
Follow the Money

Leveraging Financial Intelligence to Combat Transnational Threats

Matthew Levitt

In July 2006 al-Qaeda nearly executed what would have been its most devastating terrorist attack since 9/11. A group of British citizens had planned to detonate liquid explosives aboard at least ten airliners en route from the United Kingdom to the United States and Canada. British authorities were able to foil the plot, in large part because of critical financial intelligence. As a result they quickly announced plans to increase the use of financial intelligence tools to disrupt future terrorist operations. "Our aim is simple," then-Chancellor of the Exchequer Gordon Brown asserted. "Just as there be no safe haven for terrorists, so there be no hiding place for those who finance terrorism."¹

Mr. Brown described this effort as a "modern Bletchley Park." Much as intercepted communications foiled Axis military planning during World War II, tracking the financial footprints left by today's terrorists, proliferators, drug kingpins, and other adversaries can thwart attacks, disrupt logistical and financial support networks, and identify unknown operatives. Despite the fact that well-publicized uses of financial intelligence may be few and far between, it remains an integral component of international efforts to confront transnational threats. Tracking funds as they trav-

Dr. Matthew Levitt directs the Stein program on Counterterrorism and Intelligence at The Washington Institute for Near East Policy and served as Deputy Assistant Secretary of the Treasury for intelligence and analysis from 2005 to early 2007. He is the co-author, with Michael Jacobson, of *The Money Trail: Finding, Following and Freezing Terrorist Finances* (Washington Institute 2008)

el through the global financial system demands both interagency and international cooperation to develop intelligence collection, storage, and dissemination policies. Since 9/11, both U.S. and international intelligence agencies have restructured to reflect this current threat environment. Tremendous strides have been made to stop the flow of funds to illicit actors, but the international community must continue to emphasize the importance of financial intelligence in order to constrain terrorists' operating environment and pursue individual threats.

Effective but Underappreciated. Despite the effectiveness of financial intelligence (often referred to as FININT), it is underappreciated. Intelligence activities, when practiced best, are unreported. The public and pundits alike must judge efforts to combat the financing of transnational threats solely on overt actions such as U.S. Treasury designations, indictments and prosecutions. These are not the sum total of international efforts to combat terrorist financing—they are only the most visible. Diplomacy, law enforcement, and intelligence collection operations also provide a variety of other equally productive ways of combating terrorist financing.

Freezing funds will constrict the operating environment for illicit actors and disrupt their activities, while following the money trail up and down the financial pipelines of terrorists and insurgents will expose their donors and operators. Although these tools have tremendous tactical utility, it is important to recognize that combating the financing of transnational threats will

not independently defeat these threats—nor is it intended to. These tools must be part of a broader strategy that leverages all elements of national power to successfully confront and eliminate the international security threats we face today.

In the aftermath of nearly every recent terrorist attack, the utility of financial investigative tools has been reaffirmed. Financial data provided investigators with critical and early leads immediately following the attacks on 9/11, as they did following the 11 March 2004 attacks in Madrid and the 7 July 2005 attacks in London, among others. Focusing on the financing of transnational threats has other benefits as well:

Deterrent effect. It is difficult to deter hardcore operatives, yet the threat of terrorist designations can deter non-designated parties. Major donors inclined to finance extremist groups—who may be heavily involved in business activity throughout the world—will think twice before putting their personal fortunes and reputations at risk.

Preventive intelligence. Financial transfers are a matter of fact. Raising, storing, and transferring money leaves a financial trail for investigators to follow that links numbered accounts and moneychangers with individuals in terrorist organizations and cells. This is a powerful preemptive tool that allows authorities to interdict potential threats before they fully develop.

Disruptive tool. Denying terrorists, insurgents, and proliferators easy access to the international financial

system forces them to use more costly, less efficient, and often less reliable means of financing. This may not stop all plots, but it will likely frustrate illicit activities. In 1995, captured World Trade Center bomber Ramzi Yousef was flown over the twin towers on his way to a New York jail. When an FBI agent pointed out that the towers were still standing, Yousef replied, "They

(BDA), a small Macanese bank, access to the U.S. financial system. According to a U.S. government statement issued at the time, "Sources show that senior officials in Banco Delta Asia are working with [North Korean] DPRK officials to accept large deposits of cash, including counterfeit U.S. currency, and agreeing to place that currency into circulation."⁴ U.S. officials not-

Illicit actors leave financial footprints that can often be traced by virtue of having to operate within the single global financial system.

wouldn't be if I had enough money and explosives."²

All of these efforts are intelligence-driven and have proven to be quite successful. Those who follow the money are increasingly being called on to use their skills and tools against the hardest targets.

Identifying Illicit Conduct.

Identifying covert financial activity is inherently difficult given that criminals will go to great lengths to cover their tracks and evade detection. Often, only intelligence gleaned through a variety of sources and methods can inform policymakers as to which banks and humanitarian organizations should be targeted for engaging in illegal and deceptive financial practices that mask their support of terrorism. In the United States, the Treasury Department's Terrorism and Financial Intelligence branch discusses potential targets based on all-source intelligence.³

In 2005, for example, the U.S. government denied Banco Delta Asia

ed that the bank pursued activities on behalf of a "well-known North Korean front company" involved in distributing counterfeit currency and smuggling counterfeit tobacco products, and "has also long been suspected of being involved in international drug trafficking."⁵ The Treasury Department cited the bank as a "primary money laundering concern" under Section 311 of the USA Patriot Act and blocked BDA—and any other banks continuing to do business with BDA—from accessing the U.S. financial system.

Similarly, intelligence gathering efforts directed toward Iran's illicit activities revealed the use of Iranian state-owned banks, including its central bank, to secretly facilitate terrorism financing and WMD programs. For example, Iran has used Bank Saderat as a preferred means of transferring funds to terrorist organizations such as Hezbollah, Hamas, Palestinian Islamic Jihad, and the Popular Front for the Liberation of Palestine—General Command. In 2006 the Treasury Depart-

ment went public with declassified intelligence, stating that from 2001 to 2006 Iran transferred \$50 million to Hezbollah by sending funds from its central bank through Bank Saderat's London subsidiary.⁶ Iran's state-owned Bank Sepah was also blacklisted for providing extensive financial services to Iranian entities involved in WMD-related activities. According to the Treasury Department, Sepah engaged in "a range of deceptive financial practices in an effort to avoid detection," which included asking that its name be removed from international transactions.⁷ As U.S. officials have discovered, providing hard financial evidence helps to build international consensus and to "achieve a multilateral alignment of interests." Faced with hard evidence, even states that are not traditional allies cooperate to support actions that target the financing of illicit conduct.⁸

Following the Money Trail and Constricting the Operating Environment.

Illicit actors leave financial footprints that can often be traced by virtue of having to operate within the single global financial system. Following money up and down these financial pipelines helps provide critical intelligence that identifies which key nodes in these financial networks should be targeted. Using this financial intelligence as an investigative tool also allows intelligence agencies to more fully understand the scope of targeted networks. In the words of the 9/11 Commission, while stemming the flow of funds to terrorists is a useful tool, "Expect less from trying to dry up terrorist money and more from following the money for intelligence, as a tool to

hunt terrorists, understand their networks, and disrupt their operations."⁹ Following the money gives the added benefit of using confirmable streams of data to create linkages between known and unknown terrorist operatives and supporters. Though the nature of that link must still be determined, such lead information is critically important to investigators and analysts. Moreover, Treasury officials note, "While terrorist supporters may use code names on the phone, when they send or receive money through the banking system they often provide information that yields the kind of concrete leads that can advance an investigation."¹⁰ Armed with details like names and addresses, analysts can identify key actors and map their networks.

Consider the case of al-Qaeda in Iraq (AQI). Documents seized by the United States have revealed a treasure trove of information about AQI funding, organizational structure, and possible fissures within the organization. In one illuminating example, on 11 September 2007 coalition forces raided a suspected AQI safe house in Sinjar, an Iraqi town along the Syrian border. Analysis of seized documents revealed AQI managers' concern when they were unable to account for every dollar in their control.¹¹ Given the operational and security risks associated with maintaining such an extensive paper trail, these details provided insight into AQI operations and helped analysts understand the importance AQI senior leaders attached to the organization's finances.¹²

Financial intelligence has been successfully leveraged to disrupt terrorist operations, target individuals, and even

prevent attacks. For example, Philippine police reported that the Abu Sayyaf Group's plans to set off bombs in Manila and target a chemical plant in 2006 were never executed due to a lack of funds—a direct result of the group's inability to access the international financial system and the funds they were holding elsewhere.¹³ Similarly, intelligence analysis contributed to the capture of Hambali, Jemaah Islamiyah's operations chief, who masterminded the Bali bombings in 2002. Treasury officials stated that financial transactions between a known al-Qaeda suspect and a previously unknown figure in South Asia provided the link that helped locate Hambali in Thailand in 2003.¹⁴ According to Undersecretary of the Treasury Stuart Levey, the Terrorist Finance Tracking Program (TFTP) "played an important role in the investigation that even-

supporters in the United States.¹⁷

A Case in Point: The Terrorist Finance Tracking Program.

Following the 9/11 attacks, the U.S. Treasury Department initiated the TFTP to take advantage of the financial footprint left behind when terrorists and their backers transfer funds in order to enable the U.S. government to proactively identify terrorist threats. Under this program, the Treasury obtains financial data substantively connected to terrorist activity by issuing an administrative subpoena. The requested data is provided by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a Brussels-based entity responsible for conducting much of the world's bank-to-bank communications. Financial intelligence provided by TFTP has assisted in many investigations, including the

Financial intelligence has been successfully leveraged to disrupt terrorist operations, target individuals, and even prevent attacks.

tually culminated in the capture of Hambali."¹⁵ Additionally, the U.S. Treasury Department reported that a financial intelligence collection program supplied a key piece of evidence confirming the identity of a major Iraqi terrorist facilitator and financier, leading to his designation as a Specially Designated Global Terrorist (SDGT).¹⁶ Finally and perhaps most importantly, four different terrorist attacks abroad have been disrupted, according to the FBI, based in part on its investigations of the financial activities of terrorist

Van Gogh murder in 2004, a plot to attack New York's JFK airport in 2007, the Mumbai attacks in 2008, and the Jakarta hotel attacks in 2009. As of April 2010, over 1,550 TFTP reports have been shared with European Union member states.¹⁸ This shared information allows both the United States and the EU to direct local law enforcement toward specific threats. As Levey noted in April 2008, "In many circumstances we have found that our most effective tool is simply sharing information about illicit actors with other govern-

ments and members of the international private sector.”¹⁹

In June 2006 the New York Times and other media exposed the existence of the TFTP.²⁰ When SWIFT subsequently moved its U.S. facility to Europe, the United States and European Commission began negotiations to ensure data would continue to be available to TFTP. These talks were largely informed by two reports from French counterterrorism magistrate Jean-Louis Bruguiere, issued in late 2008 and early 2010, which found that TFTP was subject to significant and effective controls and safeguards, and generated significant value for counterterrorism investigations.²¹ After several fits and starts, an agreement was ultimately reached in July 2010 authorizing Treasury Department access to SWIFT’s data, with specific measures added to allay privacy concerns.

Structural Changes to Combat Illicit Finance. Structural reforms following 9/11 have enabled intelligence organizations to focus their attention on following the money. The FBI established a special branch at its headquarters, known as the Terror-

tion to handle financial intelligence issues. Even the Treasury Department, whose enforcement capabilities had been nearly eliminated with the 2003 reorganization that created the Department of Homeland Security, began to ramp up its efforts once again.

In 2004, the Treasury Department created the Office of Terrorism and Financial Intelligence (TFI) and the Office of Intelligence and Analysis.²² These offices couple authorities at Treasury with intelligence community resources and expertise to identify, disrupt, and follow the flow of illicit funds supporting terrorism or other national security threats.²³ In a sign of its demonstrated utility, the 9/11 Commission’s Public Discourse Project highlighted the government’s “significant strides in using terrorism finance as an intelligence tool.”²⁴

The Treasury Department has had an enhanced role at the center of a major national security initiative that reflects a broader shift in its post-9/11 mission. In the past, the Treasury—like other finance ministries around the world—was largely focused on economic and financial issues and often reluctant to get involved in matters of national secu-

Structural reforms following 9/11 have enabled intelligence organizations to focus their attention on following the money.

ist Financing Operations Section, to focus exclusively on tracking financial intelligence and coordinating investigations at its fifty-six field offices. The Justice Department also established an office within its counterterrorism sec-

urity. As a former Clinton State Department official noted, “Years ago, people at State would go to Treasury and say, ‘We’ve got a lot of financial muscle, we should use it to pursue political goals.’ But Treasury would always say it didn’t

want to mess around with the international financial system.”²⁵ This historic reticence has changed drastically in the last decade. For example, the Department of Treasury has been instrumental in building pressure on Iran outside of the UN. The Treasury has focused its strategy specifically on Iran’s illicit conduct—mainly its nuclear-related activity, support for terrorism, and deceptive financial practices—and the dangerous ramifications Iran could have on the integrity of the global financial system.

Interagency and International Efforts. While the creation of the TFI represented an important step forward, combating the financing of transnational threats must be an integrated, interagency effort. The Iraq Threat Finance Cell (ITFC), based in Baghdad, is a perfect example of one such interagency effort that works. Co-led by the Department of Defense and Treasury, ITFC was established in 2005 with the purpose of enhancing the collection, analysis, and dissemination of timely financial intelligence on the Iraqi insurgency. It has become a key component of interagency and Multi-National Force – Iraq (MNF-I) efforts to detect, identify, and disrupt financial networks supporting insurgent and terrorist elements operating in Iraq. The new Afghan Threat Finance Cell in Kabul, run by the Drug Enforcement Administration with the help of Defense and Treasury deputies, builds on the demonstrated success of the ITFC.

Other countries’ finance ministries have also assumed greater national security responsibilities. The G7 and G20 finance ministers released an

action plan to combat the financing of terrorism in the aftermath of 9/11.²⁶ In September 2006 the G7 finance ministers agreed to expand their focus to address money laundering in support of terrorist and WMD proliferation networks, and to concentrate on “those jurisdictions that have failed to recognize international standards”—a pointed reference to Iran’s support for terrorist organizations and efforts to attain nuclear weapons.²⁷

The British government has also been a leader in this effort, unveiling a comprehensive strategy in 2007 to combat terrorist financing and money laundering, titled *The Financial Challenge to Crime and Terrorism*. The strategy provided the British finance ministry—Her Majesty’s Treasury (HMT)—with additional tools to crack down effectively on terrorist financing in the United Kingdom. For example, the British established a “Terrorist Asset Freezing Unit” within HMT to work closely with British law enforcement and intelligence agencies. HMT was also, for the first time, allowed to use classified information to freeze assets in certain cases.²⁸

International and interagency efforts have produced tangible results. In his April 2008 testimony, Levey noted that the government’s efforts to combat terror financing “are more integrated than ever before” and have made “significant progress mapping terrorist networks” to enable the government to disrupt or deter some sources of al-Qaeda finance. Proof positive, in a May 2007 interview al-Qaeda leader Mustafa Abu al-Yazid stated “there are hundreds wishing to carry out martyrdom-seeking operations, but they can’t find

the funds to equip themselves.”²⁹ The CIA’s former Deputy Director John McLaughlin testified that the government’s success in this area was attributable to the “relentless grinding away at other essential components of the terrorist networks—the couriers, the facilitators, the fundraisers, the safe-house keepers, the technicians.”³⁰

Conclusion. The international community has undoubtedly made great headway combating the financing of various security threats. The United States’ efforts to combat terrorist financing have been particularly effective, earning an A- from the 9/11 Commission’s Public Discourse Project in 2005.³¹ Interagency efforts that threaten finance cells in Iraq and Afghanistan and improved intelligence gathering methods such as the TFTP are important factors in these successes.

Traditional efforts to combat terror financing by “seizing and freezing” terrorists’ assets are effective counterterrorism tools. But as terrorist groups continue to evolve and as additional

transnational threats arise, FININT will increasingly be called upon—Bletchley Park style—to connect the dots and prevent attacks. Making effective use of lead intelligence demands international cooperation. The recent renewal of the SWIFT agreement is an important step in maintaining one of the international community’s most effective financial intelligence tools. Meanwhile, it is imperative that we further strengthen our commitment to strategies aimed at making it more difficult for illicit actors to raise, launder, and access the funds they need to carry out operations. There is much that the United States can do on its own, yet in the words of Assistant Secretary of the Treasury David Cohen, “When the community of nations works together, in a coordinated fashion, to combat terrorist financing, we all benefit.”³² The public should take comfort in knowing that both financial intelligence tactics—seizing funds and following the money trail—are being pursued, even if only one makes the daily paper.

NOTES

1 “Brown outlines terror crackdown,” BBC, 10 October 2006, Internet, http://news.bbc.co.uk/2/hi/uk_news/politics/6035861.stm (date accessed: 8 January 2011).

2 Benjamin Weiser, “Suspected Chief Plotter in Trade Center Blast Goes on Trial Today,” *New York Times*, August 4, 1997, <http://www.nytimes.com/1997/08/04/nyregion/suspected-chief-plotter-in-trade-center-blast-goes-on-trial-today.html> (date accessed: 8 January 2011).

3 Remarks by Treasury Assistant Secretary for Terrorist Financing Patrick M. O’Brien, Washington Institute for Near East Policy, 27 February 2008, Internet, <http://www.washingtoninstitute.org/templateCo5.php?CID=2724> (date accessed: 8 January 2011).

4 U.S. Department of the Treasury, “Treasury Designates Banco Delta Asia as Primary Money Laundering Concern under USA PATRIOT Act,” 15 Sep-

tember 2005, <http://www.ustreas.gov/press/releases/js2720.htm> (date accessed: 8 January 2011).

5 *Ibid.*

6 U.S. Department of the Treasury, “Treasury Cuts Iran’s Bank Saderat Off From U.S. Financial System,” 8 September 2006, <http://www.ustreas.gov/press/releases/hp87.htm> (date accessed: 8 January 2011).

7 U.S. Department of the Treasury, “Prepared Remarks of Stuart Levey Under Secretary for Terrorism and Financial Intelligence On the Designation of Bank Sepah for Facilitating Iran’s Weapons Program,” 9 January 2007, <http://www.treas.gov/press/releases/hp220.htm> (date accessed: 8 January 2011).

8 Testimony of Daniel Glaser, Deputy Assistant Secretary for Terrorist Financing and Financial Crimes, before the House Committee on Foreign Affairs Subcommittee on the Middle East and South Asia and the Subcommittee on Terrorism, Nonpro-

liferation, and Trade, 17 April 2008, <http://www.treas.gov/press/releases/hp933.htm> (date accessed: 8 January 2011).

9 9/11 Commission, "Final Report of the National Commission on Terrorist Attacks Upon the United States: Executive Summary," http://govinfo.library.unt.edu/911/report/911Report_Exec.htm (date accessed: 8 January 2011).

10 Testimony of Stuart Levey, Undersecretary for Terrorism and Financial Intelligence, U.S. Department of the Treasury, before the House Financial Services Committee on Oversight and Investigations, 11 July 2006, <http://www.treas.gov/press/releases/hp05.htm> (date accessed: 8 January 2011).

11 The Sinjar documents show that the AQI's border emirate spent \$727 on food during a two-month period, in addition to tracking a number of other different subcategories for expenditures, including salaries, weapons, document forgeries, and smuggling costs.

12 Brian Fishman, ed., "Bombers, Bank Accounts, and Bleedout: Al-Qai'da's Road in and Out of Iraq," *Harmony Project*, Combating Terrorism Center at West Point, 2008, Internet, http://www.ctc.usma.edu/harmony/pdf/Sinjar_2-Jul_23.pdf (date accessed: 8 January 2011).

13 "Militants in SE Asia Rely on Donations – Experts," Reuters, 9 July 2008.

14 Eric Lichtblau and James Risen, "Bank Data is Sifted in by U.S. in Secret to Block Terror," *New York Times*, 23 June 2006, Internet <http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=print> (date accessed: 8 January 2011).

15 Elizabeth Kelleher, "U.S. Defends Use of Bank Messaging System to Track Terrorists," *The Washington File*, Bureau of International Information Programs, U.S. Department of State, 23 June 2006, Internet, <http://www.america.gov/st/washfile-english/2006/June/20060623173804berehelleko.1277277.html> (date accessed: 8 January 2011).

16 U.S. Department of the Treasury, "Treasury Designates Financial Supporter of Iraqi Insurgency," 17 June 2005, Internet, <http://www.treas.gov/press/releases/js2500.htm> (date accessed: 8 January 2011).

17 Federal Bureau of Investigation, Testimony of John S. Pistole before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, "Identifying, Tracking and Dismantling the Financial Structure of Terrorist Organizations," 25 September 2003, www.fbi.gov/congress/congress03/pistole092503.htm.

18 U.S. Department of the Treasury, "Assistant Secretary for Terrorism and Financial Intelligence David S. Cohen, Remarks to the Washington Institute for Near East Policy," 7 April 2010, Internet, <http://www.washingtoninstitute.org/templateC07.php?CID=522> (date accessed: 8 January 2011).

19 U.S. Department of the Treasury, "Under Secretary for Terrorism and Financial Intelligence Stuart Levey Testimony Before the Senate Committee on

Finance," 1 April 2008, <http://www.treas.gov/press/releases/hp898.htm> (date accessed: 8 January 2011).

20 *The New York Times* would later run an apology. See Byron Calame, "Can 'Magazines' of The Times Subsidize News Coverage, Banking Data: A Mea Culpa," *New York Times*, 22 October 2006, <http://www.nytimes.com/2006/10/22/opinion/22pubed.html?pagewanted=2&r=2>. For more on the protections built into the TFTP program, see States Department of the Treasury, "Statement of Undersecretary Stuart Levey on the Terrorist Finance Tracking Program," 23 June 2006, <http://www.treas.gov/press/releases/js4334.htm>. Also see Elizabeth Kelleher, "U.S. Defends Use of Bank Messaging System to Track Terrorists," *The Washington File*, Bureau of International Information Programs, United States Department of State, 23 June 2006, Internet, <http://www.america.gov/st/washfile-english/2006/June/20060623173804berehelleko.1277277.html> (date accessed: 8 January 2011).

21 U.S. Department of the Treasury, "Assistant Secretary for Terrorism and Financial Intelligence David S. Cohen, Remarks to the Washington Institute for Near East Policy," 7 April 2010, Internet, <http://www.washingtoninstitute.org/templateC07.php?CID=522> (date accessed: 8 January 2011).

22 U.S. Department of the Treasury, "Bush Administration Announces Creation of New Office in Ramped Up Effort to Fight the Financial War on Terror," press release, 8 March 2004, Internet, www.treas.gov/press/releases/js1219.htm (date accessed: 8 January 2011).

23 OFAC and FINCEN participate in the process of enforcing sanctions and tracking criminal organizations, but they continue to rely on the intelligence organizations within the U.S. government (such as the TFI) to provide the intelligence necessary to carry out their office missions."

24 Thomas H. Kean et al., "Final Report of the 9/11 Commission Recommendations," 9/11 Public Discourse Project, December 5, 2005, http://www.9-11pdp.org/press/2005-12-05_report.pdf.

25 Bay Fang, "Treasury wields financial sanctions; US strategy straddles the line between diplomacy, military might," *Chicago Tribune*, 23 April 2007.

26 Statement of G-7 Finance Ministers and Central Bank Governors, Washington, D.C., 6 October 2001; Statement of G-20 Finance Ministers and Central Bank Governors, Ottawa, Ontario, Canada, 17 November 2001.

27 Statement of G-7 Finance Ministers and Central Bank Governors, Singapore, 16 September 2006.

28 "Move to combat terror gang funding," *London Evening Standard*, 28 February 2007; "The Financial Challenge to Crime and Terrorism," February 2007.

29 U.S. Department of the Treasury, "Under Secretary for Terrorism and Financial Intelligence Stuart Levey Testimony Before the Senate Committee on Finance," 1 April 2008, <http://www.treas.gov/press/releases/hp898.htm>.

FOLLOW THE MONEY

30 Testimony of John McLaughlin, before the Senate Foreign Relations Committee, "The Changing Face of Terror – A Post 9/11 Assessment", 6 June 2006, Internet, <http://www.senate.gov/~foreign/testimony/2006/McLaughlinTestimony060613.pdf> (date accessed: 8 January 2011).

31 U.S. Department of the Treasury, "Under Secretary for Terrorism and Financial Intelligence Stuart Levey Testimony Before the Senate Committee

on Finance," 1 April 2008, Internet, <http://www.treas.gov/press/releases/hp898.htm> (date acce.

32 Remarks by Assistant Secretary for Terrorism and Financial Intelligence David S. Cohen, Washington Institute for Near East Policy, 7 April 2010, Internet, <http://www.washingtoninstitute.org/templateCo7.php?CID=522>. (date accessed: 8 January 2011).