 to a bank account in Ashland belonging to Al Haramain.¹⁰⁴ In an e-mail, the donor stated that the money was designed "to participate in your noble [sic] support to our muslim brothers in Chychnia [sic]." Shortly after the money was wired, one of Al Haramain's directors, Soliman al-But'he, flew from Saudi Arabia to the United States, where he met another director, Pete Seda (a.k.a. Pirouz Sedaghaty). On March 10, the two men went to a branch office of Bank of America and bought 130 American Express traveler's checks, all in the \$1,000 denomination.¹⁰⁵ Al-But'he signed a check for \$131,300 to buy the traveler's checks; the next day, Seda returned to the bank and collected the rest of the funds that had been wired from Egypt, in the form of a \$21,000 Bank of America cashier's check.

Al-But'he left the U.S. for Saudi Arabia on March 12 with the traveler's checks and cashier's check. On the way out, he failed to file a Form 4790 indicating that he

was transporting \$150,000 out of the United States, in violation of federal law. Al Haramain then attempted to disguise al-But'he's money transfer by inflating the cost of a building that it purchased in Missouri in the income tax return that it filed at the end of the year.¹⁰⁶

The indictment against Al Haramain states that the group attempted to disguise the monetary transfer because the organization intended "that the funds be delivered to the Chechen mujahideen."¹⁰⁷

■ Hizballah

A number of individuals and groups that raised money for Hizballah in the United States illegally transferred money and other items of support to the terrorist group. One such case, detailed above, is the cigarette-smuggling cell in Charlotte, North Carolina. The second superseding indictment in that case explains that members of the terrorist cell sent money to Hizballah leaders and also purchased equipment that they sent to Lebanon. This equipment included night-vision goggles, global positioning systems, mine- and metal-detection equipment, advanced aircraft analysis and design software, stun guns, and laser range finders.¹⁰⁸ Ultimately, the defendants in the Charlotte case were convicted under a Patriot Act provision that outlaws providing anything of value to a group designated as a terrorist organization.¹⁰⁹

There are other cases of individuals in the U.S. supporting Hizballah through money laundering. For example, after the indictment of a Dearborn, Michigan, group involved in cigarette smuggling and counterfeiting was unsealed in March 2006 (as mentioned above), the DOJ's press release explained that the group had engaged in these criminal enterprises in order to launder money.¹¹⁰

Money raised in the U.S. through both legal and illegal means has frequently made its way to terrorist groups in the Middle East. Authorities can vigorously counteract terrorist financing by being cognizant of organizations that are known affiliates of terrorists or terrorist groups, or else supportive of terrorists' messages—and should check their bank and other

financial records to determine whether they have been involved in terrorist financing.

Law enforcement should also keep abreast of ways that terrorists adapt in an effort to thwart investigations. Stuart Levey, undersecretary of the Treasury's Office of Terrorism and Financial Intelligence, said in Senate testimony that his office has witnessed "a decrease in the average amount of transactions that we learn about."¹¹¹ Levey remarked:

[T]his observation carries across various financial conduits and terrorist organizations and we have no reason to believe that it is unrepresentative. Interpreting this indicator is more difficult. It could reflect an overall decrease in the amount of money moving to and from terrorists. Just as easily, it could indicate that terrorists are breaking their transactions out into smaller sums, fearing interception. Alternatively, the trend could be an outgrowth of a movement by terrorist organizations away from banks towards less formal mechanisms, like cash couriers.¹¹²

Terrorists frequently adapt to policing and intelligence measures. For example, after learning that the National Security Agency could monitor only the e-mails that had been sent, some terrorists began using shared e-mail accounts (to which all members of a cell would have the password) and saving messages as drafts. Since the messages were never sent, terrorists were able to avoid NSA surveillance. Likewise, terrorists may be adapting to anti-money-laundering efforts.

IMMIGRATION VIOLATIONS

For many terrorists, immigration violations are the first acts taken in a long line of criminal activities. A significant number of terrorists who came from overseas have done so illegally, through such mechanisms as document fraud and sham marriages. Michael Cutler, a fellow at the Center for Immigration Studies, has written that when "an alien acquires immigration benefits through fraud and deception, the security of the system is breached and it leaves the door open to criminals and terrorists gaming the system."¹¹³

Individuals who have planned acts of terror against the United States or raised money for terrorist organizations have often engaged in immigration violations. Ramzi Yousef, the mastermind of the first World Trade Center attack, in 1993, used an altered passport and fraudulent documents.¹¹⁴ Some members of the Charlotte cell that raised money for Hizballah were in the country illegally. Following 9/11, the government has aggressively pursued immigration violation cases against known Islamic radicals and individuals who are suspected of terrorist ties.

■ Document Fraud

Several kinds of document fraud can occur during the immigration process. Document fraud, through forgery, lying, false statements, or the misuse of visas, is punishable under federal law. The Immigration and Naturalization Act makes it illegal for an alien to use, acquire, or provide fraudulent documents for the purpose of acquiring citizenship or naturalization.¹¹⁵ Document fraud violations may result in civil and criminal penalties. Most significantly, there are also immigration consequences: an alien who is culpable in document fraud may be prevented from receiving visas to be admitted to the United States.¹¹⁶ Document fraud “is also a ground for deportability.”¹¹⁷

Suspected terrorists have been deported from the U.S. or else arrested for document fraud. One example is Fawaz Damra, a Cleveland-based imam who was born in the West Bank. In 2004, Damra was convicted of lying on his citizenship application by failing to disclose his links to terrorist organizations.¹¹⁸ Even though he was convicted of an immigration violation rather than terrorism charges, government attorneys sought Damra’s deportation “because they consider him a national security threat.”¹¹⁹ Ultimately, Damra agreed to be deported in January 2006. Another example is Maher Amin Jaradat, a naturalized U.S. citizen of Palestinian descent, who was indicted in May 2005 for making false statements on his application for citizenship: he failed to disclose his membership in the Democratic Front for the Liberation of Palestine.¹²⁰

But in the past, there may have been under-enforcement of immigration laws when it comes to known

terrorists operating in the United States. Janice Kephart, former counsel to the 9/11 Commission, authored a report titled *Immigration and Terrorism*, which examines the histories of ninety-four foreign-born terrorists who operated in the United States between the early 1990s and 2004.¹²¹ It concludes that of these ninety-four terrorists, “about two-thirds (59) committed immigration fraud prior to or in conjunction with taking part in terrorist activity.”¹²² Because of these widespread terrorist violations of U.S. immigration law, Kephart suggests that the “lax immigration system” poses a danger and recommends “strict enforcement of immigration law—at American consulates overseas, at ports of entry, and within the United States.”¹²³

The report details various methods that terrorists have used to enter the United States. Those covered in her study applied for naturalization twenty-one times; twenty applications succeeded. Yet she notes that there were “eleven clear indications of fraud” in these applications, including document fraud and withholding of material facts.¹²⁴ Kephart notes that with naturalization comes a U.S. passport, which can create particular problems. For example, Iyman Faris, who in 2003 admitted to plotting to cut the Brooklyn Bridge’s suspension cable and derail passenger trains on orders from al-Qaeda, was a naturalized U.S. citizen.¹²⁵ Thus, after his 1999 naturalization, Faris could easily travel in and out of the U.S. He traveled to Afghanistan at least twice, conducting business for al-Qaeda upon each return.¹²⁶

The fact that terrorists have in the past obtained entry to the United States and have even become naturalized U.S. citizens through fraudulent means has national security implications.

■ Sham Marriages

Sham marriage is a commonly used method of allowing terrorists to stay in the United States, even opening the door for them to become permanent residents or naturalized citizens. Federal law allows an alien who is a spouse of a U.S. citizen to be considered the citizen’s immediate relative, thus allowing the alien to gain lawful permanent residency in the U.S.¹²⁷ Great leeway is provided for aliens to remain

in the United States if they are able to marry a citizen. However, federal law also prohibits marriage fraud, which is defined as a marriage that is entered into solely “for the purpose of evading any provision of the immigration laws.”¹²⁸

A number of terrorists and terror supporters affiliated with al-Qaeda, Hizballah, and the Palestinian Islamic Jihad used sham marriages to stay in the United States. One example is the Charlotte Hizballah cell, where one of the key figures was Said Mohamad Harb. Kephart writes that Harb “helped secure three fraudulent visas and three sham marriages for the purpose of ‘legally’ bringing in the United States his brother, his brother-in-law, and sister so that they might become legal permanent residents.”¹²⁹ In one case, two of the women who “married” conspirators were in reality a lesbian couple who lived together rather than with their “husbands.”

Immigration laws should be our first line of defense against those who would enter the United States to raise money for terrorist groups or participate in acts of terrorism. So there is a national security reason to ensure that immigration laws are not under-enforced when individuals violating these laws are suspected of involvement in terrorism. Clamping down on immigration violations is one of the government’s major tools in employing the Al Capone model of preventing another major terrorist attack on U.S. soil. In mid-2005, the *Washington Post* noted that “in the past two years, officials have filed immigration charges against more than 500 people who have come under scrutiny in national security investigations.”¹³⁰ The reason for the high number of immigration charges is that authorities are using immigration laws against suspected terrorists.

IMPLICATIONS OF THE AL CAPONE MODEL

Many analysts have wondered why the United States hasn’t been attacked since 9/11. Surely, terrorists have not lost their desire to attack America, as successful attacks in Britain, Egypt, Indonesia, Israel, the Philippines, Russia, Spain, Tu-

nisia, Turkey, and many other countries make clear. While there is no single answer to this question, the government’s law enforcement model seems to have played an important role.

The Al Capone model of anti-terror policing holds that law enforcement should disrupt would-be terrorists before they can strike. Terrorists can be disrupted through prosecution of all crimes committed, including minor offenses. As this paper has shown, there are many indications of heavy terrorist involvement in criminal activity. This criminal involvement, coupled with the increasing difficulty of winning convictions for terrorism offenses, makes pursuing lesser offenses worthwhile.

■ The British Experience

British law enforcement and intelligence has had many notable successes in dismantling terrorist cells. However, some of the failures of British anti-terror policing highlight the importance of the Al Capone model’s aggressive pursuit of leads and disruptive prosecutions. This pursuit of leads involves not only digging until there’s no more dirt but also undertaking cross-referencing and background checks of other subjects who are found to be associated with radicals or potential terrorists. Often when an individual or group that is being investigated meets or develops a relationship with another individual or group, it’s for a reason.

The British system tends to let radicals operate longer because of the intelligence benefits gained from seeing what the suspects do. The problem is that this policing model allows some terrorists to slip through the cracks, as shown in the wake of a recently concluded trial in which five men were sentenced to life in prison for a plot to attack a number of London targets with bombs made of fertilizer (known as the “fertilizer plot”). Before the fertilizer plotters were arrested in March 2004, they had come into contact with 7/7 transit-bomb plotters Mohammed Siddique Khan and Shehzad Tanweer. Agents listening in on a bug monitoring the fertilizer plotters heard Khan state that he planned to kill non-Muslims; moreover, a tracking device was placed in Khan’s car a year before the 7/7

attacks, his meetings with radicals were reported to British domestic spy agency MI5 at least four times, and he underwent terrorist training in Pakistan with some of the fertilizer plotters.¹³¹ Nevertheless, counterterrorism officials were forced to concede after the fertilizer-plot trial that “intelligence that could have raised alarms before the July 7 transit attacks was never thoroughly investigated.”¹³² Those attacks ended up killing fifty-two people.

British counterterrorism officials explained that they never thoroughly investigated the 7/7 bombers because other intelligence leads seemed more urgent. The Intelligence and Security Committee’s investigation into the London attacks states that because of limited resources, “it was decided not to investigate [Khan and Tanweer] further or seek to identify them. When resources became available, attempts were made to find out more about these two and other peripheral contacts, but these resources were soon diverted back to what were considered to be higher investigative priorities.”¹³³ But MI5’s report on links between the 7/7 bombers and the fertilizer plotters reveals that MI5 *did* have enough information to prosecute Khan and Tanweer—for lesser offenses. The report shows that Khan and Tanweer met with the fertilizer plotters on five occasions, and explained methods of fund-raising to them: “Conversations record Khan and Tanweer discussing how to raise cash through a variety of fraud scams, such as purchasing building equipment on credit, defaulting on payment and selling the goods on for cash.”¹³⁴

Under the British model of anti-terror policing, Khan and Tanweer were allowed to continue operating even though they shared their criminal expertise with known terrorists and expressed a desire to kill British citizens. In contrast, they probably would have been picked up under the Al Capone model and tried for their involvement in financial scams. In the situation that the British faced—when so many potential plots are being investigated that not all leads can be aggressively pursued—there is even more reason to arrest radicals who are clearly involved in criminal enterprise in order to disrupt their activities. Had the British done so, the 7/7 attacks may have been prevented.

■ Critics of the Al Capone Model

Critics of the current U.S. anti-terror policing model do not appreciate the value of disruption. The New York University School of Law’s Center on Law and Security published a *Terrorist Trial Report Card* in 2006, containing a comprehensive database of all cases that came through the federal court system that were at some point classified as terrorism cases.¹³⁵ The report had a number of factual findings descriptive of the adoption of the “Al Capone model” at the federal level:

- ***Conviction, no matter how short the period of time or how minor the charge, is the primary goal.*** The average prison time for individuals who were arrested on suspicion of terrorism is 51 months, or just over three years, a valid technique if the goal is disruption of alleged plots but not a sufficient means of long-term incapacitation or deterrence. The average sentence for federal terrorism charges is 206 months, or just over 17 years.
- ***The DOJ’s pattern of pursuit is focused on early detection rather than conviction on federal terrorism charges.*** This has resulted in a relatively small share of federal terrorism convictions out of the total convictions—only 15% of the total 307 convictions were for federal terrorism crimes. . . .
- ***No sleeper cell with logistical or tactical links to al-Qaeda has been convicted of plotting an attack to be carried out within the U.S.*** While the government has convicted groups in the United States conspiring and attempting to levy war against the U.S. abroad (like the Portland Seven), individuals conspiring to commit terrorism here at home (like Siraj in Brooklyn), and groups linked to al-Qaeda (like the Virginia Jihad Network), the government has not convicted al-Qaeda cells in the U.S. with instructions to attack inside the country.
- ***The vast majority of cases turn out to include no link to terrorism once they go to court.*** In the 510 cases announced as ter-

rorism cases, only 158 individuals have been prosecuted on charges of terrorism and material support to terrorism. The remaining 352 individuals have been prosecuted on lesser charges and no criminal link to terrorism was substantiated in court.¹³⁶

Based on these findings, the *Terrorist Trial Report Card* argues that either the terrorist threat is much less than originally assumed or else “the policies of the United States have reduced the threat through deterrence, and, yes, through excessive vigilance.”¹³⁷ The report then concludes that there seems to be “few, if any, prevalent terrorist threats currently within the U.S.” and argues that “[a]ny future policy must be premised on this conclusion.”¹³⁸ Although this statement is vague, it suggests that a less aggressive law enforcement model should be adopted.

The *Terrorist Trial Report Card* is clearly critical of the Al Capone model of anti-terror policing. Its first conclusion is that the current model only works if the goal is disruption, not if it is deterrence or incapacitation. But how do you deter this enemy? The 9/11 attacks and our subsequent experience fighting Islamic insurgents in Afghanistan and Iraq show that many Muslim radicals are willing to die for their cause. They are unlikely to be deterred by a seventeen-year prison term. There is indeed a trade-off between disruption and long-term incapacitation, but Britain’s failure to stop the 7/7 bombers despite all that was known about them shows that the value of disruption should not be underestimated.

The *Terrorist Trial Report Card* also asserts that there are now “few, if any, prevalent terrorist threats” in the U.S. While it may be true that policymakers overestimate the domestic terrorist threat, the *Terrorist Trial Report Card’s* statistics prove no such thing—and, in fact, the report’s other conclusions undermine this finding. The report concedes that the DOJ wants to win convictions “no matter how short the period of time or how minor the charge” and that DOJ “is focused on early detection rather than conviction on federal terrorism charges.” This applicable prosecution model helps to explain both the lack of proof in the courtroom of sleeper cells with logistical or tactical links to al-Qaeda and the reason that the majority of cases have “no link to terrorism once

they go to court.” This phenomenon is entirely explainable by authorities’ earlier disruption of plots.

Brian Michael Jenkins, senior advisor to the president of the RAND Corporation, has noted that “suspects may be apprehended while their plans are in the talking stage,” which makes prosecution difficult because suspects “can claim that they were only talking and never had serious intentions.”¹³⁹ The practical result is predictable:

As a consequence, the number of prosecutions is small compared with the number of people detained, which reflects a preventive law enforcement approach rather than the traditional reactive approach. It is sufficient to say that the operational capabilities of the jihadists have been degraded and that terrorist operations are being thwarted. Keeping score is difficult and irrelevant.¹⁴⁰

Jenkins may overstate: perhaps keeping score is not irrelevant, but it certainly is difficult. It is clear, though, that the *Terrorist Trial Report Card* does not come close to proving a lack of jihadist threat inside the United States. The only factor that the report considers is what has been proved in the courtroom, which is far from determinative. The fact that Al Capone was only convicted of tax evasion doesn’t change the fact that he was a powerful and vicious mobster: focusing only on the crime someone was convicted of may obscure his actual activities. Thus, premising future policy on the *Terrorist Trial Report Card’s* conclusion, as the report urges, is a risky path to follow.

The value of the Al Capone model should thus be apparent: it allows authorities to disrupt terrorist activity before plots can become operational. It is designed to succeed where other models, such as the British model, would allow terrorists to continue to operate.

CONCLUSION

After the 9/11 attacks, the United States was faced with an unprecedented challenge. Americans learned how devastating a terrorist attack could be, and there were fears that the next attack could be even worse. An open society like the

United States has a number of inherent vulnerabilities, and when 9/11 occurred, the government had little information about other possible terrorist activity inside the country. It was then that law enforcement adopted the Al Capone model of fighting terrorism.

This paper examined five kinds of illegal activity that terrorists have engaged in: drug trafficking, financial scams, cyber-crime, illegal money transfers, and immigration violations. Terrorists gain many advantages from engaging in these enterprises, advantages that range from raising funds to posing a risk of a catastrophic cyber-terrorist attack to entering the country in the first place. And just as terrorists can gain from their illegal activities, law enforcement can exploit the crime-terror nexus by charging suspected terrorists with lesser—and easier to prove—offenses than involvement in a terrorist plot.

There are three principles that law enforcement should adopt in trying to gain advantage in this manner. First, law enforcement should have a method of determining who is a possible terrorist threat. One important element in this analysis is terrorist associations that individuals or organizations may have.

Second, law enforcement should be aware of the kind of criminal enterprises that terrorists have entered. For example, after the government learned that terrorists were smuggling cigarettes to raise money, more law enforcement resources were devoted to combating that practice. It is proper to devote more resources to an area that has not just criminal, but also national, security implications.

Third, law enforcement should continue to recognize the value of using all available laws to combat suspected terrorists. Modifications may be necessary; for example, perhaps law enforcement should wait longer before making arrests in some cases, to maximize the intelligence that it gains. But after 9/11, it was proper for authorities to prosecute terrorists for the full range of offenses that they committed. The value of disrupting plots should not be underestimated. The difficulty of prosecuting terrorist offenses increases the importance of law enforcement using all the tools at its disposal that are within the law.

ENDNOTES

1. See, e.g., Bruce Hoffman, *Is Europe Soft on Terrorism?*, FOREIGN POLICY, Summer 1999, at 62, 69 (arguing that “the meteoric rise of bin Laden and his transnational al Qaeda network” shows a shift away from state-sponsored terrorism and toward “loose associations of self-funded, transnational groups, such as radical Islamic cells”); Richard T. Micco, Note & Comment, *Putting the Terrorist-Sponsoring State in the Dock*, 14 TEMPLE INTERNATIONAL & COMPARATIVE LAW JOURNAL 109, 146 (2000) (“Rather than relying on sponsorship from established nation-states, terrorist groups have come to rely on and be influenced by subnational and multinational groups, religious and quasi-religious cults and private individuals”).
2. For background on Al Capone and his prosecution, see, e.g., Laurence Bergreen, *CAPONE: THE MAN AND THE ERA* (1994); John Kobler, *CAPONE: THE LIFE AND WORLD OF AL CAPONE* (1971).
3. Daniel C. Richman & William J. Stuntz, *Al Capone’s Revenge: An Essay on the Political Economy of Pretextual Prosecution*, 105 COLUMBIA LAW REVIEW 583–84 (2005).
4. Attorney General John Ashcroft, *Prepared Remarks for the US Mayors Conference*, Oct. 25, 2001, at http://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks10_25.htm (last visited Dec. 4, 2006).
5. For example, see Richman & Stuntz, *supra* note 5.
6. See Ashcroft, *supra* note 6.
7. See Graham Allison, *NUCLEAR TERRORISM: THE ULTIMATE PREVENTABLE CATASTROPHE* (2004) (detailing the threat of a terrorist attack with nuclear weapons).
8. David Kaplan, *Paying for Terror*, U.S. NEWS & WORLD REPORT, Dec. 5, 2005.
9. Steven W. Casteel, Assistant Administrator for Intelligence, Drug Enforcement Agency, *Narco-Terrorism: International Drug Trafficking and Terrorism—A Dangerous Mix*, Hearing Before the Senate Judiciary Committee, May 20, 2003, available at http://judiciary.senate.gov/testimony.cfm?id=764&wit_id=2111.
10. See Alex Schmid, *Links Between Terrorism and Drug Trafficking: A Case of Narco-Terrorism?*, International Summit on Democracy, Terrorism and Security, Jan. 27, 2005, at <http://english.safe-democracy.org/causes/links-between-terrorism-and-drug-trafficking-a-case-of-narcoterrorism.html> (last visited Dec. 9, 2006). In Schmid’s report, Appendix II lists twelve definitions of narco-terrorism.
11. *Quoted in* Casteel, *supra* note 11.
12. For example, Loretta Napoleoni has defined narco-terrorism as “the use of terror tactics by the narco-traffickers and drug lords to protect their illegal businesses. It also describes the alliance between drug lords and armed organizations. Both have interests in destabilizing governments and breaking down the established social order.” *Quoted in* Schmid, *supra* note 12.

Some scholars have even suggested that the links between terrorists and drug traffickers are so prevalent that the two should not be dissociated. However, Alison Jamieson has argued persuasively to the contrary:

Organised crime and terrorism are correctly viewed as quite distinct phenomena. Essentially, the terrorist is a revolutionary, with clear political objectives involving the overthrow of a government or the status quo, and a set of articulated strategies to achieve them. Organised crime actors are inherently conservative: they tend to resist political upheaval and seek conditions of order and stability, those more conducive to their business activities. Unlike terrorists, who project an “ideal state” for which they are prepared to sacrifice their lives, organised crime sees no virtue in sacrifice, has no comparable sense of “victory” or “defeat”, but operates according to a set of short- and medium-term goals to be realised with maximum profit and minimum risk.

In general, the organised criminal power system is not “anti-state”, but a parallel organisational model with its own legal and ethical rules, hierarchy of authority and military force. . . . Thus, unlike terrorist actors whose raison d’être is direct confrontation with the state against which they practice violence, the survival of an organised crime group depends upon operating within the state, on the penetration by criminal actors of the legitimate political, economic and social spheres.

Quoted in ibid.

13. *Peterson v. Islamic Republic of Iran*, 01-CV-2092, memorandum opinion (D. D.C. May 30, 2003). For more background on Hizballah, see, e.g., Ahmad Nizar Hamzeh, *IN THE PATH OF HIZBULLAH* (2004); Amal Saad-Ghorayeb, *HIZBU’LLAH: POLITICS & RELIGION* (2002).

14. All three examples appear in Steven Emerson, *JIHAD INCORPORATED: A GUIDE TO MILITANT ISLAM IN THE U.S.* (2006), in a section for which one of the coauthors of this paper served as the primary researcher. See *ibid.* at 226–27.

15. See *U.S. Drug Ring Tied to Aid for Hezbollah*, N.Y. TIMES, Sept. 3, 2002.

16. *Ibid.*

17. *Ibid.*

18. See Greg Krikorian, *Terrorists Received Drug Money*, U.S. SAYS, L.A. TIMES, May 10, 2002.

19. Emerson, *supra* note 16, at 227.

20. See Sean Holstege, *Drug Probe Links Oakland to Mideast*, OAKLAND TRIBUNE, Sept. 22, 2002.

21. Emerson, *supra* note 16, at 227.

22. Andrew Chang, *Is Afghanistan’s Drug Trade Paying Al Qaeda?* ABC NEWS, Sept. 19, 2002, at <http://abcnews.go.com/International/print?id=79842>.

23. *Quoted in* Rowan Scarborough, *Drug Money Sustains al Qaeda*, WASHINGTON TIMES, Dec. 29, 2003.

24. Tim McGirk, *Terrorism’s Harvest*, TIME ASIA, Aug. 2, 2004.

25. *Ibid.*

26. *Ibid.*

27. See Scarborough, *supra* note 25.

28. *Ibid.*

29. See Michael Yon, *Afghanistan’s Other War*, CBS NEWS, Sept. 12, 2006, at <http://www.cbsnews.com/stories/2006/09/12/opinion/main2000748.shtml>.

30. See Scarborough, *supra* note 25.

31. See Sebastian Rotella, *Holy Water, Hashish and Jihad*, L.A. TIMES, May. 23, 2004.

32. *Ibid.*

33. Ahmidan was either transformed into a jihadist in 2000 while in a Madrid detention center for illegal aliens or during a later stint in prison. A Spanish antiterrorism official has explained that while in the detention center, Ahmidan “set himself up

as an imam and told the guards he would come back and kill them. No one took him seriously then, but he already had quite a following.” Bruce Crumley & Scott Macleod, *Across the Divide*, TIME EUROPE, Mar. 13, 2005.

34. Rotella, *supra* note 33.

35. *Ibid.*

36. *Ibid.*

37. Dennis Lormel, Chief of the Federal Bureau of Investigation’s Terrorist Financial Review Group, Testimony Before the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, July 9, 2002, at <http://www.fbi.gov/congress/congress02/idtheft.htm>.

38. *Ibid.*

39. *Ibid.*

40. National Commission on Terrorist Attacks upon the United States, THE 9/11 COMMISSION REPORT at 384 (2004).

41. *Ibid.* at 384, 390.

42. Bob Sullivan, *9/11 Report Light on ID Theft Issues*, MSNBC, Aug. 4, 2004, at <http://www.msnbc.msn.com/id/5594385>.

43. *Ibid.*

44. Brian Koerner, *Terrorist Groups Relying on Identity Theft for Funding and Operations*, ABOUT.COM, at <http://idtheft.about.com/od/useofstolenidentity/p/IDTheftTerror.htm> (last visited Dec. 11, 2006).

45. *Ibid.*

46. Federal Bureau of Investigation, FINANCIAL CRIMES REPORT TO THE PUBLIC at E1 (May 2005), at http://www.fbi.gov/publications/financial/fcs_report052005/fcs_report052005.pdf.

47. See 18 U.S.C. § 1028A(a)(2).

48. 18 U.S.C. § 1344.

49. Sullivan, *supra* note 44.

50. Federal Bureau of Investigation, REPORT TO THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES: THE FBI’S COUNTERTERRORISM PROGRAM SINCE SEPTEMBER 2001 at 70 (Apr. 14, 2004).

51. Emerson, *supra* note 16, at 220.

52. Douglas Farah, BLOOD FROM STONES 164 (2004).

53. Sari Horwitz, *Cigarette Smuggling Linked to Terrorism*, WASHINGTON POST, June 8, 2004, at A1; see also Stratfor, *Islamist Militants and Organized Crime*, June 15, 2004, at http://www.stratfor.com/products/premium/read_article.php?id=233125 (noting an “increased awareness” among officials that terrorist groups are taking part in cigarette smuggling).

54. Mark S. Hamm, *Crimes Committed by Terrorist Groups: Theory, Research and Prevention* 148, at <http://www.ncjrs.gov/pdffiles1/nij/grants/211203.pdf> (June 1, 2005).

55. For background on Abdel Rahman, see Steven Emerson, AMERICAN JIHAD 48–51 (2002); Gerald Posner, WHY AMERICA SLEPT (2003).

56. Emerson, *supra* note 16, at 224.
57. U.S. Department of Justice, Press Release, *Nineteen Charged with Racketeering to Support Terrorist Organization*, Mar. 29, 2006, at http://www.atf.gov/press/fy06press/field/032906det_mancharged.htm [hereinafter Dearborn Indictment Press Release].
58. Dan Ephron & Michael Isikoff, *Nasrallah's Men Inside America*, NEWSWEEK, Aug. 14, 2006.
59. See, e.g., 18 U.S.C. § 2318 (outlawing trafficking in counterfeit labels, illicit labels, and counterfeit documentation).
60. Ronald K. Noble, Interpol Secretary-General, Testimony before the House Committee on International Relations, *The Links Between Intellectual Property Crime and Terrorist Financing*, July 16, 2003.
61. Horwitz, *supra* note 55.
62. Abraham D. Sofaer & Seymour E. Goodman, *Cyber Crime and Security: The Transnational Dimension*, in THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM at 1, 8 (ed. Abraham D. Sofaer & Seymour E. Goodman, 2001).
63. H. H. Whiteman, *Cyber Terrorism and Civil Aviation*, in THE TRANSNATIONAL DIMENSION, ed. Sofaer & Goodman), 73, 74.
64. Seymour E. Goodman, *International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism*, in THE TRANSNATIONAL DIMENSION, ed. Sofaer & Goodman), 69.
65. *Ibid.* at 70.
66. Gabriel Weimann, CYBERTERRORISM: HOW REAL IS THE THREAT? (United States Institute of Peace Special Report No. 119, Dec. 2004), at <http://www.usip.org/pubs/specialreports/sr119.html> (last visited Dec. 13, 2006).
67. *Ibid.*
68. Rita Katz & Michael Kern, *Terrorist 007, Exposed*, WASHINGTON POST, Mar. 26, 2006, at B1.
69. SITE Institute, 007 UNVEILED: A PORTRAIT OF A CYBER-TERRORIST at 1 (2006), at <http://siteinstitute.biz/new/lrhaby007/lrhaby007.pdf> (last visited Dec. 13, 2006).
70. Katz & Kern, *supra* note 70.
71. SITE Institute, *supra* note 71, at 2.
72. *Muslim Hackers Blast Denmark in Net Assault*, COMPUTER SHOPPER, Feb. 7, 2006, at <http://www.pcpro.co.uk/shopper/news/83314/muslim-hackers-blast-denmark-in-net-assault.html>.
73. U.S. Army Training and Doctrine Command, CYBER OPERATIONS AND CYBER TERRORISM (DCSINT Handbook No. 1.02, Aug. 15, 2005), at <http://www.fas.org/irp/threat/terrorism/sup2.pdf>. The handbook discusses a number of tools that terrorists could use, pages II-8 to II-11.
74. Maj. Bill Nelson et al., CYBERTERROR: PROSPECTS AND IMPLICATIONS at xi (prepared for Defense Intelligence Agency Office of Counterterrorism Analysis, Oct. 1999).
75. Robert Walker, FBI Special Agent, Affidavit in Support of Compliant at 4, *United States v. Benevolence International Foundation*, 02 CR 0414 (N.D. Ill., Apr. 29, 2002).
76. John Roth et al., MONOGRAPH ON TERRORIST FINANCING 94 (Staff Report to the National Commission on Terrorist Attacks Upon the United States, 2004).

77. *Ibid.* at 94–95.

78. *Ibid.* at 95.

79. *Ibid.*

80. *Ibid.* at 97.

81. *Ibid.* at 98.

82. U.S. Department of the Treasury, Office of Foreign Assets Control, *Recent OFAC Actions*, Nov. 19, 2002, at <http://www.treas.gov/offices/enforcement/ofac/actions/20021119.shtml>.

83. Roth et al., *supra* note 78, at 108.

84. *United States v. Arnaout*, 282 F. Supp. 2d 838, 840 (N.D. Ill., 2003).

85. See *United States v. Arnaout*, Second Superseding Indictment; see also Roth et al., *supra* note 78, at 104–5 (summarizing evidence of BIF and Arnaout’s links to al-Qaeda’s formation).

86. *United States v. Holy Land Foundation for Relief and Development*, Indictment at 6 (N.D. Tex., July 26, 2004) [hereinafter Holy Land Foundation Indictment].

87. *Ibid.* at 5, 8.

88. *Ibid.* at 8.

89. *Ibid.* at 8–9.

90. *Ibid.* at 9.

91. *Ibid.* at 10.

92. On January 11, 2006, the first government-wide analysis of money laundering in the United States was released. See Money Laundering Threat Assessment Working Group, U.S. MONEY LAUNDERING THREAT ASSESSMENT (Dec. 2005). The report analyzes thirteen money-laundering methods, including bulk cash smuggling, trade-based money laundering, and online payment systems.

93. United Nations Office on Drugs and Crime, *Glossary of Money-Laundering Terms*, at http://www.unodc.org/unodc/money_laundering_glossary.html#M (last visited Dec. 14, 2006).

94. 18 U.S.C. § 1956.

95. Holy Land Foundation Indictment, *supra* note 88, at 26–30.

96. *Ibid.* at 27.

97. See 18 U.S.C. §§ 1956(a)(2)(A), (h).

98. See, e.g., Neil MacFarquhar, *Muslim Charity Seeks Dismissal of Charges of Terrorism*, N.Y. TIMES, Dec. 12, 2006 (describing how HLF seeks the dismissal of many of the charges against it).

99. One of the authors of this paper worked for the U.S. branch of al-Haramain for approximately a year. See Daveed Gartenstein-Ross, MY YEAR INSIDE RADICAL ISLAM (2007). For background on Wahhabism, Saudi Arabia’s austere brand of Islam, see Dore Gold, HATRED’S KINGDOM: HOW SAUDI ARABIA SUPPORTS THE NEW GLOBAL TERRORISM (2003).

100. Roth et al., *supra* note 78, at 115.

101. *United States v. Al-Haramain Islamic Foundation*, Indictment at 3 (D. Ore., 2005) [hereinafter Al-Haramain Indictment].

102. The government ultimately dropped the prosecution against al-Haramain corporation because neither of the persons indicted was in the country to stand trial. The defendants insisted that the prosecution proceed against the shell corporation while the two defendants were safely overseas. The government's motion to dismiss explains the prosecution's decision to cease prosecution of the corporation:

[I]t is the actions of the fugitive defendants [Pirouz] Sedaghaty and [Soliman] Al-But'he which are at the core of the indictment. Those actions are also the legal and factual basis for AHIF [Al-Haramain Islamic Foundation], Inc.'s status as a defendant in the indictment. Given the current state of affairs with respect to AHIF, Inc. and the fugitive defendants Sedaghaty and Al-But'he, expending the significant resources necessary to prosecute the shell corporation would be inefficient and wasteful, until at least one of the individual defendants are apprehended. Moreover, even were the government to prosecute the corporation, a conviction without the presence of one of the individual defendants would prove hollow. The Al-Haramain Islamic Foundation, Inc. has no currently available assets with which to pay a fine, and the only existing responsible corporate officers who could authorize the payment of a fine, or ensure that the corporation complies with any other type of remedial sanction in conducting its future affairs, are fugitives in the same criminal case. So, even were the government to obtain a conviction against the Al-Haramain Islamic Foundation, Inc., there is no one before the Court, or even in the United States, who could truly represent the corporate defendant. Expending the resources of the Court and prosecution to obtain this Pyrrhic victory would not be in the taxpayers' best interests.

Government's Motion to Dismiss Defendant Al-Haramain Islamic Foundation, Inc. at 7–8, *United States v. Al-Haramain Islamic Foundation, Inc.*, No. CR 05-60008-01, Aug. 4, 2005.

103. Al-Haramain Indictment, *supra* note 103, at 5; see also 31 U.S.C. §§ 5316, 5342.

104. Al-Haramain Indictment, *supra* note 103, at 9.

105. *Ibid.* at 10.

106. *Ibid.* at 15–16.

107. *Ibid.* at 7.

108. *United States v. Hammoud*, Indictment at 24–26, 33, 3:00CR147 (W.D. N.C., Mar. 12, 2002).

109. Rachel Ehrenfeld, FUNDING EVIL 138 (2003).

110. See Dearborn Indictment Press Release, *supra* note 59.

111. Testimony of Stuart Levey, undersecretary, Office of Terrorism and Financial Intelligence, U.S. Department of the Treasury, *Before the Senate Committee on Banking, Housing and Urban Affairs*, Apr. 4, 2006, at <http://www.ustreas.gov/press/releases/js4155.htm>.

112. *Ibid.*

113. Michael Cutler, *Marriage Fraud Perpetrated by Terrorists and Criminals*, COUNTERTERRORISM BLOG, Nov. 9, 2006, at http://counterterrorismblog.org/2006/11/marriage_fraud_perpetrated_by.php.

114. Thomas R. Eldridge et al., 9/11 AND TERRORIST TRAVEL 47 (Staff Report of the National Commission on Terrorist Attacks Upon the United States, 2004).

115. See 8 U.S.C. § 1324c.

116. Michael John Garcia, IMMIGRATION-RELATED DOCUMENT FRAUD: OVERVIEW OF CIVIL, CRIMINAL, AND IMMIGRATION CONSEQUENCES at 9 (CRS Report for Congress Dec. 7, 2005), at <http://www.ilw.com/immigdaily/news/2006,0130-crs.pdf>.

117. *Ibid.* at 10.

118. See Mike Tobin, *Feds Can't Find Nation to Take Damra*, CLEVELAND PLAIN DEALER, July 14, 2006.

119. *Ibid.*

120. See Jerry Seper, *Man Held in Citizenship Case*, WASHINGTON TIMES, June 7, 2005.

121. Janice Kephart, IMMIGRATION AND TERRORISM: MOVING BEYOND THE 9/11 STAFF REPORT ON TERRORIST TRAVEL (Center for Immigration Studies, Sept. 2005), at <http://www.cis.org/articles/2005/kephart.pdf>.

122. *Ibid.* at 5.

123. *Ibid.*

124. *Ibid.* at 11.

127. Michael Isikoff et al., *Terrorists in Our Midst*, NEWSWEEK, June 19, 2003, at <http://www.msnbc.msn.com/id/3067877/site/newsweek> (describing the plea-bargain agreement).

126. See Kephart, *supra* note 123, at 11.

127. 8 U.S.C. § 1151(b)(2)(A)(i).

128. 8 U.S.C. § 1325(c).

129. Kephart, *supra* note 123, at 14.

130. Mary Beth Sheridan, *Immigration Law as Anti-Terrorism Tool*, WASHINGTON POST, June 13, 2005, at A1.

131. *Convicted Fertilizer Bomb Plotters Get Life*, FoxNews.com, Apr. 30, 2007.

132. *Ibid.*

133. INTELLIGENCE AND SECURITY COMMITTEE'S REPORT INTO THE LONDON TERRORIST ATTACKS ON 7 JULY 2005 at 16, ¶ 55, May 2006, at <http://www.official-documents.gov.uk/document/cm67/6785/6785.pdf>.

134. MI5, *Links Between the 7 July Bombers and the Fertiliser Plot*, no date given, at <http://www.mi5.gov.uk/output/Page602.html>.

135. New York University Center on Law and Security, TERRORIST TRIAL REPORT CARD: U.S. EDITION, 2006, at <http://www.lawandsecurity.org/publications/TTRCCComplete.pdf>.

136. *Ibid.* at 2–3.

137. *Ibid.* at 3.

138. *Ibid.*

139. Brian Michael Jenkins, UNCONQUERABLE NATION: KNOWING OUR ENEMY, STRENGTHENING OURSELVES 29 (2006).

140. *Ibid.*

FELLOWS

R.P.Eddy , *Senior Fellow*
Tim Connors, *Director*

The Manhattan Institute's Center for Policing Terrorism (CPT) connects a core group of police departments with some of the world's most prominent tactical and academic counter terrorism experts in order to provide local law enforcement with uniquely useful knowledge products, advice, insights and services. CPT incorporates what it learns from working closely with First Preventers into best practices manuals, and advocates for enhancing the capabilities of state, tribal, and local public safety agencies as a necessary component of our national security fabric.

The Manhattan Institute is a 501(C)(3) nonprofit organization. Contributions are tax-deductible to the fullest extent of the law. EIN #13-2912529