21st Century Intelligence

The Need for a One-Team-One-Fight Approach

BY LESLIE IRELAND

We've been through this before. Now we're just waiting to see how soon it fails." As I put down the phone, the dismissive words about integration from one of the Iran watchers within the Intelligence Community (IC) resonated in my ears. In November 2005, less than two months into my role as the first Iran Mission Manager for the Director of National Intelligence (DNI), I was face-to-face with the unfolding skepticism the IC felt about the implementation of the Intelligence Reform and Terrorism Prevent Act (IRTPA) of 2004 that reorganized the Community and created the DNI position.[1] In retrospect, I am thankful for those words. They braced me for the challenges that lay ahead and helped shape my approach to integrating IC efforts on Iran. They were not far from the truth. I had been part of a number of "tiger" or "hard target" teams assembled to tackle particular intelligence challenges. They saw success in discreet areas that tapered off after the team was disbanded or new concerns siphoned off resources. The challenge for integration now was how to make it sustainable and enduring beyond changes in leadership. I am also thankful for the person who spoke those words. By the end of my three-year tenure, they were a champion for integration and a big supporter of the mission management concept.

The Robb–Silberman Commission—commonly known as the Iraq Weapons of Mass Destruction Commission, identified this concept in its March 2005 report to President George W. Bush that famously concluded the "IC was dead wrong in almost all of its pre-war judgements about Iraq's weapons of mass destruction. This was a major intelligence failure." The IC was "not a community in any meaningful sense," rather, it was a "loose confederation of 15 separate intelligence entities." No single individual or office within the IC was responsible for getting the answers right on the most pressing intelligence questions. According to the report,

Ms. Leslie Ireland is a former Assistant Secretary of the Treasury and was the first National Intelligence Manager for Iran.

IC elements were "allocating among intelligence priorities in a way that seemed sensible to them, but were not optimal for a community-wide perspective." In essence, the Community's aggregate support was far less than the sum of its parts.

As the Iran Mission Manager, I could see across the business lines of the other 16 intelligence agencies as well as Iran's business lines, such as support for terrorism, development of weapons of mass destruction, and foreign policy objectives.[3] Iran does not address those issues in isolation—why should we? And it was not just important that I be able to see across the entire Iran problem set. A core team of Iran watchers from across the IC—responsible for collection and analysis—needed that visibility as well. Working together, and armed with knowledge of each other's capabilities and the direction of U.S. policy, we moved forward on addressing strategic intelligence gaps.

The goal of this integration was to provide the President and his national security team with timely and accurate information from which to make informed policy decisions about Iran. For the first time, all intelligence agencies were welcome to contribute intelligence and analysis to the President's Daily Brief (PDB), once the nearly exclusive purview of the CIA.[4] Mission managers represented the IC, and any differing views within the Community, at National Security Council deputies meetings that informed U.S. policy discussions. This integrated Iran effort also allowed the IC to concentrate on a honed set of priorities keyed to the direction of U.S. policy. In 2005, the Iran mission was hampered by a plethora of "number one" priorities. So many, in fact, that some collectors were conflicted about where to place resources. The value of establishing priorities on enduring challenges cannot be underestimated. Building or developing capabilities in collection and analysis can take years. A colleague at one intelligence agency recently told me that the Iran priorities set out in 2006 caused them to develop the accesses necessary to provide the intelligence the Obama Administration needed to enter and conclude negotiations with Iran under the Joint Comprehensive Plan of Action.[5]

In 2006, Under Secretary Stuart Levey, the first head of Treasury's Office of Terrorism and Financial Intelligence (TFI), approached me to ask that intelligence collectors expand their aperture to include information on Iranian financial flows. The Treasury Department wanted to increase its efforts to use sanctions as part of U.S. policy on Iran. The status of the dollar as the world's reserve currency, the central role of the U.S. financial sector in the global economy, and the aversion bankers have for negative risk make Treasury's ability to cut-off access to the U.S. financial sector a powerful and persuasive tool for the U.S. government. The impact on the target of sanctions can be powerful and persuasive, too. For example, sanctions can make it more difficult for terrorists to raise and/or move money and to conduct operations, frustrate the ability of proliferators to obtain critical materials and equipment, or even cause broader negative impact on a country's economy. Treasury's newly-minted intelligence element, the Office of Intelligence and Analysis (OIA) under the direction of Assistant Secretary Janice Gardner, needed the additional financial intelligence to provide the unique analysis

Treasury policy and enforcement would use to support sanctions programs.[6]

Treasury analysts knew well the value of following financial flows. Money moves for a specific purpose between individuals or organizations that know and trust each other. There is nothing casual about the relationship. It provides insights about personalities, relationships, networks, and patterns of life or activity. Stopping what seems like a small amount of money can have a significant impact, particularly for the individual or organization depending on it. And like water running through a river, money finds a way to move again even after it hits an obstacle. Following "the money" is a full time job. This early work by Treasury/OIA would lead to near-term and long-term integrated efforts that would move the use of tracking money flows beyond sanctions to addressing the broad range of threats to U.S. national security. That near-term integration would be in an active war zone—Iraq.

Multi-National Forces–Iraq (MNF–I) was charged with, amongst other tasks, building Iraqi security forces from scratch and enabling them to be carry more of the burden themselves. In the face of the insurgency that started in summer 2003 and intensified in spring 2004, it was particularly challenging. In a September 26, 2004 *Washington Post* Op-ed Lieutenant General David Petraeus, then the Commander of Multi-National Security Transition Command–Iraq (MNSTC–I), said trying to build Iraqi security forces in the face of multiple insurgent groups was "akin to repairing an aircraft while in flight—and while being shot at."[7] Something had to be done to give MNSTC–I and the nascent Iraqi security forces much needed breathing room. In 2005, the National Security Council directed the creation of the Iraq Threat Finance Cell (ITFC) to "enhance the collection, analysis, and dissemination of timely and relevant financial intelligence to combat the insurgency." Under the joint leadership of Treasury/OIA and DOD, the ITFC for the first time integrated military, civilian and law enforcement analysts in theater who used financial information to define and track insurgent networks, help inform counterinsurgency operations and DOD debriefings of detainees, and aid efforts by the Government of Iraq to build its own counter-threat finance capabilities. The cell grew to more than 30 officers at its height. In addition to analysts from Treasury/OIA and U.S. Central Command, the cell enjoyed support from the Defense Intelligence Agency, Central Intelligence Agency, Federal Bureau of Investigation, Secret Service, Immigration and Customs Enforcement, as well as the Internal Revenue Service.

The ITFC's location, first in Baghdad and later at additional sites in Iraq, gave it the advantage of integrating analysts with each other, sitting side by side, and in many cases with military operators. Analysts who served in the cell noted that stovepipes frequently found in Washington D.C. came down and the sense of urgency and mission of the war zone fostered an invaluable one- team-one-fight spirit. There were lessons learned as well. Financial information was not commonly collected and frequently left behind during sensitive site exploitation. That is not surprising. Following financial flows was a relatively new art and financial information can be found in many places. Ledgers and bank account statements are well known, while financial trails can be found in travel data, on cell phones, and in pocket litter. As analysts sensitized collectors, more and more information became available. However, technology lagged and analysts lacked adequate tools to exploit financial data to the maximum amount possible. The ITFC was best at triaging information as it came in, but did not have the search capability they needed.

The success of the ITFC was replicated in Afghanistan with the creation in 2008 of the Afghan Threat Finance Cell (ATFC) under a Drug Enforcement Agency (DEA) lead, with Treasury and DOD as co-deputies. It grew to nearly 60 integrated analysts, special agents, and personnel from the IC, law enforcement, and every branch of the military. The ATFC embedded with military commands across Afghanistan and provided actionable intelligence to civilian and military leaders in theater. Co-location helped improve the targeting of insurgents' financial infrastructure, yielded tens of thousands of documents and led to raids, detentions, arrests, and extraditions. Like their counterparts in the ITFC, analysts in the ATFC needed to sensitize collectors to seize financial information during raids. Unlike their counterparts, however, they benefited from new analytical tools developed by DARPA specifically for the ATFC's unique financial mission to ingest structured and unstructured data and perform data visualization. The cell shared its findings outside of Afghanistan through IIRs (Intelligence Information Reports), enabling additional actions, including sanctions. The ATFC also worked with Afghan authorities to build an independent capability to track and disrupt illicit financial activity. Kirk Meyer, the DEA agent who stood up the ATFC, and his Treasury Deputy, Frank Calestino, were finalists for the 2010 Samuel J. Heyman Service to America Medal. This was clear recognition of the contribution the ATFC made the U.S. and allied efforts in Afghanistan and a testament to the value of integration.

DEA's lead role apparently reflected the perceived significance of the Afghan drug trade as a funding source of terrorist and insurgent groups. As analysts in the cell began digging into financial flows, a different picture emerged. According to Kirk Meyer, "you couldn't just look at the Taliban, you couldn't just look at corrupt officials, and you couldn't just look at the drug traffickers. Even though on the surface, these groups were at odds, in reality, everybody was in the money game to some degree. You had corrupt Afghan officials; you had bad actors in the Afghan business and financial sector, the Taliban and drug traffickers, all of whom were frequently acting in tandem. So you could look at one thing, say a *hawala*, or a bank, or a drug trafficker, and the connections would spider out and connect to other illicit areas in operations in Afghanistan."[8]

Afghanistan's banking system was rudimentary and relied on an informal system of hawalas to conduct some 80 percent of the financial transactions in the country. Hawalas are used for many legitimate transactions, but are also exploited by terrorists and insurgents to move large amounts of money quickly, cheaply, and with little or no oversight. Following illicit transfers through hawalas would be one of the ATFC's challenges. Little did they realize they would uncover massive corruption in the fledgling formal banking system. The ATFC learned that several senior executives at Kabul Bank, the largest private bank in

Afghanistan, were diverting bank deposits to Afghani elites in "loans" that were not being repaid. It was, in essence, a pyramid scheme. Depositors were average Afghani citizens, NGOs, and most anyone else who needed banking services in the country. That included the United States and the International Security Assistance Force, which used Kabul Bank to transfer the money to pay the salaries of Afghan Government employees, mostly in the military and police. Of the roughly $1.2–.3 billion in deposits, more than $800 million was stolen. In addition to aiding military efforts against insurgent and terrorist groups, the ATFC played an important role in exposing high-level corruption that threatened U.S. and allied measures to build Afghani governance and security capacities.

While I have just discussed the benefits of successful interagency cooperation, integration is much easier said than done. Agencies and institutions need to trust each other and have confidence that their information and capabilities will be treated with respect and care. If I share my information, will I risk losing a source? Will my ability to prosecute a law enforcement case be compromised? Can a civilian organization truly appreciate the sensitivity of military operations? The examples of integration outlined above all share one feature: a sense of urgency. Once urgency is gone, or people return to their home organizations, the natural tendency is to revert to silos. Integration is not sustainable without a change in culture. The interagency mission management concept—now embodied in DNI National Intelligence Managers (NIMs)—is an important vehicle for such change in the national security arena.

In 2008, DNI James Clapper made IC integration the core mission of the ODNI. During his tenure, he established 17 NIMs—formerly known as Mission Managers—to cover a range of regional and functional missions. Today, NIMs play a lead role in honing the IC's focus on national security challenges. As IC representatives in interagency discussions they have a clear view of the direction of policy—that can change with world events or elections—and work with the IC to prioritize collection and analysis resources accordingly. NIMs champion their mission priorities within the ODNI. They are best positioned to inform discussions about the resource trade-offs that always come when there is a change in focus or emphasis. Lastly, NIMs and their staffs come from all parts of the Intelligence Community. This reinforces integration and leads to professional relationships that will benefit the employee and the IC for years to come.

NIMs are also powerful advocates for new missions. In 2010, DNI Clapper added Threat Finance (TF) as a mission area and created the NIM–TF, a position I also filled until I retired in November 2016. When I began that role, the intelligence and law enforcement professionals who used financial flows more closely resembled the "loose confederation" that the Robb–Silberman Commission described. In 2005, many saw financial information as a niche capability exclusive to Treasury's sanctions programs or for use in theater, such as by the ITFC and ATFC. Today, "following the money" is increasingly used to address the broad range of national security concerns facing the United States. That is due, in part, because having a NIM allowed the IC to tackle two of the challenges that emerged in Baghdad and

Afghanistan—insufficient analytical tools and inconsistent collection focus. We worked with DARPA to develop a customized government-owned tool specific to mining financial data. It was based largely on the work DARPA did for the ATFC. In addition, we were able to introduce and elevate threat finance as an intelligence collection focus. It was gratifying to see what began with the ITFC and ATFC grow into a broader integrated effort.

In my experience, organizations are more likely to enthusiastically participate in integration efforts when they address a gap or meet an unmet need. The IC Information Technology Enterprise—IC ITE, pronounced "eye sight"— is one example of this. For the first time, the IC will be able to easily and securely share information, technology and resources across a common IT infrastructure. IC ITE will mean cost savings for larger agencies. Smaller ones will have access to tools, applications and innovations that their IT budgets normally could not afford. The overall mission will benefit from the changes in communication, collaboration and information sharing. IC ITE is only possible because of IC leadership committed to contributing their resources, sharing their information and adopting the common IT infrastructure within their agencies. I hope the IC continues pursuing IC ITE. It will play an important role in reinforcing a culture of integration in the IC.

Looking forward, I believe an integrated model will be critical to addressing the challenges posed by cyber threats. While I was at the Treasury Department, I watched the capabilities of the department and its interaction with the financial services sector on cyber threats grow. This sector, perhaps more than any other part of U.S. critical infrastructure, faces a broad range of malicious cyber activity, including theft of funds and sensitive client information, ransomware, breaches in the retail sector, disruptive or destructive attacks and insider threats.[11] For example:

- In February 2016, cyber actors stole $81 million from Bangladesh Bank's New York Federal Reserve account using stolen credentials and laundered the money through several Filipino casinos.
- Cyber criminals have grown more sophisticated in their attacks on ATMs, where they use both physical and remote means to steal cash directly from machines. Attacks against ATMs in Thailand and Taiwan last year netted close to $2.5 million for the thieves, and attacks have also occurred across Europe with as of yet undisclosed results.
- The financial sector is impacted by second-order effects from cyber attacks on retailers—both brick and mortar and online stores—that remain attractive targets. Think about the breaches at Target or Home Depot.
- In 2013, three major South Korean banks came under cyber attack where customers were unable to access funds through ATMs and some 40,000 computers were rendered unusable, also known as being "bricked." From 2011–13, there was a lengthy campaign of distributed denial of service attacks against numerous U.S. financial institutions, where public-facing

websites were overwhelmed in the face of a coordinated flood of data.

- Cyber criminals have been seen on the dark web actively soliciting bank employees in England and Mexico to conduct fraudulent activities. In another instance, a threat actor advertised alleged access to insiders at two Brazil-based financial institutions who could provide sensitive information about clients, including account passwords and personally identifiable information.

These cyber threats to the financial sector are critical because they threaten to erode trust and confidence, both between financial institutions and customers, and between institutions themselves. Trust and confidence are the lifeblood of the financial sector. In the extreme, their loss could lead to consumer panic. The sector, and I would argue our economy, would be at risk of not continuing to function. In fact, due to the global nature of the financial sector, cyber threats present a worldwide risk.

I believe the mission management model is well-suited to the challenges presented by cybersecurity in the financial sector. Take, for example, the Avalanche network, so called by law enforcement because of the aggressive onslaught of attacks cyber criminals conducted primarily against banks. After operating out of Eastern Europe for nearly four years, it was dismantled in an international law enforcement operation in

DEA

Burning hashish seized in 2008 during a joint Afghan, NATO, and DEA operation.

late 2016. The network offered cyber attacks as a criminal service to customers globally, advertising through postings on exclusive underground online criminal fora. There were multiple criminal campaigns ongoing simultaneously. Services included phishing attacks that delivered ransomware, banking trojans that stole sensitive banking credentials later used to conduct fraudulent wire transfers, and a network of "mules" who purchased goods to launder stolen funds. This range of activity would cut across several departments in a financial institution, including IT systems, fraud departments, and anti-money laundering (AML) sections. The Avalanche network undoubtedly understood the totality of its efforts against the financial sector, but were the affected institutions in a position to connect the dots, particularly if cyber attacks impacted both domestic and global operations?

A cybersecurity "mission manager" would be responsible for overseeing cyber-related activity across a financial institution. The day-to-day operations to detect, deter, and mitigate attacks would remain within the departments themselves. When I was the Iran Mission Manager, intelligence agencies knew that I acted under the authority of the DNI and reported directly to him on the status of efforts on Iran. In a financial institution, a cybersecurity mission manager would need to act with the authority of the CEO and report directly to him/her about the scope of cyber threats facing a financial institution. This process would better inform discussions and decisionmaking in the C-Suite and by the Board of Directors. For example, in the face of a successful ransomware attack, the C-Suite and Board of Directors would need to quickly weigh whether to pay a ransom. Does the bank have the recovery and resiliency capabilities to resume operations if its data remains encrypted? Or, must it pay? If the bank does pay, can it be certain that criminals will release its data? Will it be marked as a victim who will pay in the future?

Information sharing is a critical part of integration. The need is no different in the face of cybersecurity threats. The financial sector has set the gold standard for cybersecurity information sharing since it established one of the first Information Sharing and Analysis Centers (ISACs) almost 20 years ago. Recently, the heads of the eight U.S.-chartered banks considered to be "globally systemically important banks" (G-SIBs) took this a step further and created the Financial Systemic Analysis and Resilience Center (FSARC).[10] The goal of the FSARC is to integrate the work of threat intelligence teams to go beyond protection of individual institutions to systemic defense of the financial sector against current and emerging cybersecurity threats. The Center is being stood up in Virginia, adjacent to the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) to facilitate greater information sharing with the U.S. Government. A smaller presence is being stood up in New York to facilitate collaboration with the law enforcement community. The question still remains about the extent of information sharing in the FSARC. As I know from my time in government, intentions can be overshadowed by institutional stovepipes, different interpretation of authorities and outright restrictions on sharing.

The Intelligence and National Security Alliance (INSA) has developed a concept to take public-private cooperation and integration on cybersecurity a step further.[10] INSA's Financial Threats Task Force recently drafted a proposal recommending that elements from DHS, Treasury, FBI, and the Secret Service partner with essential financial institutions to establish a public-private cybersecurity/information assurance program unique to the financial sector. It would be modeled after the Defense Industrial Base (DIB) Cybersecurity Program (CS), which began in 2007 between DOD and its core contractors and was expanded in 2012 to other members of the DIB. Members are able to access a range of services and information through the Defense Cyber Crime Center (DC3), including information about cyber activity in real-time through a Secret-level system called DIBNet. The DC3 "fosters a cyber threat sharing information partnership with DIB participants by offering analytic support, incident response, mitigation and remediation strategies, malware analysis, and other cybersecurity best practices." A similar "FINnet" system which allows for real-time sharing of classified cyber attack indicators and defense measures between the government and the private sector would seem to be warranted, given the critical role the financial sector plays in the strength of the United States.

As with all successful integration, a "FINnet" most likely will require a culture change. The DIB was accustomed to operating in a classified environment when DIBNet was created. Companies already had facilities to handle classified information and equipment to conduct secure communications, as well as employees with government-granted security clearances. While the financial services sector is experienced in sharing information about cyber security threats through the FS–ISAC, it does not have an intelligence-driven approach to security. The FSARC could be an important step in that direction. Intelligence analysts and collectors are some of the best informed on intentions and capabilities of threat actors and could provide unique insights to members of the FSARC. In return, experts from the financial sector could help intelligence professionals hone their focus on the areas that are most critical. Security clearances for members of the Center would be very beneficial.

If we truly believe cybersecurity is a global threat, we will need to consider a global solution. Cyberattacks know neither boundaries nor victim nationality. The financial sectors in Asia and Europe—that host the additional 22 G-SIBs—should consider an FSARC-like approach, if they have not done so already. This could lead to global sharing of unclassified information on cyber threats to the financial sector. During my tenure at the Treasury Department, I participated in the Treasury-led series of public-private tabletop exercises known as the Hamilton Program, which led participants from the financial sector, regulatory agencies and the government (including policy, law enforcement, and the intelligence communities) through simulated cyber incidents. One of the exercises was cross-Atlantic. All of them were very instructional in revealing faulty assumptions, managing expectations and defining roles in the event of a cyber incident. Participants walked away with a clear sense of areas for improvement.

Looking for a global solution could eventually mean giving non-U.S. citizens access to classified information on a Secret-level network. Many financial institutions—particularly those with a global presence—employ foreign nationals. Moreover, protecting the interconnected global financial system could eventually require including the 22 G-SIBs in Asia and Europe in a FINnet system. Hopefully, those countries would have intelligence to share on cyber threats as well. Consideration for protecting sources and methods will impact the intelligence any country would provide, as it should.

Personally identifiable information (PII) must be protected in any information sharing circumstance, whether domestic or global. The Cybersecurity Information Sharing Act (CISA), passed in December 2015, calls on the government to develop procedures to share cybersecurity threat information between the public and private sectors. PII that does not link a person directly to cybersecurity threat cannot be shared. Privacy and civil liberties guidelines placing limits on the receipt, use, retention and dissemination of PII must be reviewed every two years. Critics of CISA vigorously question whether these measures go far enough to protect privacy. It will be important for all parties involved to proceed carefully and ensure that effective mechanisms and processes to strip out PII are in place. A pilot project testing the concept of public-private information sharing between the government and the financial sector, perhaps at the unclassified level, could be an important test bed for demonstrating how PII would be protected and determining how often and under what circumstances PII would need to be shared.

My last decade of Federal Service convinced me that approaching U.S. national security interests from a one-team-one-fight perspective is the only path to take. The IC needs to develop a culture of integration, and the ODNI is positioned to lead the way through continued support of NIMs and the IC ITE. That integration needs to extend to a deepening public-private partnership. I cannot think of a more critical area to begin than cybersecurity. We cannot wait for a "cyber 9/11" to give us the urgency to increase information sharing. The level of integration I am advocating has not been tried before. Failure is not an option. "We've been through this before. Now we're just waiting to see how soon it fails?" Not again. PRISM

Notes

[1] The U.S. Intelligence Community is comprised of 17 organizations. This includes two independent agencies—the Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA); eight Department of Defense elements—the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial- Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and intelligence elements of the four DOD services; the Army, Navy, Marine Corps, and Air Force. Also included are seven elements of other departments and agencies—the Department of Energy's Office of Intelligence and Counter-Intelligence; the Department of Homeland Security's Office of Intelligence and Analysis and U.S. Coast Guard Intelligence; the Department of Justice's Federal Bureau of Investigation, and the Drug Enforcement Agency's Office of National Security Intelligence; the Department of State's Bureau of Intelligence and Research; and the Department of the Treasury's Office of Intelligence and Analysis. Before signing the IRTPA President George W. Bush said, "A key lesson of September the 11th, 2001 is that America's intelligence agencies must work together as a single, unified enterprise."

[2] The Commission in its March 2005 report to the U.S. President concluded that the "IC was dead

wrong in almost all of its pre-war judgements about Iraq's weapons of mass destruction. This was a major intelligence failure." Established by President Bush in Executive order 13328 nearly one year prior, the Commission in its report looked beyond Iraq in their review of IC capabilities to assess state and nonstate proliferation threats. The Commission acknowledges the nomination of U.S. Ambassador to Iraq John Negroponte as first Director of National Intelligence as a move toward making the DNI responsible for integrating the IC, which did not include the DEA until February 2006. A full copy of the report is available at < https://fas.org/irp/offdocs/wmd_report.pdf>.

[3] DNI John identified four areas for mission management: Iran (myself); North Korea (Ambassador Joseph DeTrani); WMD (Ambassador Kenneth Brill, Director of the Non-Proliferation Center (NCPC); and Counterterrorism (Admiral Scott Redd, USN (ret.), Director of the National Counterterrorism Center (NCTC).

[4] Writing for the President is hard—as it should be—and it has taken time for the broader IC to contribute to the PDB. Being able to verbally communicate differences was that much more important.

[5] In July 2015, the five permanent members of the UN Security Council—China, France, Germany, Russia, the United Kingdom, and the United States—along with the European Union and the Islamic Republic of Iran, reached a Joint Comprehensive Plan of Action to ensure Iran's nuclear program will be exclusively peaceful.

[6] In 2005, Treasury was leveraging several Executive Orders (EOs) to sanction Iran. It targeted Iran's support for terrorism largely through EO 13224, which authorized the U.S. government to "designate and block the assets of foreign individuals and entities that commit, or pose a significant risk of committing, acts of terrorism," and Iran's 1984 designation as a State Sponsor of Terror. Treasury targeted Iran's WMD and ballistic missile developments primarily through EO 13382, which authorized the U.S. Government to freeze "the assets of proliferators of weapons of mass destruction and their supporters."

[7] David H. Petraeus, "Battling for Iraq," *The Washington Post*, September 26, 2004, available at < http://www.washingtonpost.com/wp-dyn/articles/A49283-2004Sep25.html>.

[8] This paper looks at the value of integration that the ITFC and ATFC represent. For a fuller treatment of the concept of Threat Finance Cells supporting military operations see: J. Edward Conway, "Analysis in Combat: The Deployed Threat Finance Analyst," Small Wars Journal, July 5, 2012. For an in-depth view of the creation of the ATFC, see the 2014 interview of Kirk Meyer, conducted by Global ECCO Director Michael Freeman and CTAP coordinator Amina Kator-Mubarez as part of the Combating Terrorism Archive Project (CTAP), and published in the Combating Terrorism Exchange Quarterly, Vol. 4, no. 3, August 2014. Hawala is an informal financial system based on honor and trust. Simply put, money is transferred through a network of money brokers, or hawaladars. A customer gives money to a hawaladar in one city with instructions on passing it to another customer, many times in a foreign city. The trusted hawaladar on the other end contracts the second customer to collect their money, minus a small commission.

[9] The financial sector is one of 16 critical infrastructure sectors under the protective mission of the Department of Homeland Security. The Treasury Department is the Sector Specific Agency responsible for representing the financial services sector within the U.S. Government.

[10] The U.S.-chartered G–SIBs are Bank of America, Bank of New York Mellon, Citigroup, Goldman Sachs, JP Morgan Chase, Morgan Stanley, State Street, and Wells Fargo. A G–SIB is defined as "a financial institution whose distress or disorderly failure, because of its size, complexity and systemic interconnectedness, would cause significant disruption to the wider financial system and economic activity." An additional 22 banks in Japan, China, Belgium, France, Germany, the Netherlands, Italy, Spain, Sweden, Switzerland, and the United Kingdom are currently considered to be globally systemically important.

[11] INSA is a Washington D.C.-based nonpartisan, nonprofit membership organization that provides venues for developing and promoting collaborative, public-private approaches to national security challenges. It established the Financial Threats Task Force in 2015 to "strengthen public-private cooperation and information sharing regarding the broad ranges of threats faced by the government, the financial services sector, and other industries, which include cybersecurity, money laundering, terrorist finance, transnational organized crime, corruption, and confidence in U.S. and global financial infrastructure."