

Financial Tools and Sanctions: Following the Money and the Joumaa Web

Robert ("J. R.") McBrien

In 2011, two units of the U.S. Treasury Department, acting on DEA-led investigations, imposed closely aligned financial countermeasures to expose, disrupt, and incapacitate a major international drug trafficking and money laundering network linked to the terrorist organization Hezbollah. The network, headed by Lebanese national Ayman Joumaa, had exploited the U.S. and international financial systems to launder hundreds of millions of dollars from narcotics trafficking and other criminal activities in Europe and the Middle East, moving the illicit moneys through West Africa and back into Lebanon. The U.S. dollars moving through this scheme included the proceeds of car sales between the United States and West Africa, transacted to conceal the money's criminal origins. A significant portion of this illicit money moved through courier and security networks controlled by Hezbollah or affiliated individuals.

The Lebanese Canadian Bank (LCB), its subsidiaries, and five Lebanese money exchange houses participated with Joumaa's network in a complex money laundering scheme of global breadth. LCB not only facilitated the Joumaa network's drug trafficking activities by laundering hundreds of millions of dollars through its accounts but also provided financial channels for Hezbollah, which drew financial support from the network's criminal enterprises. For ease of discussion, we refer to this web of illicit networks and actors as the "Joumaa Web."

This chapter explores the concept of *counter threat finance*, also known as "follow the money," and chronicles the real-life application of its core tools against a transnational network of illicit actors. The tools include economic sanctions, special anti-money laundering measures, civil forfeitures, and criminal investigations and charges. Their sustained application has resulted in criminal indictments, denial of assets and of access to the legitimate financial system, and exposure and disruption of the players' criminal activities.

This chapter introduces the tools and provides some perspective on their use against the transnational criminal and threat networks that constitute illicit power structures.¹ We do not address the investigative techniques and information collection practices that support use of sanctions and traditional criminal justice tools. Nor do we examine the military and other national security means that may be employed as elements of a broader, whole-of-government approach to countering the financial challenge of transnational threats. (Covering those aspects of counter threat finance would be a book-length enterprise in itself.)

As this case study shows, following the money is not a speedy process. The measures described, from the first actions in early 2011 to the July 2014 Kingpin Act designation, span three and a half years. Factor in the underlying DEA investigations that began in 2007, and this counter threat finance case has spanned more than seven years. The judicial proceedings have continued over three years, and some still have not reached final

The author and editors extend their sincerest gratitude to Dane Shelly and Josh Meservey for their research and analysis on the seizing and freezing of assets held by Muammar Qaddafi and associates.

¹ See especially, *Department of Defense Counternarcotics and Global Threats Strategy*, Apr. 27, 2011, 4.

resolution. For example, Ayman Joumaa, though indicted as well as designated, remains a fugitive.

This chapter seeks to improve whole-of-government collaboration and cross-fertilization of disciplines by making the military and other national security elements more familiar with the core players using follow-the-money measures in a real-life campaign against a transnational criminal web. The lessons and insights are intended to illuminate planning factors, expectations, and risks for planners and strategists alike. Critically, the case study does not tout counter threat finance as a silver bullet. But it does demonstrate how one key element, “follow the money,” achieves a specific subset of results within the complex of whole-of-government tools for combating networked illicit actors.

The Money Trail

Since the 9/11 attacks, “follow the money” has become a central (though not always well understood) tenet of anti-money laundering and counter threat finance.² This principle contemplates a set of distinct but interrelated tools that government can use against the individuals, entities, organizations, and networks making up the phenomena that have come to be known as *transnational threats*.

Transnational Threats

These dangers to U.S. national security have two essential properties that, together, make them a prime target for a particular set of counter threat financial tools: they contain an element of criminality, and their participants have an underlying need for money. Consequently, effective countermeasures against them must include disrupting their nexus with the funding that keeps them in business.

With few exceptions, the illicit power structures discussed throughout the volume have this element in common: attacking their finances is an essential element of disrupting and degrading the threat. Whenever possible, we must disrupt or dismantle the sources, facilitators, and channels of financing that sustain transnational threat networks. That is, we must *follow the money*. But what does this really mean in practice?

The Agencies Involved

The principal agencies in counter threat finance are law enforcement and regulatory, and the authorities that they use are embedded in our criminal and civil justice systems and in administrative law. They are fundamentally non-Defense Department and non-military. The lead agencies in this study are the Justice Department—principally, the

² See, for example, Department of Defense Directive “DoD Counter Threat Finance (CTF) Policy,” DoDD 5205.14, Aug. 19, 2010, Incorporating Change 1, Nov. 16, 2012, at Glossary, Part II, Definitions: “DoD CTF activities and capabilities . . . to deny, disrupt, destroy, or defeat finance systems and networks that negatively affect U.S. interests. . . . DoD CTF counters financing used to engage in terrorist activities and illicit networks that traffic narcotics, WMD, [IEDs], other weapons, persons, precursor chemicals, and related activities that support an adversary’s ability to negatively affect U.S. interests.” This DoD definition should be distinguished from that of the Financial Action Task Force (FATF) definition of “AML/CFT.” See FATF, “Glossary,” 2015, www.fatf-gafi.org/pages/glossary/.

Drug Enforcement Administration (DEA) and four United States Attorneys' offices – and the Treasury Department, through the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN).

These lead agencies work in close cooperation with multiple other agencies – federal, local, and foreign. Many of the actions involved have been coordinated through inter-agency task forces, particularly the Justice Department's Special Operations Division, which is headed by DEA. Drug trafficking and related money laundering investigations by DEA have been the foundation for most of the government countermeasures against this web of illicit actors. Nevertheless, in the mosaic of investigations and actions that have been under way since 2007, coordination through a single, integrated operating center has not been possible or, indeed, necessary. Inevitably, command and control in this multidisciplinary exercise of authorities is imperfect. But the mixing of authorities has worked synergistically, and the interagency participants continue to learn from it.

The Tool Kit for Countering Illicit Finance

Nearly every federal criminal investigation now includes inquiry into possible money laundering and other finance-related offenses. And along with criminal prosecution, criminal or civil forfeiture of assets is another possible option. When a national security dimension involving foreign threats is added, economic sanctions and special anti-money laundering measures become major parts of the follow-the-money arsenal. To disrupt the financial structures that keep the transnational threat operating, four established authorities are dominant: *financial (economic) sanctions, Section 311 actions under the PATRIOT Act, criminal and civil forfeitures, and criminal prosecutions.*

Sanctions

Whenever foreign governments or nonstate foreign adversaries – which include transnational illicit networks – are found to present a threat to the U.S. national security, foreign policy, or economy, economic sanctions are often first in the arsenal of legal instruments used to attack these foreign adversaries and their financial resources.³ Sanctions directed against nonstate actors, such as international drug cartels, foreign terrorist groups, and other transnational threat networks, are often termed “financial sanctions” – not only because they focus on the financing of the drug trade, terrorism, and other threat activities but also because they help protect the U.S. financial system from manipulation and misuse by illicit actors.⁴

Sanctions against Governments. The use of economic sanctions has grown as an instrument of national power directed against foreign governments and ruling regimes that have adversarial relationships with the United States. These include several regimes and governments that are subjects of this book's case studies. Indeed, since 1987, when sanc-

³ Michael Miklaucic and Jacqueline Brewer, eds., *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington, DC: National Defense Univ. Press, 2013).

⁴ See, for example, U.S. Treasury Dept., “Executive Orders,” May 28, 2015, www.treasury.gov/resource-center/sanctions/Pages/eolinks.aspx.

tions were imposed against Panama under the Noriega regime, through March 2015, economic sanctions have been employed in international emergencies in more than 30 national security situations.⁵ Some of these emergencies, most prominently Iran, involve multiple Executive Orders and statutes. In many instances, U.S. sanctions have been complemented by international sanctions involving, for example, the United Nations, the European Union, and the Organization of African Unity. This multilateralizing of sanctions has not been confined to the well-known international sanctions against al-Qaeda and Iran, and those related to Russia and Ukraine. For example, many in the international community joined in the sanctions against Qaddafi's Libya and Bashar al-Assad's government in Syria.

Sanctions against nonstate actors. Economic or financial sanctions against nonstate actors have gained wider recognition since the United States imposed sanctions against al-Qaeda and other foreign terrorist groups following the attacks of September 11, 2001.⁶ But this innovative use of targeted sanctions against nonstate actors actually began in 1995, with two innovative Executive Orders: E.O. 12947, against terrorists threatening the Middle East peace process, and E.O. 12978, against drug cartels centered in Colombia.⁷ Those two Executive Orders focused the power of economic sanctions through tailored Specially Designated Nationals (SDN) programs designed and implemented by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). OFAC is the lead office responsible for implementing economic and trade sanctions based on U.S. foreign policy and national security goals.

Sanctions directed against nonstate actors — often referred to in the post-9/11 world as “targeted sanctions” — are focused on particular individuals, companies, and groups of nonstate actors that commonly operate as illicit networks. These include the transnational threat networks discussed in this chapter. Targeted sanctions are also employed against specific entities and individuals involved with sanctioned foreign governments and illicit regimes, but the number and frequency of designations against nonstate actors such as transnational threat networks are much greater than designations related to governments and illicit regimes.

Imposition of sanctions depends heavily on the use of OFAC's Specially Designated Nationals List (SDN list). The SDN list further defines and identifies the individuals and entities that make up the sanctioned foreign government or sanctioned transnational threat network. In most programs, this includes entities and individuals that are controlled by the principal targets of the sanctions, act for them, or provide services or support. This is where the front companies, middlemen, facilitators, financiers, and penetrators of the legitimate economy are identified and exposed to the financial and commercial world and to the public at large. This is also the means through which sus-

⁵ Ibid.

⁶ E.O. 13224, *Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism*, Sept. 23, 2001, 66 Fed. Reg. 49079, www.treasury.gov/resource-center/sanctions/Documents/13224.pdf.

⁷ E.O. 12947, *Prohibiting Transactions with Terrorists Who Threaten to Disrupt the Middle East Peace Process*, Jan. 23, 1995, 60 Fed. Reg. 5079, www.treasury.gov/resource-center/sanctions/Documents/12947.pdf; E.O. 12978, *Blocking Assets and Prohibiting Transactions with Significant Narcotics Traffickers*, Oct. 21, 1995, 60 Fed. Reg. 54579, www.treasury.gov/resource-center/sanctions/Documents/12978.pdf.

tained and adaptable sanctions pressure is maintained on the threat network. Sanctions designations are now a key instrument in the set of financial countermeasures that the U.S. government employs against both established and emerging transnational threats. Following the U.S. lead, sanctions designations on a multilateral scale have developed significantly since the terrorist attacks of 9/11.

The most recent new program of nonstate sanctions against a transnational threat began in July 2011 with Executive Order 13581, issued to deal with transnational criminal organizations (TCOs).⁸ That Executive Order was the lead-off measure directed by the national Strategy to Combat Transnational Organized Crime.⁹ The sanctions imposed by E.O. 13581 were directed by the TOC strategy; and they address, in part, the strategy's policy objectives. The most specific policy objectives are worth restating in full because they reflect what may be viewed as a policy concept for dealing with the broader set of transnational threats:

*"Break the economic power of transnational criminal networks and protect strategic markets and the U.S. financial system from TOC penetration and abuse."*¹⁰

*"Defeat transnational criminal networks that pose the greatest threat to national security, by targeting their infrastructures, depriving them of their enabling means, and preventing the criminal facilitation of terrorist activities."*¹¹

The use of sanctions, particularly targeted sanctions designations, against nonstate actors was introduced in 1995, and those innovative early Executive Orders had objectives much like those of the TOC E.O. They are the foundation on which the subsequent sanctions programs against nonstate adversaries—including the Foreign Narcotics Kingpin Designation Act ("Kingpin Act"), which has been center stage in the actions against the Joumaa Web—have been modeled.

Although the policy framework of the TOC Executive Order helps us understand the use of economic sanctions against the Joumaa Web, this particular E.O. has not been one of the sanctions tools employed against the multiple networks involved. The sanctions tools used against the Joumaa Web—more than 180 designations under the Kingpin Act and one under E.O. 13224 (on global terrorists)—already existed and had been used many times before the TOC Executive Order was issued. Indeed, at the time of this writing, more than 1,700 Kingpin Act designations have occurred since June 2000.

Seizing and freezing. A misconception with economic sanctions is that they are principally concerned with, and measured by, the value of the assets that are blocked (frozen). Although blocking funds and other property and, thus, actually immobilizing or freezing economic wealth is a powerful intended consequence of sanctions, it is not the

⁸ E.O. 13581, *Blocking Property of Transnational Criminal Organizations*, July 24, 2011, 76 Fed. Reg. 44757, www.treasury.gov/resource-center/sanctions/Documents/13581.pdf.

⁹ White House, "Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security," July 2011, www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf. See especially key policy objective number 3, "Strategy," 20.

¹⁰ *Ibid.*, 14.

¹¹ *Ibid.*

principal instrument of impact. More often, it is merely part of a larger strategy of *denial and disruption*.

For example, on February 25, 2011, President Obama signed Executive Order 13566, which froze the assets of Colonel Muammar Qaddafi, his family members, and the government-owned enterprises that he was using to fund his regime. According to the *Washington Post*, banks around the world froze over \$30 billion of Qaddafi's assets within 72 hours of the signing of the Executive Order. Thus began multiple rounds of sanctions on the Libyan government, by which the international community achieved several objectives. First, the international freeze of Qaddafi's assets held abroad deprived him of most of his foreign currency reserves. Meanwhile, targeted sanctions on the Libyan oil sector made earnings from exports impossible. Thus deprived of his foreign holdings and prevented from earning new income, Qaddafi had trouble buying tribal support or hiring mercenaries. Also, targeted sanctions on the energy sector and Libyan ports prevented him from importing fuel for his trucks and tanks. Thus, the freezing of his foreign assets was a key link in the combined U.S., EU, and UN sanctions that helped starve Qaddafi of the funds and fuel he needed to stay in power. That was a major success for sanctions, but only a tactical success in the geopolitical sense. Most obviously, achieving those U.S. and international sanctions objectives has not led to a desired geopolitical end state of a stable, nonrepressive, and nonthreatening Libyan government. The case of Libya demonstrates that sanctions and their targeted economic effects are no substitute for a comprehensive, whole-of-government, preferably multilateral national security-foreign policy strategy. This means planning well beyond sanctions.

Denial and disruption. Denial and disruption, against nonstate adversaries especially but also against hostile regimes and governments, are essential levers in achieving the goals of degrading, delegitimizing, and incapacitating the target. This is particularly important in sanctions programs targeting nonstate actors, because the forms and expectations of the leverage gained through sanctions are different from those with foreign state/regime sanctions.

Sanctions imposed against a foreign state or ruling regime are only rarely undertaken with the express goal of regime change. (Those levied against the Qaddafi regime in Libya illustrate a rare and, unfortunately, tragic instance of sanctions being used successfully to help weaken a government enough that it toppled. The goals of having a stable, nonrepressive, and nonthreatening Libyan government and a largely intact country failed even though the sanctions were a tactical success.) More commonly, sanctions against governments/regimes are intended to achieve leverage that leads to a desirable change in behavior (e.g., abandoning a nuclear weapons program) or a cessation in an activity (e.g., stopping human rights abuses, eliminating terrorist safe havens).

The results are not always successful, however, even when many governments join in. For example, as of this writing, Bashar al-Assad continues the war on his own people despite sanctions against the Syrian government, and strong international sanctions have not yet persuaded Iran's supreme leader to shutter that nation's nuclear program. Although a deal with Iran was reached in July 2015, it remains to be seen whether or how Iran will follow through on its reluctant commitments. These are just two of the most recent examples of sanctions failing to persuade bad actors to give up their most cherished goals.

In many cases, multiple changes in behavior or cessations of activities are the desired end state. Even though the international and domestic political dynamics are more complex for foreign states and ruling regimes than for nonstate actors, concessions leading to the elimination or reduction of sanctions may be a more realistic possible outcome with state actors than nonstate actors.

Cessation of the “casus belli” is much less likely to be relevant to criminals, extremists, their financiers and facilitators, and other participants in their networks than to a governing regime. The hybrid criminal-extremist-facilitator networks and their key individual players (for the purposes of this discussion, *transnational threat networks*) are more likely to reduce or cease illicit activity or change bad behavior because they have been degraded and incapacitated than because they have been persuaded through the leverage brought by sanctions. Transnational threat networks and their specific participants are a new and malignant manifestation of an increasingly interconnected and mobile world. But most of the threat elements are still common criminal activities by traditional bad actors, albeit with greater scope, complexity, and sophistication than before. Consequently, the realistic desired end state in cases of sanctions against transnational threat networks is not to bring the bad actors into alignment with international norms of nation-state behavior. Rather, we seek a combination of complementary objectives against some of the targeted networks: deter, contain, or minimize the threat; disrupt, degrade, and delegitimize their financial and commercial backbones; impede, halt, and reverse their penetration of the legitimate economy. Ultimately, the optimal result is to incapacitate the transnational threat network. The more probable result is to *mitigate the severity* of the threat.

Sanctions are a powerful mechanism for combating nonstate threats and their evasive schemes for illicit finance. But sanctions alone are not enough. While they are particularly appropriate (and perhaps uniquely adaptable) in the transnational threat environment, it is their synergistic use with other tools – and not exclusively financial tools – that provides the best opportunities for effective countermeasures against transnational threat networks. By looking at the other follow-the-money tools, both new and old, we will see how an evolving whole-of-government approach can attack transnational threat networks with “official networks” instead of in the isolation of bureaucratic silos.

Section 311 Actions

In the aftermath of the al-Qaeda terrorist attacks of 9/11, Congress enacted the USA PATRIOT Act.¹² Among the act’s many provisions is Section 311.¹³ Section 311 (31 U.S.C. 5318A) gives the treasury secretary authority to find that a foreign jurisdiction, financial institution, class of transaction, or type of account is “of primary money laundering concern.”

The authority for Section 311 has been delegated to the director of Treasury’s Financial Crimes Enforcement Network (“FinCEN”). Under Section 311, domestic financial institutions and financial agencies (e.g., banks) can be required to take “special measures” against an entity identified by Treasury as being of primary money laundering

¹² USA PATRIOT Act, Pub. L., Oct. 26, 2001, 107-56.

¹³ USA PATRIOT Act, Section 311, 31 U.S.C. section 5318A, www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf.

concern. The range of options can be adapted to protect the U.S. financial system from specific money laundering and terrorist financing risks.

The most potent of the special measures is Special Measure 5: prohibitions on the opening or maintenance of any correspondent or payable-through accounts of the entity or jurisdiction identified as “of primary money laundering concern.”¹⁴ According to the FFIEC BSA/ AML Examination Manual, “a ‘correspondent account’ is an account established by a [U.S.] bank for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of the foreign bank, or to handle other financial transactions related to the foreign bank.” These transactions generally are done on behalf of the bank’s customers, thus enabling international transactions. Payable-through accounts (PTAs) are distinct from correspondent accounts because a PTA permits the foreign bank’s customers to access funds in the U.S. bank’s account of the foreign bank. With a PTA, the individual customers are basically subaccount holders with direct access to the bank. For a foreign financial institution, this determination can be a catastrophic disruption of its ability to operate, as well as a reputational disaster.

It is important to understand that the “special measures” of Section 311 do not involve directly either the freezing of assets, such as could occur with an OFAC designation, or the seizing and forfeiting of assets by the Justice Department (discussed below). They do, however, lay the groundwork for the Justice Department and U.S. Attorneys’ offices to undertake civil forfeiture proceedings and, in some cases, arrive at forfeiture settlements, as has occurred with LCB and other financial institutions involved in the Joumaa Web.

Since the inception of Section 311, “special measures” have been taken against four foreign jurisdictions and 19 foreign financial institutions. Five of those 311 actions against financial institutions are currently active, and of those, three are associated with the Joumaa Web. One of Treasury’s more recent Section 311 actions was also the first use of the authority against nonbank financial institutions: Rmeiti Exchange and Halawi Exchange. Both were based in Lebanon, and both facilitated money laundering by Hezbollah and by Colombian and other drug trafficking and money laundering networks. We discuss these two entities and their networks in greater depth below. And using them, we can explore the synergistic relationship between Section 311, sanctions designations, and more traditional law enforcement-centered follow-the-money authorities.

Seizure and Forfeiture

Among nonsanction financial countermeasures, the most prominent are those that have been used the longest: criminal investigations and prosecutions, and their companions, seizure and forfeiture. Indictments for money laundering activities became increasingly important over the latter half of the twentieth century. It is important to bear in mind that these money laundering cases commonly involve other traditional substantive criminal charges, which constitute the predicate offenses (Specified Unlawful Activities, or SUAs) that are necessary for the money laundering counts in the indictments.¹⁵

¹⁴ Ibid., 117; Bank Secrecy Act/ Anti-Money Laundering Examination Manual, Federal Financial Institutions Examination Council (FFIEC), Apr. 29, 2010, 1830185, 198-200.

¹⁵ 18 U.S.C. section 1956(c) (7).

The forfeiture authorities under federal law are key instruments in the tool kit, and while this is not a primer in asset forfeiture, some basics are worth mentioning. Federal forfeiture can be criminal or noncriminal. Criminal forfeiture occurs in the context of a federal criminal prosecution of a defendant. The property used or derived from the alleged crime (e.g., bank accounts, securities, real estate, boats, automobiles) is charged in the indictment along with the individuals or entities who are the defendants. It is a decision for the jury to find the property forfeitable or not. An affirmative finding by the jury results in the court issuing an order of forfeiture in addition to the sentences for convicted defendants.

There are also two noncriminal forfeiture processes. One is civil judicial forfeiture. This is an action brought against the property itself and adjudicated in court or through settlement. The owner of the property need not be charged with a crime. The other is administrative forfeiture against the property itself and does not involve the courts. There is separate, specific statutory authority for administrative forfeiture; and it includes monetary instruments.¹⁶ When seizure and forfeiture proceedings are completed successfully for the federal government, title to the forfeited assets (e.g., cash, bank accounts, securities, real property, vehicles) passes to the U.S. government.

Criminal Prosecution

As seen in the cases described below, the main goal from the criminal justice system perspective is for the criminal investigations to result in indictments, arrests, and criminal prosecutions and convictions if the evidence developed is sufficient.¹⁷ But that does not exclude cooperation where “criminal, civil, regulatory, and/or agency administrative parallel . . . proceedings” may also arise.¹⁸

The criminal investigations of the Joumaa Web have led to indictments of at least three different offenders for drug trafficking and money laundering. But while those actions are fundamental aspects of the U.S. criminal justice system and integral to confronting global illicit actors, they are unlikely, by themselves, to project U.S. power against foreign threat networks that reach around the world. Nor are they sufficient to safeguard the U.S. financial system and channels of global commerce from such networks. The inherent limitations on jurisdictional reach, on the types of evidence and nature of the defendants, on capture and extradition, and on the transnational nature of threat finance mean that other measures are also needed to bring a unity of effort against actors whose pursuits not only are criminal but also present a threat to U.S. national security.

¹⁶ U.S. Justice Dept., “Types of Federal Forfeiture,” Mar. 9, 2015, www.justice.gov/afp/types-federal-forfeiture.

¹⁷ U.S. Justice Dept., U.S. Attorneys Organization and Functions Manual, “27. Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings,” Memorandum of Jan. 30, 2012, www.justice.gov/usao/eousa/foia_reading_room/usam/title1/doj00027.htm.

¹⁸ *Ibid.*

Important Distinctions between CTF Measures

It is important to recognize the major distinctions between these instruments of counter threat finance. The traditional law enforcement approach may involve arresting suspects, seizing assets and contraband, putting individual violators in prison, and causing violators' assets to be forfeited to the United States. These processes occur daily as a core aspect of our criminal justice system and are a major impediment to those criminals and networks that fit into the broader realm of transnational threats to our national security and foreign policy.

In the case of blocking (or freezing) assets under sanctions programs, title to the blocked assets does not pass to the U.S. government; it remains with the owner. But *control* of the blocked assets resides with the government. Their use is denied to the target of the sanctions as well as to all others. Beyond that denial of specific blocked assets is the broader impact of the exposure and isolation of the sanctioned parties. This includes denial of access to the U.S. financial system, and disruption, degradation, and delegitimization of the designated entities and individuals.

Although Section 311 actions require an administrative process to find that their target is "of primary money laundering concern," they have the benefit of not requiring a prior declaration of a national emergency, as is necessary with economic sanctions programs enforced by OFAC. It is important to understand that the "special measures" of Section 311 do not involve directly either the freezing of assets, such as would likely occur with an OFAC designation, or the seizing and forfeiting of assets by the Justice Department. But as in the case of the Lebanese Canadian Bank (LCB, discussed in more detail below), the use of Section 311 can ultimately result in a substantial civil forfeiture as well as termination of the entity.

CTF "Follow the Money" Tools in Action

How do CTF operations work in practice? What does a successful, synergistic operation look like? Who is involved, what resources are required, and how long does it take? The answers to these questions vary widely from case to case, but closer examination of the Joumaa Web operation is instructive and provides a healthy dose of reality as we strive to confront impunity within an increasingly internationalized system of banking, finance, and transnational crime.

The following timeline for the Joumaa Web operation does not begin with the DEA investigations that started in 2007. But the DEA operations are relevant and must be kept in mind when thinking about planning horizons from an operational perspective. For the purposes of this study, we can begin with the 18 separate events that started in January 2011 as a set of Kingpin designations, against a single drug trafficking and money laundering organization that was believed to be associated with Hezbollah. Nearly four years later, a multiplicity of discrete actions—investigations, sanctions designations, special measures, indictments, and forfeiture activities—had collectively exposed the Joumaa Web, a complex network of illicit organizations and individuals reaching around the globe. By July 2014, the known linkages included other crime-terror hybrids, drug traffickers, money launderers, and terror financiers in more than 25 countries. This

network encompassed everything from illegal drug, arms, and human trafficking to money laundering and an ostensibly licit traffic in used cars.

Setting the Stage

To understand the events as they unfold, it is worth taking a moment to briefly examine common characteristics of the web of organizations, entities, and individuals that form this vast, intricate transnational threat network. The most publicized view centers the web on one entity, the Lebanese Canadian Bank, and LCB's involvement with Hezbollah. An alternative view centers it on one individual: Ayman Joumaa. Given the complex relationships of the participants, the scope and diversity of their activities, and the routes and geography involved, neither viewpoint is entirely accurate. We are looking at a web of connections with multiple elements, including Lebanon, South America, Africa, used cars, drug cartels, money laundering, players with dual nationalities, hundreds of millions of dollars in bulk cash transfers and structured wire transactions, and, woven throughout, Hezbollah.

Chronology of Follow-the-Money Actions

An actual blow-by-blow account of legal measures taken against the Joumaa Web will paint a clearer picture of how whole-of-government coordination works to disrupt, degrade, and delegitimize a transnational threat.

January 2011. Kingpin Act designation action. The first public action against the Joumaa drug trafficking and money laundering organization was OFAC's designation of Colombian/Lebanese national Ayman Saied Joumaa, his organization, nine other individuals, and 19 entities as specially designated narcotics traffickers (SDNTs) under the Kingpin Act.¹⁹ One immediate effect of this set of designations was the blocking (asset freezing) of more than 300 used cars awaiting export from the United States.²⁰ Interagency collaboration and coordination were publicly underscored by the Drug Enforcement Administration's announcement that OFAC's designation of the Joumaa network was based on "an ongoing DEA investigation."²¹

February 2011. PATRIOT Act 311 action. Two weeks after the Joumaa network designation, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) announced the identification, under Section 311 of the PATRIOT Act, of LCB as a financial institution of primary money laundering concern. Treasury's press announcement and the FinCEN report in support of its 311 action linked LCB to the Joumaa DT/MLO and to the global terrorist organization Hezbollah. DEA's administrator spoke out in

¹⁹ U.S. Treasury Dept., "Treasury Targets Major Lebanese-Based Drug Trafficking and Money Laundering Network."

²⁰ U.S. v. LCB, et al., Verified Amended Complaint, 11 Civ. 9186 (PAE), SDNY, Oct. 26, 2012, para. 5, and Schedule A, para. V.

²¹ DEA, "DEA Investigation Leads to OFAC Designation of Lebanese-Based Drug Trafficking and Money Laundering Network."

support of the 311 action, as she had done earlier with OFAC's designation of the Joumaa network, further underscoring Hezbollah's connection to LCB, Joumaa, drug trafficking, and money laundering.²²

November 2011. Drug trafficking and money laundering indictment of Joumaa. The inter-agency actions against Ayman Joumaa and his organization expanded when the U.S. Attorney in Alexandria, Virginia, indicted Joumaa on drug trafficking and money laundering charges.²³ This time, the connections were to Colombian drug traffickers and to the brutally violent Mexican drug trafficking organization los Zetas. President Obama had previously added the Zetas to the Kingpin Act list in April 2009, and on July 24, 2011, the group had been identified as a TCO in the Annex to Executive Order 13581 on Transnational Organized Crime.²⁴

December 2011. OFAC Kingpin Act designations of the Cheaitelly-Khansa DT/MLO. The second related OFAC designation action involving networking organizations identified Jorge Fadlallah Cheaitelly and Mohamad Zouheir El Khansa, along with nine other individuals and 28 entities involved in an international drug trafficking and money laundering network based in Colombia and Panama, with a global span and major connections in Lebanon and Hong Kong.²⁵

December 2011. Forfeiture and civil money laundering complaint. On December 15, 2011, the U.S. Attorney for the Southern District of New York filed a forfeiture and civil money laundering complaint seeking nearly \$450 million in civil money laundering penalties against LCB and six other entities that had been designated by OFAC or subjected to the 311 action by FinCEN, and the forfeiture of "property in or traceable to the money laundering offenses" of the LCB group and thirty used-car purchasers involved with the Joumaa-LCB networks.²⁶

June 2012. More OFAC designations under the Kingpin Act and the E.O. on terrorism: the Harb Network. In June 2012, OFAC designated four individuals and three entities under the Kingpin Act, and an additional connected individual under the terrorism Executive Order. The "Harb Network" was a Colombia- and Venezuela-based organization that laundered money for the Joumaa network through the Lebanese financial sector. The designations expanded the maze of connections to Joumaa and Hezbollah and high-

²² U.S. Treasury Dept., "Treasury Identifies Lebanese Canadian Bank Sal as a 'Primary Money Laundering Concern,'" Treasury Press Center, Feb. 10, 2011, www.treasury.gov/press-center/press-releases/Pages/tg1057.aspx. Note that the Treasury press release contains links to FinCEN's contemporaneous finding against LCB and to its Notice of Proposed Rule Making.

²³ U.S. Justice Dept., "U.S. Charges Alleged Lebanese Drug Kingpin with Laundering Drug Proceeds for Mexican and Colombian Drug Cartels," press release, U.S. Attorney's Office, Eastern District of Virginia (VAED), Dec. 13, 2011; *U.S. v. Ayman Joumaa*, U.S. District Court (EDVA), Nov. 23, 2011, www.vaed.uscourts.gov.

²⁴ EO 13581.

²⁵ U.S. Treasury Dept., "Treasury Targets Key Panama-based Money Laundering Operation."

²⁶ *U.S. v. LCB, et al.*, Forfeiture and Civil Money Laundering Complaint and Post-Complaint Restraining Order, Case 1:11-cv-09186-RJH, Docs. 1 and 2, SDNY, Dec. 15, 2011.

lighted the international linkages between illicit actors in Colombia, Venezuela, and Lebanon.²⁷

October 2012. Amended forfeiture and civil money laundering complaint. This complaint was filed in the Southern District of New York, against LCB, the other six entities named in the original complaint, and four used-car buyers.²⁸ In the ongoing process of the government perfecting its evidence against LCB and the other persons involved, the amended forfeiture complaint was a crucial step toward an eventual June 2013 settlement agreement with LCB, and forfeiture.

February 2013. OFAC Kingpin Act designation of José Linares Castillo. This Colombian cocaine boss had ties to the narco-terrorist group FARC. In naming Linares Castillo under the Kingpin Act, Treasury unraveled another strand in the drug trafficking and money laundering web.²⁹

February 2013. Drug trafficking and money laundering indictment of Rodriguez Vasquez associates. On February 14, 2013, the U.S. Attorney for the Eastern District of Texas indicted 17 individuals on drug trafficking and money laundering charges. The indictment was unsealed on August 5, 2013, and Colombian authorities arrested several of those named. In February 2014, OFAC designated seven of the accused under authority of the Kingpin Act. The sanctions designation action would further extend the reach of U.S. authorities against these foreign drug traffickers and money launderers.³⁰

April 2013. Another Section 311 action by FinCEN. The pressure exerted against the Joumaa Web and its interconnections grew when FinCEN named two Lebanese exchange houses, Kassem Rmeiti & Co. for Exchange and Halawi Exchange Co., as foreign financial institutions of primary money laundering concern. The 311 action against the two exchange houses was a countermeasure to their role in filling the gap for the Joumaa network's money laundering after the 311 action against LCB. This was the first use of Section 311 against a nonbank financial institution.³¹

²⁷ U.S. Treasury Dept., "Treasury Targets Major Money Laundering Network Linked to Drug Trafficker Ayman Joumaa and a Key Hizballah Supporter in South America," Treasury Press Center, June 27, 2012, www.treasury.gov/press-center/press-releases/Pages/tg1624.aspx.

²⁸ *U.S. v. LCB, et al.*, Verified Amended Complaint 11 Civ. 9186 (PAE), USDC SDNY, Oct. 26, 2012.

²⁹ U.S. Treasury Dept., "Treasury Designates Head of Aviation Drug Smuggling Operation: Action Targets Drug Trafficking Organization Tied to the FARC," Treasury Press Center, Feb. 20, 2013, www.treasury.gov/press-center/press-releases/Pages/tg1857.aspx.

³⁰ U.S. Justice Dept., "Seventeen Colombians Indicted in Eastern District of Texas Drug Conspiracy," press release, Aug. 26, 2013, www.justice.gov/usao/txe/News/2013/edtx-colombia-vasquez082613.html; U.S. Treasury Dept., "Treasury Designates Colombian Narcotics Trafficker," Treasury Press Center, Feb. 19, 2014, www.treasury.gov/press-center/press-releases/Pages/jl2295.aspx; *U.S. v. Fernain Rodriguez-Vasquez, et al.*, No. 4:13-cr-00038-MAC-ALM, Doc. 38, filed 2/27/13, U.S. District Court, Eastern District of Texas.

³¹ U.S. Treasury Dept., "Treasury Identifies Kassem Rmeiti & Co. for Exchange and Halawi Exchange Co. as Financial Institutions of 'Primary Money Laundering Concern,'" www.treasury.gov/press-center/press-releases/Pages/jl1908.aspx; U.S. Treasury Dept., "Notice of Finding that Kassem Rmeiti & Co. for Exchange Is a Financial Institution of Primary Money Laundering Concern"; U.S. Treasury Dept., "Notice of Finding that Halawi Exchange Co. Is a Financial Institution of Primary Money Laundering Concern."

June 2013. \$102 million settlement. On June 25, 2013, one of the paths of CTF actions against the Joumaa Web's drug and money laundering connections achieved a much-desired outcome when a settlement was reached requiring LCB to forfeit \$102 million to the U.S. government. The U.S. Attorney for Manhattan (SDNY) praised DEA's New York OCDETF, a multiagency unit, for its "outstanding work" on the investigation.³²

July 2013. Double Actions: OFAC designates, and the U.S. Attorney in Miami indicts, persons in another money laundering network connected to Joumaa. OFAC made 31 more designations under the Kingpin Act. It named nine individuals and 22 entities involved in yet another network (Guberek Network) of international drug-money launderers with connections to Ayman Joumaa and José Linares Castillo.³³ That same day, the U.S. Attorney for the Southern District of Florida indicted four key individuals in the network for their alleged participation in an international money laundering conspiracy investigated by the DEA.³⁴ The government actions against the Joumaa Web and its visible dimensions continued to expand.

October 2013. OFAC designates Spain-based associates of the Guberek Network. The CTF net affecting the Joumaa Web expanded again when OFAC used the Kingpin Act to designate two individuals (spouses) and the five entities they controlled in Spain and Peru, for their role as a "major node in the Guberek money laundering network, which provides a significant pipeline for illicit narcotics proceeds to flow from Europe to Colombia."³⁵

February 2014. OFAC designates a Colombia-based drug trafficker and his network. Actions against participants in the Joumaa Web expanded again with the February 2014 designation of a significant Colombian drug trafficker, seven associates, and five entities. This group, the Fernain Rodriguez Vasquez network, was identified with connections to

³² U.S. Justice Dept., "Manhattan U.S. Attorney Announces \$102 Million Settlement of Civil Forfeiture and Money Laundering Claims Against Lebanese Canadian Bank," SDNY press release, June 25, 2013, www.justice.gov/usao/nys/pressreleases/June13/LCBSettlementPR.php; *U.S. v. Lebanese Canadian Bank SAL, et al., All Assets of Lebanese Canadian Bank SAL or Assets Traceable Thereto, et al.*, Stipulation and Order of Settlement, 11 Civ. 9186 (PAE), SDNY, June 25, 2013.

³³ U.S. Treasury Dept., "Treasury Targets Major Money Laundering Network Operating out of Colombia," Treasury Press Center, July 9, 2013, www.treasury.gov/press-center/press-releases/Pages/jl2002.aspx.

³⁴ U.S. Justice Dept., "Four Colombian Nationals Charged in International Drug Money Laundering Conspiracy," press release, July 9, 2013, www.justice.gov/usao/fls/PressReleases/130709-01.html; *U.S. v. Solorzano-Lozano, Grimberg Ravinovicz, Guberek-Grimberg and Ceballos-Bueno*, 1:13-cr-20497-MGC U.S. District Court, FLSD, July 9, 2013.

³⁵ According to the Treasury Department, Isaac Perez Guberek Ravinovicz, a Colombian national, and his son, Henry Guberek Grimberg, a dual Colombian and Israeli national, led a money laundering network based in Bogotá, Colombia, that laundered narcotics proceeds for numerous drug trafficking organizations, including organizations based in Colombia. When announcing the Kingpin designation against the Guberek Grimberg network, Treasury officials specifically noted that Ayman Joumaa and José Evaristo Linares Castillo, who was designated in February 2013, were known to have laundered their drug proceeds through this money laundering network. U.S. Treasury Dept., "Treasury Targets Major Money Laundering Network Operating Out of Colombia"; U.S. Treasury Dept., "Treasury Targets Spanish Cell of Guberek Money Laundering Network," Treasury Press Center, Oct. 29, 2013, www.treasury.gov/press-center/press-releases/Pages/j12193.aspx.

the Lebanese-Colombian Cheaitelly network (itself designated on December 29, 2011), the Colombian narco-terrorist group FARC, Mexico's los Zetas DTO, and the Sinaloa Cartel.³⁶ The designation further exposed the expansive transnational connections and illicit activities among the actors in the Joumaa Web, and the U.S. government was able to impose sanctions that would cut the foreign nonstate actors off from transactions and commerce with the United States.

May 2014. OFAC Kingpin Act designation. Panama connection of the Cheaitelly DT/MLO. Treasury's OFAC designated eight more individuals and 20 entities, centered in Panama and operating internationally, tied to the Cheaitelly DT/MLO designated in December 2011.³⁷

June 2014. OFAC Kingpin Act designation: la Oficina de Envigado. Another link in the web of networks appeared with the designation of the Medellín-based DTO la Oficina de Envigado. La Oficina was cited for its recent support to the Sinaloa Cartel, and its interconnection with Colombia's AUC narco-terrorist organization and AUC's rural paramilitary successors.³⁸ The link to the Joumaa Web became more apparent when OFAC designated the Mejía Salazar DMLO, which had connections with la Oficina and Ayman Joumaa's network.

July 2014. OFAC Kingpin Act designation: Medellín-based Mejía Salazar drug money laundering organization. Treasury's OFAC highlighted the close money laundering connections between the Mejía Salazar DMLO, la Oficina, and Ayman Joumaa's international networks.³⁹

Analysis of the Joumaa Web Operations

As of the date of this case study, the web of organizations, entities, and individuals that form this vast, intricate transnational threat network can be summarized in the following table:

³⁶ U.S. Treasury Dept., "Treasury Designates Colombian Narcotics Trafficker - Action Targets Individuals and Entities Tied to the FARC and Mexican Cartels," Treasury Press Center, Feb. 19, 2014, www.treasury.gov/press-center/press-releases/Pages/jl2295.aspx.

³⁷ U.S. Treasury Dept., "Treasury Targets Major Money Laundering Network Operation Based in Panama," Treasury Press Center, May 14, 2014, www.treasury.gov/press-center/press-releases/Pages/jl2397.aspx.

³⁸ U.S. Treasury Dept., "Treasury Designates Colombian Organized Crime Group La Oficina de Envigado."

³⁹ U.S. Treasury Dept., "Treasury Designates a Medellin, Colombia-based Drug Money Laundering Network."

Essential Elements of the Joumaa Web

- Lebanese banks, money exchange houses, and money launderers
- African banking and commercial subsidiaries
- drug and money laundering networks centered in South and Central America
- drugs moving from South America to West Africa and on to Europe and the Middle East
- close family members in banks and drug trafficking / money laundering organizations
- dual-nationality participants, including several members of the Lebanese diaspora
- trade-based money laundering (TBML) involving used cars and Asian commercial goods
- bulk cash transfers and structured electronic wire transfers
- multiple U.S.-based and West African car dealerships
- regular transfers involving hundreds of millions of dollars
- Hezbollah
- other groups with a terror-crime nexus

This far-flung array of terrorist and other criminal enterprises included not only the Ayman Joumaa drug trafficking/money laundering organization (DT/MLO), but also the LCB, five Lebanese money exchange houses, and the terrorist organization Hezbollah. Also identified and exposed during this time frame were seven other drug trafficking and money laundering networks, the Mexican drug trafficking organizations los Zetas (also classified as a TCO) and the Sinaloa Cartel, the Colombian narco-terrorist organization FARC, the Colombian drug trafficking crime group known as la Oficina de Envigado (including remnants of the narco-terrorist Autodefensas Unidas de Colombia [AUC]), and the Medellín drug money laundering network of Pedro Claver Mejía Salazar.⁴⁰

To expose these elements and degrade their capabilities, federal government agencies had to employ legal mechanisms from the full range of CTF tools. Specifically, the federal government took the following actions against the Joumaa Web:

1. Ten separate but interrelated OFAC designation actions under the Kingpin Act, against eight DT/MLOs, resulting in 183 designations (117 entities and 66 individuals);

⁴⁰ U.S. Treasury Dept., "Treasury Designates Colombian Organized Crime Group La Oficina de Envigado for Role in International Narcotics Trafficking," June 26, 2014, www.treasury.gov/press-center/press-releases/Pages/jl2441.aspx; U.S. Treasury Dept., "Treasury Designates a Medellin, Colombia-based Drug Money Laundering Network with Ties to La Oficina de Envigado and Ayman Saied Joumaa," Treasury Press Center, July 1, 2014. www.treasury.gov/press-center/press-releases/Pages/tg1035.aspx.

2. Two separate but interconnected PATRIOT Act Section 311 determinations by FinCEN that three Lebanon-based financial institutions and their subsidiaries are of primary money laundering concern;
3. Three separate federal indictments of individual leaders of two of the designated DT/MLOs (Ayman Joumaa, indicted in the Eastern District of Virginia; four key figures of the Guberek DMLO, indicted in the Southern District of Florida; and drug trafficking and money laundering associates of the Rodriguez Vasquez organization, indicted in the Eastern District of Texas);⁴¹
4. The \$102 million settlement, in Manhattan, of the SDNY's civil forfeiture-money laundering complaint against LCB, and the \$720,000 forfeiture-money by one of the Lebanese money exchange houses (Ayash Exchange) designated by OFAC as part of the Joumaa DT/MLO;
5. Other Hezbollah network connections exposed in 15 additional OFAC designation actions, most of them under the global terrorism Executive Order, and one additional 311 action against a Lebanese-originated bank located in Cyprus.

Federal agencies also relied on the traditional law enforcement tools that were being used by domestic and international law enforcement partners throughout the investigation, in multiple jurisdictions at home and abroad. How they did so, and the lessons learned from these events, bears further analysis.

2011: from designation through indictment. The series of government actions that occurred from January to December 2011 had a major impact on the Joumaa Web and the U.S. government's ability to degrade the network. Following OFAC's designation of Ayman Joumaa under the Kingpin Act, sanctions included the designations of nine other individuals, including three of Joumaa's brothers, and 19 entities located in Lebanon, Panama, Colombia, Benin, and the Republic of the Congo. All were alleged to be connected to Joumaa's DT/MLO.⁴²

FinCEN found LCB to be a financial institution of primary money laundering concern because Joumaa's network was moving illegal drugs from South America to Europe and the Middle East via West Africa and laundering hundreds of millions of dollars monthly through accounts held at LCB. The activities involved trade-based money laundering of consumer goods throughout the world and included multiple used-car dealerships in the United States and West Africa. The finding for the Patriot Act 311 action in February 2011 also exposed the terrorist organization Hezbollah's links to LCB and Joumaa and to the international narcotics trafficking and money laundering network that LCB

⁴¹ A third federal indictment occurred in the Eastern District of Texas on February 14, 2013, and was unsealed and announced in August 2013. U.S. Justice Dept., "Seventeen Colombians Indicted in Eastern District of Texas Drug Conspiracy," U.S. Attorney's Office, Eastern District of Texas, press release, Aug. 26, 2013, www.justice.gov/usao/txe/News/2013/edtx-colombia-vasquez082613.html.

⁴² U.S. Treasury Dept., "Treasury Targets Major Lebanese-Based Drug Trafficking and Money Laundering Network," Treasury Press Center, Jan. 26, 2011, www.treasury.gov/press-center/press-releases/Pages/tg1035.aspx.

was facilitating. At the time of the OFAC designation action, Joumaa's network was described as a "complex money laundering scheme moving hundreds of millions of dollars of illicitly derived proceeds through businesses operated by him and his associates."⁴³ DEA's administrator remarked, "These are not legitimate businesses. These are illegal enterprises that fuel the drug trade and its violence and corruption. As we continue to follow the money trail, we starve these traffickers of their assets and eventually put their criminal networks out of business."⁴⁴

In terms of countermeasures against Joumaa's network, the designations of the other individuals and entities were as significant as Joumaa's own designation because they exposed these individuals and entities publicly, disrupted their ability to conduct transactions involving the U.S. financial system, and cut them off from trade with persons subject to U.S. jurisdiction. This further constrained the ability of Joumaa's network to engage in money laundering and drug trafficking and complicated its connections with others in the Joumaa Web.

Expanded operations as the Joumaa Web is exposed. Joumaa's indictment in November 2011 was a pivotal moment, and events unfolded rapidly thereafter. OFAC continued its designations. A series of nine additional designations occurred during the next three and a half years. The first of those, occurring in December 2011, was against the international DT/MLO of Jorge Fadlallah Cheaitelly ("JFC") and Mohamad Zouheir El Khansa. The Treasury Department described their network as a "Panama-based money laundering operation linked to Mexican and Colombian drug cartels." It was also linked to Lebanon and Hong Kong. That designation action covered JFC and El Khansa along with nine other individuals, including three of JFC's siblings. Among the other individuals designated under the Kingpin Act was Ali Mohamad Saleh of Colombia, who appeared again in a subsequent designation further linking Hezbollah to the Joumaa Web. Twenty-eight businesses of the JFC network were designated. Seventeen – at least three of them money exchange businesses – were in Panama. Among them was a Cheaitelly-controlled business in the Colon Free Zone, linked to Ayman Joumaa and his brothers.⁴⁵ Among all the designation actions eventually taken against the Joumaa Web, this was the largest group of entities to be designated at one time.

Meanwhile, shortly after Joumaa was indicted in the Eastern District of Virginia, and nearly simultaneously with the first JFC network designations, the U.S. Attorney in Manhattan filed the civil forfeiture and money laundering complaint against LCB and others involved in Joumaa's Hezbollah-connected DT/MLO. The federal complaint also included the two Lebanese money exchange businesses Ellissa Holding and the Ayash Exchange, along with other front companies that OFAC had designated as part of Joumaa's network. At that point in the stream of ongoing CTF actions, all the follow-the-money tools were in play. The June 2013 settlement of the civil forfeiture case against

⁴³ Ibid.

⁴⁴ DEA, "DEA Investigation Leads to OFAC Designation of Lebanese-based Drug Trafficking and Money Laundering Network," DEA Public Affairs, Jan. 26, 2011, www.justice.gov/dea/divisions/hq/2011/hq012611.shtml.

⁴⁵ U.S. Treasury Dept., "Treasury Targets Key Panama-based Money Laundering Operation Linked to Mexican and Colombian Drug Cartels," Treasury Press Center, Dec. 29, 2011, www.treasury.gov/press-center/press-releases/Pages/tg1390.aspx.

LCB was a major victory for the government, and forfeiture from Ayash Exchange followed within the month.⁴⁶

Together with the indictment of Ayman Joumaa, and the civil forfeiture and money laundering lawsuit brought against LCB the following month, the blend of sanctions designations, Section 311 actions, criminal indictments, and civil forfeitures had exposed the linkages among eight DT/MLOs and their connections to Hezbollah as well as to the Sinaloa Cartel, los Zetas, FARC, the Envigado organized crime group in Colombia, and other groups and individuals. From that point to the present, the actions illuminated the vast reach and complexity of connections within the Ayman Joumaa network and the broader Joumaa Web.

Impact and implications as operations progress. Two months before the LCB settlement and forfeiture, Treasury's FinCEN identified two Lebanese exchange houses, Rmeiti Exchange and Halawi Exchange, as foreign financial institutions of primary money laundering concern under Section 311. This was the first use of Section 311 against a nonbank financial institution, and it enabled the government to effectively cut off the Rmeiti and Halawi Exchanges from the U.S. financial system. David Cohen, Treasury's undersecretary for terrorism and financial intelligence at the time, explained that after the 311 action against LCB, "the Joumaa narcotics network turned to Rmeiti Exchange and Halawi Exchange to handle its money laundering needs."⁴⁷ LCB was out of the game, but substitutes had taken its place, handling the network's money laundering, including the TBML schemes involving American used cars and Asian consumer goods.⁴⁸ Now many of the same actions that had neutralized LCB were being employed against its successors.

The network continued to be exposed and disrupted. Using additional 311 actions, FinCEN's finding on the Rmeiti and Halawi exchange houses connected the dots further by exposing that two individuals associated with Joumaa and designated by OFAC under the Kingpin Act in June 2012, Abbas Hussein Harb and his partner, Ibrahim Chedli, "regularly coordinated and executed financial transactions . . . that were processed through the Halawi Exchange."⁴⁹ (The Harb network is discussed below.) The Rmeiti Exchange was described as working with the Halawi Exchange in money laundering and also engaging in trade-based money laundering for the Kingpin-designated Ellissa Exchange and its designated owner, Ali Mohammed Kharroubi.⁵⁰ Both Halawi Exchange and Rmeiti Exchange were also cited for facilitating or promoting money laundering for Hezbollah.⁵¹

⁴⁶ U.S. Justice Dept., "Manhattan U.S. Attorney Announces \$102 Million Settlement of Civil Forfeiture and Money Laundering Claims against Lebanese Canadian Bank," June 25, 2013. www.justice.gov/usao/nys/pressreleases/June13/LCBSettlementPR.php.

⁴⁷ U.S. Treasury Dept., "Treasury Identifies Kassem Rmeiti & Co. for Exchange and Halawi Exchange Co. as Financial Institutions of 'Primary Money Laundering Concern,'" www.treasury.gov/press-center/press-releases/Pages/jl1908.aspx.

⁴⁸ Ibid.

⁴⁹ U.S. Treasury Dept., "Notice of Finding that Halawi Exchange Co. Is a Financial Institution of Primary Money Laundering Concern," 78 Fed. Reg. 24596, Apr. 25, 2013, www.gpo.gov/fdsys/pkg/FR-2013-04-25/pdf/2013-09785.pdf.

⁵⁰ Ibid.

⁵¹ Ibid.

The June 2012 sanctions action against the Harb money laundering organization imposed Kingpin Act designations on Lebanese-Venezuelan individuals and business entities closely allied with Joumaa. That action also included the terrorism designation, under E.O. 13224, of Ali Mohamad Saleh, the Colombian national who had been designated in December 2011, under the Kingpin Act, as part of the JFC network. Ali Mohamad Saleh was described as a “key Hezbollah facilitator” who had raised funds for Hezbollah and coordinated transfers of money from Colombia, via Venezuela, to Hezbollah in Lebanon.⁵² Again the Hezbollah connection was prominent.

More fronts and individuals were linked to the Joumaa Web in July 2013 when OFAC made 31 more designations under the Kingpin Act. Nine individuals and 22 entities were involved in the Colombia-based Guberek international drug money laundering network (DMLO). The Guberek network, tied to both Ayman Joumaa and Colombian cocaine boss José Evaristo Linares Castillo, was connected into the web with Hezbollah and the FARC.

On May 14, 2014, 20 additional entities and eight more individuals connected to JFC were designated. Fourteen of those entities were in Panama and included several shell companies used for money laundering. Again relatives of JFC were among those designated, along with the Panamanian attorney involved with the JFC network’s fronts and money laundering. This designation expanded the total designations against JFC’s network to 48 entities, of which 31 were located in Panama.⁵³

Either Joumaa or his close associate Cheaitelly was directly implicated in all but one Kingpin Act designation of Joumaa Web actors occurring from February 2011 to July 2014. The exception, the June 2014 Kingpin Act designation of the Colombian organized crime group la Oficina de Envigado, was later connected to Joumaa and the Joumaa Web via the designation of the Pedro Claver Mejía Salazar network in July 2014.

More intersections. An additional aspect of this set of CTF actions was disclosed in the SDNY’s amended civil forfeiture and money laundering complaint against LCB, filed in late October 2012.⁵⁴ The complaint set forth detailed information about LCB’s connections to, and actions on behalf of, Hezbollah, including its connections to Hezbollah networks and financial channels that were the focus of four earlier OFAC designations from September 2006 to December 2010.⁵⁵ Those links included eight designated individuals, nine entities, and multiple subsidiaries on several different continents. They added four

⁵² U.S. Treasury Dept., “Treasury Targets Major Money Laundering Network Linked to Drug Trafficker Ayman Joumaa and a Key Hizballah Supporter in South America.”

⁵³ U.S. Treasury Dept., “Treasury Targets Major Money Laundering Network Operation Based in Panama.”

⁵⁴ *U.S. v. LCB, et al.*, Amended Forfeiture and Civil Money Laundering Complaint, 11 Civ. 9186 (PAE), U.S. District Court, SDNY, Oct. 26, 2012.

⁵⁵ *Ibid.*, 2833; U.S. Treasury Dept., “Treasury Designation Targets Hizballah’s Bank,” Treasury Press Center, Sept. 7, 2006, www.treasury.gov/press-center/press-releases/Pages/hp83.aspx; U.S. Treasury Dept., “Twin Treasury Actions Take Aim at Hizballah’s Support Network,” Treasury Press Center, July 24, 2007, www.treasury.gov/press-center/press-releases/Pages/hp503.aspx; U.S. Treasury Dept., “Treasury Targets Hizballah Network in Africa,” Treasury Press Center, May 27, 2009, www.treasury.gov/press-center/press-releases/Pages/tg149.aspx; U.S. Treasury Dept., “Treasury Targets Hizballah Financial Network,” Treasury Press Center, Dec. 9, 2010, www.treasury.gov/press-center/press-releases/Pages/tg997.aspx.

African countries, one Caribbean island, and Argentina, Brazil, and Paraguay, the three countries of South America's Tri-Border Area, to the more than 20 countries already identified in the web of networks and connections making up the Joumaa Web transnational threat complex. Those four counterterrorism designations not only intersect with the follow-the-money measures against the Joumaa Web, but also fit within a larger group of 15 mainly counterterrorism sanctions designations and one Section 311 action that were directed against Hezbollah's network of supporters and facilitators over eleven years (June 2004-February 2015). These other financial actions against Hezbollah and affiliates occurred independently of, but in the same time frame as, the Joumaa Web actions.

Observations and Implications: What Planners Need to Know

Civilian Lead and the Requirement for a Whole-of-Government Approach

The mutually reinforcing counter threat finance approach used in the Joumaa Web cases presents a valuable real-world example of a whole-of-government effort to counter complex illicit threats. The Joumaa Web cases also demonstrate that CTF actions do not operate in an exclusive "CTF stovepipe." Quite the contrary; they operate in a dynamic environment that includes and relies on traditional law enforcement methods and authorities. The innovation that successful CTF illustrates is not found in the special administrative authorities and designations themselves, but rather in how they are orchestrated synergistically across disciplines. The Joumaa Web cases combined criminal investigations, indictments, and forfeiture proceedings. They also leveraged OFAC's and FinCEN's ability to coordinate the inherent authorities of multiple U.S. government departments, bureaus, and agencies. Thus, the principle lesson is that tracking the complex financial networks that enable illicit power structures to succeed requires a sustained, well-resourced interagency effort with a legally empowered civilian lead.

For military planners, the importance of civilian lead cannot be overstated. CTF represents a balancing of security resources and shared responsibilities between defense, law enforcement, intelligence, and diplomacy. Defense policy emphasizes the primacy of multiagency CTF capabilities. In accordance with current directives, DOD's primary contributions include (a) incorporation of CTF operations into joint campaign plans; and (b) collection, analysis, and interagency sharing of signal, financial, and human intelligence supporting the necessary targeting and interdiction to attack or block financial lines of communication and disrupt networks.⁵⁶

These activities must be carefully coordinated to ensure that any military support to CTF does not compromise the web of criminal and civil actions and objectives that civilian agencies are pursuing in legal jurisdictions around the United States. Where overseas operations occur, the lines of command authority between geographic and functional combatant commands can create additional coordination challenges, par-

⁵⁶ Joint Chiefs of Staff, *Commander's Handbook for Counter Threat Finance*, Sept. 13, 2011, <https://publicintelligence.net/ufouo-joint-chiefs-of-staff-commanders-handbook-for-counter-threat-finance/>; U.S. Defense Dept., "DoD Directive 5205.14, Aug. 19, 2010, www.dtic.mil/whs/directives/corres/pdf/520514p.pdf.

ticularly when they do not align with similar lines of authority used by the lead civilian agencies. Each side of the equation, military and civilian, has its own set of security-related objectives that are furthered by CTF. Determining the means for reaching those objectives, and whose objectives take primacy, will always be a challenge. Recognizing the challenges, and establishing the mechanisms to align operations, targets, objectives, and authorities so that turf conflicts do not arise, is a critical component of strategic planning and operational design.

Timing and Synchronization

Timelines and planning horizons are critical planning factor. It is important to recall that the Joumaa Web operations spanned more than seven years, and three of the four federal court actions that resulted are still not resolved. CTF is an effective enabler in the fight against illicit power, but it is not a quick fix. Targets and opportunities take years of intelligence and investigation to develop. Because effective illicit finance networks are complex networks, the cases against them tend to be unusually long and difficult to prove. Cross-border law enforcement operations require significant diplomatic engagement. Powerful international economic and banking interests come into play. Each of these factors adds not just to the difficulty of CTF but also to the time required.

Also, follow-the-money operations are not linear. The juxtaposition of the government's actions under different authorities is not always a clear sequence of cause-and-effect actions. For example, the first step in the actions against the Joumaa Web was the designation of Ayman Joumaa and others in his drug trafficking/money laundering network. That sanctions designation action preceded Joumaa's criminal indictment by 11 months. Although some of the evidence concerning these two CTF measures is similar, the measures are not interdependent. (Joumaa's indictment reported the designation of his network as factual background, but the designation did not itself give rise to the charges in that indictment.) Interestingly, if Joumaa committed specific acts after his Kingpin Act designation, those might be used as evidence of violations of the criminal or civil provisions of the Kingpin Act. Those criminal penalties range up to 10 years' imprisonment for most violators, and up to 30 years when a corporate official is involved, along with large fines).⁵⁷

Often, a gap occurs between the public announcement of an indictment and later designations directed against the same persons or others in the illicit network. In the Joumaa Web series of actions, the U.S. Attorney announced the indictment of Fernain Rodriguez Vasquez and others in August 2013; and the OFAC designations occurred in February 2014. But in many other Kingpin Act designation cases, the indictments and designations occur simultaneously or nearly so. The indictments, in Miami, of key individuals in the Guberek Grimburg network (another Joumaa Web participant) were announced on the same day that OFAC sanctions designations were issued against the Guberek Grimburg network. In any of these situations, the designations, and their public disclosure, are coordinated and managed between OFAC, the criminal investigative agencies, the Justice Department, and others in a manner that will protect investiga-

⁵⁷ Foreign Narcotics Kingpin Designation Act, 21 U.S.C. 1901-1908.

tive and prosecutorial efforts. When indictments, designations, and 311 actions are used against actors in the same threat networks, convictions on the criminal charges are not necessary for the use of either designations or 311 actions.

Complexity

Time is not the only planning factor that cannot be precisely predicted. The degree to which CTF investigation will expand in both geographic scope and operational complexity can be only guessed at when an investigation begins. This is not “mission creep.” It is the reality of how illicit organizations’ financial networks function. It is highly likely that when the Joumaa Web operations began, no one anticipated how broad a network would come to light. As time and investigation went on, the Joumaa Web exposed intersections between transnational drug trafficking and organized-crime enterprises, poly-crime money launderers and threat finance facilitators, global terrorist organizations, and separate bad actors whose connections arise mainly through similar financial and facilitation needs. As outlined in the preceding sections, the Joumaa Web eventually included some 25 countries on five continents; more than 18 separate networks, organizations, and entities; and countless individuals.

Daniel Glaser, the U.S. Treasury Department’s assistant secretary for terrorism financing, pointed out this unanticipated complexity during his remarks before the 2013 Annual Arab Banking Conference in Beirut: “The facts of LCB demonstrate that what at first appears to be a criminal money laundering scheme might actually have broader implications. In the case of LCB, Hizballah benefitted from a global narcotics trafficking and money laundering network. This should not be surprising given Hizballah’s involvement in a wide range of illicit activities.”⁵⁸ In hindsight, Assistant Secretary Glaser was correct: it should not have been surprising. But hindsight can sometimes encourage foresight. As we move forward in our efforts to counter ever-evolving and increasingly networked illicit power structures, this is one lesson from the Joumaa Web that we need to take with us: however complex we believe the illicit finance network to be when the investigation effort begins, it will likely prove far more complex and far-reaching before the investigation ends.

Interagency Coordination and the Government CTF Players

Public actions dealing with the Joumaa Web of networks are the result of close coordination and cooperation among multiple agencies. DEA investigations were the basis for the OFAC designations, the Section 311 actions by FinCEN, the criminal indictments, the forfeitures achieved by U.S. Attorneys’ offices, and the global exposure of this multifaceted web of transnational threat networks. Many other agencies have been involved, in addition to the lead agencies described above. They include, for example, Homeland Security’s Immigration and Customs Enforcement (ICE), Customs and Border Protection, the Bureau of Alcohol, Tobacco, and Firearms, the FBI, IRS Criminal Investigations,

⁵⁸ U.S. Treasury Dept., “Remarks of Assistant Secretary Glaser on ‘Protecting the Lebanese Financial Sector from Illicit Finance’ at the 2013 Annual Arab Banking Conference,” Treasury Press Center, Nov. 15, 2013, www.treasury.gov/press-center/press-releases/Pages/jl2219.aspx.

the multiagency New York Organized Crime and Drug Enforcement Task Force, the New York Police Department, and a foreign law enforcement agency, the Colombian National Police.

It is also important to note that for designations under the Kingpin Act, the statute requires significant interagency coordination. Thus, in the OFAC designations of the Joumaa Web networks, the entities and individuals were listed after formal consultation by Treasury with DOJ, FBI, DEA, DHS, CIA, National Intelligence, Defense, and State. This formal process took place in addition to the day-to-day working collaboration between those agencies (for example, OFAC and DEA) with direct interest in the specific persons to be listed.

Options and Effects

On the positive side, the federal actions in the Joumaa Web cases also demonstrate that there is no single path to disrupting the money trail and denying assets and financial access. Indeed, there are many options, thereby enabling a sustained campaign on several fronts. Applying multiple elements of counter threat finance against the various key players of an illicit-threat network should include some of the “fixers, super fixers, and shadow facilitators” who provide money laundering, threat financing services, and other enabling activities.⁵⁹ These should be pursued as aggressively, and on as broad a scale, as the drug kingpins, high-value terrorists, and other key actors. Both the secret and the merely compromised channels of commerce, aided by their middlemen, are vital supply lines feeding the entire web of transnational illicit enterprises. And CTF measures directed against these smaller middlemen, fixers, and facilitators can be as damaging to transnational threat networks as efforts against the high-value leaders, with far less political cost or operational risk.

Conclusion

General Stanley McChrystal wrote, “It takes a network to defeat a network.”⁶⁰ He may have been referring to countering insurgents when he said it, but the principle applies equally to counter threat finance.

The finances and assets of transnational threat networks and their participants present a unique spectrum of vulnerabilities and opportunities for a whole-of-government approach to disrupting, containing, or even eliminating those networks and their participants. But counter threat finance alone is not enough. As the cross-disciplinary approach of CTF matures, the set of direct activities that could be used to thwart substantive offenses (e.g., drug and human trafficking) and gravely transcendent perils (e.g., terrorist possession of weapons of mass destruction) should not be isolated from CTF. On the contrary, nonfinancial investigative and direct operational methods (“action tools”) need more integration with CTF measures. Ultimately, neither CTF measures nor other investigative, intelligence, and action tools should operate in stovepipes. The universe of transnational threats is too diverse, too adaptable, and too innovative for either isolated or short-term countermeasures. Synergy will always be vital to success.

⁵⁹ Miklaucic and Brewer, *Convergence*, ch. 5.

⁶⁰ Stanley A. McChrystal, “Becoming the Enemy,” *Foreign Policy*, Mar.-Apr. 2011.