Working Paper Series

WP # 19-02

April 2019

Tracking Transnational Terrorist Resourcing Nodes and Networks

By Christian Leuprecht, Arthur Cockfield, Pam Simpson, Maseeh Haseeb

christian.leuprecht@queensu.ca

Table of Contents

I. Introduction

In light of ongoing terrorist attacks in Europe and elsewhere, the study of terrorism financing has attracted renewed attention. About 0.5-0.1 percent of transactions, amounting to US$300,000, are estimated to move internationally for illicit purposes every day. This begs the question, how are terrorists and their networks financed? Who raises the financial resources and how do they transfer them across borders? How does the global financial industry facilitate or impede these transfers? The answers to these and other questions can help law enforcement investigate, disrupt and ultimately shut down cross-border terrorist financing. The problem is that evidence and data on this phenomenon is scarce, of questionable quality, irreplicable and/or difficult to come by. This study is the first comprehensive effort to collect, code, compare, and analyze all available open source data on transnational terrorist financing networks. It thus contributes to the ongoing optimization of anti-terrorist resourcing laws, policies, and risk-management practices.

Initially the study operationalizes some key concepts, then goes on to review efforts to contain terrorist financing by the Financial Action Task Force (FATF), the UN, and various Financial Intelligence Units (FIUs). It then proposes a shift from the conventional yet strict focus on terrorist *financing* to broaden the remit to *resourcing* in an effort to include forms other than cash, such as trade-based fraud. To this effect, the study introduces a five-step approach dubbed the Terrorism Resource Model. Combined with the basic premise of Social Network Analysis that focuses on coding nodes and understanding the nature of the edges that connect these nodes, the following section presents the results of 32 transnational cases of terrorist resourcing. That is the universe of known transnational terrorist resourcing cases for which sufficient data points exist. These cases consist largely of civil and criminal cases. Not all of these cases have been prosecuted; some were settled out of court, some are still winding their way through the courts. There exists obvious selection bias: many of these cases were brought before US courts, several by a specific subset of plaintiffs and law firms. Since not all cases ended up being prosecuted, and since the burden of proof in civil cases is lower than in criminal cases, not all data are equally robust. Nonetheless, these are a good starting point – better, in any event, than the proliferation of anecdotal evidence and single narrative case studies that often rely on conjecture. Although these

32 cases differ markedly, they show surprisingly similar patterns that differ only in scale; they also reveal indicative findings with regards to financial hubs, banks and entities. Following this analysis, the study delves more deeply into three case studies to illustrate the broader findings: in terms of (1) the patterns used to raise and transfer resources, (2) the value-added of broadening the remit from financing to resourcing, and (3) the vexing problem of attribution of the purpose of funds. Finally, the paper capitalized on the findings to offer a preliminary assessment of international and domestic strides on curbing terrorist resourcing.

II. Concepts

In the aftermath of 9/11, anti-terrorist financing laws were grafted onto existing anti-money laundering laws, which makes an ill fit in some situations. The main difference is that money laundering, by definition, involves taking illicit proceeds (e.g., profits from the sale of illegal narcotics) and making these proceeds seem like they came from a legal source. As subsequently discussed, terrorist financing in some cases initially emanates from perfectly legal sources that are subsequently used for the criminal purpose of financing terrorists.

The methods of terrorism and criminal resourcing are converging (Leuprecht, et. al., 2015). In some cases, however, terrorist financing differs from global crime by using legitimate means to fund illegal operations. On the one hand, the goal of terrorist organizations is to conceal the money trail which is usually done through money laundering. (Gardner, 2007) Alternatively, criminal money laundering hides the criminal identity of funds so they appear legitimate in the end, whereas terrorist financing at-times uses legitimate means for illegal ends (Kreiger, 2011). For instance, an individual could take the profits of a legitimate business and donate them to a foreign terrorist group, a tactic the Tamil Tigers had perfected in Australia with the use of international calling cards (Jayasekara, 2007). One way terrorist groups raise money is by operating legitimate businesses and not reporting all income to the government (Freeman, 2011). For example, many legitimate businesses operated by Al-Qaeda in South Sudan, by hosting farms, trading companies, a tannery, furniture companies, a bakery, and an investment company. Since all businesses operated legally as per domestic laws, the state was unable to detect the criminal activity (Freeman, 2011). Other legitimate means of transferring money include legal donations, funds from charities, fundraising, and private investors (Rose, forthcoming). Charities donating to relief missions in

tumultuous regions of the world using a multitude of transfer mechanisms in a globally linked economy, creates a network that is increasingly difficult to track the funds destination. Once the funds have been transferred overseas, it is possible a portion of the proceeds are being diverted to terrorist organizations. Misuse of funds can originate from even high profile charities such as World Vision in the Australian branch, who donated to relief efforts in Gaza and were found to be diverting 60% of donations to Hamas (Rose, forthcoming). Transferring funds are becoming increasingly difficult to audit by domestic institutions because of the many ways of diverting and channeling cash through licit and illicit networks. Cash can be funneled through bank transfers, or transferred manually. Financial institutions can divide patrons using the service to fund illegal activities into two types of consumers, 'mission specific' referring to active terrorist cells on the one hand, and inactive groups on the other (Bantekas, 2003). For example, nineteen hijackers involved in the 9/11 attack opened twenty-four domestic bank accounts with amounts ranging between $3,000-$5,000 and infrequent addresses and no social security numbers (Bantekas, 2003). The dormant accounts – or sleeper cells – hold small sums of money that can easily be withdrawn and transferred.

Illegal methods of terrorist financing encompass an array of activities, from petty crime, extortion, and kidnapping to trade-based money laundering (Cassara, 2015; Cassara, 2016: 51-52). Cassara identifies familiar relations as a pattern among trade-based money laundering networks. This is replicated through Leuprecht et al.'s 2015 study of Hezbollah's networks. Analyzing Operation Bathwater and Operation Smokescreen show a pattern emerge in which trade-based cigarette smuggling and fraud in Michigan and North Carolina respectively, uniformly flowed through familiar connections (Leuprecht, 2015). These informal value transfer systems, as Cassara states, makes trade-based money laundering incredibly difficult for Western counter-terrorist financing institutions to detect and stop (Cassara, 2006). These illicit economies of trade can contribute extensively to the formal economy through money laundering the proceeds (Winer, 2008). In economies with weaker financial institutions, and when proceeds come from illicit sources, navigating the international financial system must be done in a covert fashion, making Hawala transfer a method of choice (Winer, 2008). Hawala leaves behind few records and remains unregulated. Hawala fund transfers operate by initially giving the money to a hawaladar 'agent' in the host country who communicates with another hawaladar in the desired destination, and

transfers the money and takes the commission (Miklaucic & Brewer, 2013). Nakhasi observes that "the *hawala* system allows for the transfer of debt from one *hawaladar* to another over a series of transactions. Built on a foundation of trust among the network of *hawaladars*, each money remitter pays back his debt through a series of transactions, which eventually equalize the position of one *hawaladar* against another" (Nakhasi, 2007). An estimated $200 billion per year enters the international financial system through the method of Hawala (Hall, 2005).

An estimated US$200 billion per year enters the international financial system through the method of *Hawala* (Hall, 2005: 20-21). The *hawala* system is inchoate when the flow is predominantly unidirectional since there must eventually be a contraflow transfer, which may be detectable by conventional means. However, *hawalas* are used extensively by guest workers to remit money and terrorist financing flows may be concealable within this, typically larger, outflow (Hall, 2005: 21). United States v. Ali (2012, 2015) documents the use of *hawala* between countries such as the United States and Somalia, and involves individuals and controversial money transfer businesses (United States v. Ali, 682 F.3d 705 (8th. Cir. 2012); United States v. Ali, 799 F.3d 1008 (8th Cir. 2015)). Ripe for potential abuse, including terrorist financing, *hawala* leaves few records and remains unregulated.

III. Global Cooperation to Counter Terrorist Financing

This study uses case law and TRM to map and detect terrorist resourcing patterns. Since one of the objectives of this study is to gauge the effectiveness of current legislation, regulation, and policy, this section surveys international and domestic laws and policies that govern terrorist financing. As subsequently explored, a complex set of international laws and norms, mainly promulgated by the Financial Action Task Force (FATF) and the United Nations (UN), as well as domestic implementing laws and government agencies (primarily financial intelligence units such as FinCEN and FINTRAC) strive to inhibit terrorist financing.

A. Academic Perspectives

Collaboration between various international and domestic actors is normally viewed as indispensable to contain terrorist resourcing. The general consensus is that financing is the lifeblood of the organizations (Freeman, 2011; Miklaucic & Brewer, 2013), actively enabling terrorist organizations to operate and execute attacks. The prevailing approach to combatting

terrorist financing is through collective action (Berger, 2010, Clunan, 2006, Gardner, 2007). International organizations forge a collective-action strategy to ensure allied states comply with international standards. International cooperation is necessary to develop common standards and laws. Otherwise terrorist financiers are prone to exploiting countervailing transaction costs to establish operations in a lightly regulated country. Yet, some observers question the effectiveness of collective action and maintain that international efforts to combat terrorist resourcing during the post 9/11 era was largely superficial (Clunan, 2006). Domestic bureaucratic interests often trump collective action which in turn undermines the effectiveness of collective-action plans, building a domestic security industrial complex instead of cooperating internationally with foreign institutions for information sharing (Clunan, 2006, Vlcek, 2008). These concerns notwithstanding, domestic organizations are heavily invested in transnational intelligence sharing and building measures to confront international terrorist resourcing collectively.

As subsequently discussed in more detail, some of the main international and domestic entities that utilize counter-terrorist financing measures are the United Nations (UN), the Financial Action Task Force (FATF), the European Union (EU), and government financial intelligence units such (FIUs) as the Financial Crimes Enforcement Network' (FinCEN) and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

B. United Nations

The UN General Assembly's Seminal Declaration on Measures to Eliminate International Terrorism, used the phrase 'terrorist financing' for the first time in 1994 (Bantekas, 2003). Terrorist financing gained international notoriety after Al-Qaeda's bombing of the US embassies in Tanzania and Kenya (Clunan, 2006). The UN has multiple cooperative measures in place to fight terrorist financing through coercive diplomacy (Berger, 2010). Coercive diplomacy in this context refers to "the state backing its demands on an adversary with a threat of punishment for noncompliance that will be considered credible and potent enough to persuade that adversary to comply" (Berger, 2010). The UN employs the use of coercive diplomacy through Security Council Resolution 1373, specifically outlining coercive tactics to counter domestic terrorist financing (Berger, 2010, Romanuik, 2010). UNs initiatives also counter terrorist financing through Chapter VII of the UN Charter, which outlines compliance of member states to counter terrorist financing. The *Convention on Suppression of Terrorist Bombing* (1997) and the *Convention on the*

Suppression of Terrorist Financing (1999) were designed to prevent and deter terrorist financing (Berger, 2010). By 2004, 132 countries signed the UN's convention for the suppression of terrorist financing. However, member countries' compliance seems to be waning as 9/11 becomes more distant (Levitt & Jacobson, 2008).

The two main components of the UN's counter-terrorism strategies are the Counter Terrorism Implementation Task Force (CTITF) and the Counter Terrorism Committee Executive Directorate (CTED). The CTITF was established to coordinate the UN counter terrorism efforts of the General Assembly and the Security Council's cohesive global counter-terrorism strategy (Romanuik, 2010). The CTITF, established in 2008, manifests a common approach by member states against terrorism, that focuses on strengthening individual and collective capacities of countries alongside the UN to prevent and counter terrorism. Main tenets of the strategy include increased cooperation, especially in combatting money laundering. Similarly, countering terrorist financing is core to CTITF strategy. Results of CTITF regional efforts between 2008 and 2010 were mixed, with many unstable regions such as Africa without a sustained counter terrorism strategy (Latif & Khan, 2010).

The CTED was established in 2004 under Resolution 1535 to oversee and analyze member countries' reports on counter terrorist efforts (Millar & Fink, 2016). From 2008 to 2010, the organizational plan of the CTED was to strengthen communication and coordination among member states in forging consistent counter-terrorist measures. The CTED accumulated detailed information about countries' counter terrorist efforts such as freezing assets, preventing terrorist groups from receiving aid, etc. The CTED collaborates with the CTITF. Its interventions are based on national and regional threats in the country reports. Developing a greater understanding of regional threats will help to combat the asymmetrical nature of global conflict (Millar & Fink, 2016).

Under the UN approach, countries are encouraged to adopt laws that criminalize the provision of resources to designated terrorist organizations. For instance, terrorist financing is a criminal offence in Canada under the federal *Criminal Code*. As of July 2015, Canada had listed 54 terrorist entities under the *Criminal Code* and 36 terrorist entities under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (Department of

Finance 2015: 27). The United States has similarly criminalized terrorism at the federal level via the *Patriot Act* and designates terrorist organizations under the same United Nations resolution.

C. Financial Action Task Force (FATF)

The FATF is an intergovernmental body that was established in 1989 (FATF, 2017, Gardner, 2007). The FATF has thirty-one member states and two international bodies (the European Commission and the Gulf Cooperation Council), with all members complying with self-reporting and mutual exercises to maintain membership. The FATF does not formally possess enforcement power but effectively makes recommendations for countering transnational money laundering (Gardner, 2007). The FATF is also committed to an anti-money laundering agenda with a criminal focus and is among the most collaborative and organized networks of anti-terrorist fundraising organizations. The FATF sets out international standards to prevent terrorist financing and money laundering. The FATF's revised mandate also outlines forty recommendations for combatting money laundering since 2003 (Freeman, 2011; FATF, 2016: 7-8, 37, 47, 55).[1] The forty recommendations are accompanied by eight special recommendations initially introduced in 2002, which encompass anti-terrorist financing (ATF) measures (Gardner, 2007, Jasinski, 2011). The eight special recommendations specifically focus on denying terrorist groups and their affiliates access to the international financial system including tracing terrorist assets and investigating individual suspects who financially support terrorism (Lo, 2002).

Many countries have amended their domestic laws on terrorist financing pursuant to the FATF special recommendations. Moreover, FATF engages in peer review where reports identify areas of non-compliance with FATF recommendations. Gardner suggests that it is important to continue with the FATF's international collective action and make it as adaptable as possible.

[1] *FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FINANCIAL ACTION TASK FORCE (FATF), 7-8, 37, 39, 47, 55 (Oct. 2016), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (The FATF's original mandate outlined forty recommendations for combatting money laundering in 1990 . The forty recommendations were then revised in 2001 and 2003 to be accompanied by eight special recommendations, and later nine, respectively, to encompass anti-terrorist financing (ATF) measures. The eight special recommendations were revoked in the 2012 amendments to simply include the FATF forty recommendations. Section C of the revised forty recommendations, specifically recommendations 5-8, focus on combatting terrorist financing. Recommendation 5 reaffirms that all terrorist financing should be criminalized, while 6 focuses on the freezing of terrorists' assets in accordance with international laws and regulations. Recommendation 7 describes compliance with sanctions imposed by the UNSC, with Recommendation 8 focusing on a risk-based approach to combatting terrorist financing in NPOs.

There seems to be considerable success in many of FATF's geostrategic locations such as Middle East and North Africa (MENAFATF, 2017). The expansion into the MENA region in 2004 was necessary as terrorism transcends national boundaries (Gardner, 2007). The FATF, however, faces significant challenges in an integrated global economy. The ease of money transfers poses a global threat as terrorist cells in many countries continue to expand their financial networks (Bantekas, 2003). For the FATF to be successful in counter-terrorist financing efforts, focus needs to shift to understand the adaptive nature and operational abilities of terrorist groups. Based on these metrics, the 'real denial of assets' is the most important goal for the FATF to dismantle the political and economic environment that enables terrorist financing. Gardner recommends the best way to do this is to "follow the money" (Wechsler, 2001).

The FATF sets international standards on issues such as 'know your customer' rules (see below) for financial institutions and seeks compliance with these standards in part by 'blacklisting' uncooperative countries. Recently FATF recommended that countries adopt laws that allow financial institutions to identify the individuals who are the ultimate (or 'beneficial') owners of corporations and accounts, whether or not there is any suspicion of a crime. At present, Canadian federal and provincial laws, as well as U.S. state laws, allow for nominee directors and shareholders and do not mandate disclosure of the identity of the actual person(s) who own(s) the underlying assets held in the business entity (e.g., a corporation or a limited liability company). Moreover, both countries allow for bearer shares, which are equity instruments that entitle the owner of the share to the ownership of all underlying corporate assets. As shareholders are never registered on a share registry, bearer shares allow for anonymous ownership. Ergo, Canada and the United States are not in compliance with recent FATF reforms.

In addition to ever-evolving terrorist networks, technology developments also present challenges to law enforcement (Cockfield, 2016). Recent global financial crimes are aided by quasi-anonymous forms of digital cash over the Internet. The current most popular so-called cryptocurrency, a form of digital cash generated by the application of cryptography, is Bitcoin (Gruber, 2013). Presumably cryptocurrencies are mainly used for legal purposes, but their illegal use is reportedly on the rise (Grossman & Newton-Small, 2013). Once a taxpayer converts his or her cash into a cryptocurrency, monies can be used for personal purchases or invested in offshore equity and debt instruments via an offshore account.

Cryptocurrencies help anonymize cross-border financial dealings and hence potentially facilitate terrorist financing. Anonymity is promoted because cryptocurrencies are not backed by any financial institutions or governments and there is no central control; it is not clear how governments will be able to monitor, track usage and identify the relevant taxpayer.

In addition, cryptocurrencies are used for criminal purposes on a part of the Internet sometimes referred to as the Deep Web (or Dark Web), a private network that anonymizes many transactions and financial dealings (Grossman & Newton-Small, 2013). While there does not appear to be any evidence of terrorist financing via cryptocurrencies or the Deep Web, to the extent that terrorist financiers become more technically sophisticated they may embrace these developments to achieve their goals.

D. Limits of Collective Action: Non-Compliant States

States' intergovernmental role is imperative to prevent and deter terrorist financing. States are divided into two categories: compliant states and non-compliant states. Compliant states are members of the UN and the FATF. The members implement appropriate measures to counter terrorist financing. In contrast, non-compliant states are not members of an internationally recognized organization. These states are likely to encounter the threat of having terrorist organizations' financial intermediaries operate within their borders. Similarly, states that are considered a target of terrorism or a base for terrorist activity experience more transactions bound to commit terrorist acts (Leuprecht & Cockfield, 2016). For example, Iran is a non-compliant state and known for financially supporting the terrorist organization Hezbollah (Leuprecht & Cockfield, 2016). Many international banks including Credit Suisse, Deutsche Bank, and HSBC have dramatically reduced business in Iran, but the country remains the top state contributor of terrorist financing. Iran spends an estimated $200 million annually on funding terrorist organizations such as Hezbollah and Hamas (Levitt and Jacobson, 2008: 48). Syria is also on the international radar for extensive state-sponsored terrorism, providing weapons and safe haven for Hezbollah. The country largely operates on a cash economy which is not integrated with, or reliant on, the international monetary system. Some non-compliant states, such as Iran, have been subject to sanctions (Levitt & Jacobson, 2008).

Furthermore, state-financed terrorism is prohibited under the 1994 UN General Assembly Seminal Declaration on Measures to Eliminate International Terrorism (Bantekas, 2003). The document indicates that states need to refrain from facilitating terrorist finance and must take appropriate measures to ensure they are not a vehicle for terrorist organizations to fund themselves (UN, 1994). Miklaucic and Brewer suggest that international cooperation is critical to defeat illicit networks and operations arising from non-compliant states. Terrorist operations rely on both domestic and international actors to extract and sell illicit resources. States may be hubs for these local fixers, who are used for their connections with local resources. These fixers rely on shadow facilitators who operate in the international realm to move resources to organizations or through states. In this study, fixers translate to 'investors' and shadow facilitators as 'financial intermediaries'. These reoccurring nodes in the literature show the necessity for states to cooperate to identify criminal supply chains and networks to make law enforcement agencies more effective in counter-terrorist finance efforts (Miklaucic & Brewer, 2013, Matfess & Miklaucic, 2016).

Terrorism is also linked with organized crime (Curtis & Karacan, 2002). For example, narco-terrorism is encouraged by states' failure to prevent illegal activities contributing to terrorist financing (Realyo, 2014). In many cases, terrorist and criminal financing activity are indistinguishable from one another. Due to the interconnectedness of globalization, cartels and terrorist groups thrive on cooperation, transcending international borders to fulfill criminal needs (Miklaucic & Brewer, 2013). Aside from illicit drug smuggling, cigarette smuggling also earns a significant portion of revenue for terrorist groups (Bantekas, 2003, Shelley 2014). It is difficult to distinguish between terrorist and criminal financing when narcotics or cigarettes are transported and sold illegally (Freeman, 2011, Leuprecht, 2015). It is also difficult for states to track terrorist groups when they use legal means to fund their organization. When groups are laundering through legitimate businesses, it deceives the protocol in place for suspected terrorist activity (Levitt, 2007). Challenges for the state to combat terrorist financing include: knowledge about the terrorist organization, denying the terrorist organization assets, and executing robust state compliance (Leuprecht & Cockfield, 2016). State knowledge about the organizations' networks is critical to implement any freezes or barriers to the terrorists' funds (Barber, 2011). In some instances, states do not intentionally fail to comply but lack the institutional capacity to implement best practices (Clunan, 2007).

E. FATF and Know Your Customer Rules

The 'know your customer' (KYC) principle is the main international approach to combat money laundering and terrorist financing. Under this principle, banks and other financial intermediaries are supposed to conduct due diligence to determine if their financial services are being used to launder money or finance terrorism by identifying individual customers (Hunt, 2011). Countries such as Canada and the United Sates focus on these financial intermediaries to detect and prevent terrorist financing. Through the *Proceeds of Crime* (Money Laundering) *and Terrorist Financing Act*, Canada extends its enforcement over approximately 31,000 reporting entities, including money services businesses, casinos, life insurance and banks (Dept. of Finance 5). These reporting entities include financial institutions and designated non-financial institutions and professions.[2]

The United States also regulates U.S. financial institutions and other gatekeepers via expanded authorities granted under Title 3 of the *Patriot Act* (also known as the *International Money Laundering and Anti-Terrorist Financing Act* of 2001). Interest in tracking large autonomous funds began with the U.S. Bank Secrecy Act in 1970, which enabled banks to "create audit trails for large transactions, and to allow law enforcement access to such information" (Clunan, 2007). In 1985, financial institutions were required to submit suspicious activity reports (SARs) and if they failed to do so were subject to sanction by the Federal Reserve and the Office of the Comptroller of the Currency (Levitt and Jacobson, 2008, Winer, 2008). Originating from a joint proposal in 1998 from US federal banking agencies, the KYC principle sought to identify the source of customer funds – normal transactions performed by that customer – and to monitor accounts that were inconsistent to find a suspicious activity (Gouvin, 2003). The KYC principle evolved post-9/11 under the U.S. *Patriot Act* which incorporated wire transfers requirements and other tools that financial institutions needed to track large sums of money. In effect, this provided financial institutions with the necessary framework to identify illegal activity and counter money laundering and terrorist financing.

[2] According to the FATF: http://www.fatf-gafi.org/glossary/d-i/ a designated non-financial institution includes: "Casinos, Real estate agents, Dealers in precious metals, Dealers in precious stones, Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures, Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations"

The KYC principle has been embraced by FATF, and forms one its most important recommendations to track and inhibit terrorist financing (Stringer, 2011). As with respect to all FATF recommendations, participating countries are expected to adopt the KYC principle through domestic implementing legislation. The KYC principle evolved for individual states to authorize agencies to trace and confiscate laundered money, monitor records across borders, making information gathered available to central financial institutions and eliminate anonymous accounts (Hall, 2005). The international goal is to identify trends in the money laundering market and to create a robust framework for countering money laundering effectively. Different countries have adopted approaches that differ in some cases. As mentioned above, in the United States banks must track SARs whereas Canadian banks must report on suspicious transaction reports (STRs), which gives them a slightly narrower reporting ambit. A cash deposit in excess of $10,000, for instance, will trigger a STRs. By contrast, a SAR is discretionary and can be triggered by mere unusual conduct. Under the KYC principle, banks and other financial institutions are supposed to report to their national financial intelligence units SARs, STRs and other information.

F. FinCEN

The US-based 'Financial Crimes Enforcement Network' (FinCEN) is the US FIU under the Department of Treasury that combats money laundering and terrorist financing (FinCEN, 2017). FinCEN also utilizes reports through the *Bank Secrecy Act* from the Department of Commerce to track unusual transactional patterns assisting FinCEN to pursue cases of terrorist financing. This model is known as the money laundering and terrorist financing (ML/TF) approach. FinCEN investigates how money laundering groups place, layer, and integrate money through various transactions. Essentially, illegitimate funds are discreetly moved into a legitimate financial channel, which is then moved around through legal means to disguise the money trail. This may be done through numerous accounts and released to the organization in a legitimate way (Kurzrok & Hund, 2014). It is called money 'laundering' because the illicit sources of income are 'cleaned up' and injected into the conventional financial system. FinCEN disseminates intelligence information from financial institutions and the Commerce Department to law enforcement agencies who can then inspect the inquiry. Identifying suspicious activity is a key feature in blocking terrorist financing and money laundering.

G. FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is the Canadian-based FIU under the Department of Finance. Pursuant to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), FINTRAC seeks to "detect and deter money laundering and the financing of terrorist activities to facilitate the investigation or prosecution of money laundering and terrorist financing offences" (Financial Transactions and Reports Analysis Centre of Canada, 2015). FINTRAC, like FinCEN, is responsible for financial intelligence to uphold the integrity of financial networks in Canada, acting as a vehicle to transmit financial intelligence to relevant law enforcement to penalize illegitimate financial practices. FINTRAC employs the money laundering/terrorist financing (ML/TF) model to identify networks of terrorist resourcing, mirroring FinCEN. Unlike FinCEN, however, FINTRAC does not have any powers to investigate; rather, it can only report information to partners such as the RCMP.

III. Method

Data from the 32 course cases that comprise this study – not all of which factor into the subsequent analysis due to some incomplete or uncertain data points - was collected in two parts, by (a) exploring primary sources (legislation) and secondary sources (scholarly journals and government documents), and (b) searching electronic online legal databases including West Law, LexisNexis-Quick Law, CanLII, and EUR-Lex – access to European Union law[3]. The study relies on legislation as well as scholarly journals and government documents to explore the essential vocabulary on terrorist finance and to identity case names and citations. In the process we compiled a list of the *terms* and *categories* to narrow our focus. The list of *terms* was comprised of 'terrorist financing', 'charity', 'finance', 'donation', 'funds', 'alms', 'money laundering', 'transaction', 'informal transfer' etc. while the *categories* included 'online', 'social media', 'hawala', 'bank',

[3] The rationale for coding legal cases as the basis for this study is a function of validating information from primary sources. Analyzing legal cases enables the extraction of court-validated primary-source information of investor and financial intermediaries' names, locations, terrorist entities, and ultimately enabled identification of transnational pattern. Additional primary and secondary sources were used to supplement information.

'money transfer business', etc. The *terms* and *categories* narrowed our focus to track international, transnational, and cross-border transaction of monetary and other formal/informal financial proceeds that contribute to terrorist finance. These criteria also set the limitations to explore specific cases to address the complexity of terrorist resourcing. Similarly, the interplay of *terms* and *categories* made it possible to identify those cases that involve circulation of currency for the purpose terrorism. Cases included jurisdictions in North America, Europe, Australia, etc. and were searched using legal databases.

We also searched cases via Quick Law to find cases by name and citation. We narrowed our search to jurisdiction, content type, legal topics, and advanced search. For example, we narrowed our search tabs to identify the domains including international, Australia, Canada, and the United States. Subsequently, we pinpointed the specific level of courts (Supreme Court, Appellate Courts, Superior Courts, etc.) in the drop-down menu under the source type to identify cases. We then used connectors (i.e., &/or) to find cases by relying on the interplay of *terms* and *categories*. For example, 'funds & social media', 'charity or hawala', 'transaction & money transfer business', 'donation & online', 'charity & bank', etc. Other connectors we added were: and not, w/, pre/n, /n, /p, /s, w/seg, I, *, ?, near/n, and onear/n. Each of the connectors have a specific function and are necessary to locate the *terms* and *categories* within judicial decisions. A similar approach was used on West Law using different connectors. Both databases provide a list of connectors to search within cases.

We also used CanLII to search judicial decisions. We primarily searched *terms*, and *categories* to locate cases by filtering the type and jurisdiction. CanLII and West Law are effective search tools to explore domestic cases while we found QuickLaw more useful to find international cases. Finally, EUR-Lex is a useful database to search legislation, documents, regulations, and directives pertaining to the European Parliament. For example, we restricted our focus on directives by the European Parliament to explore data that help us understand how terrorist funds are channelled through a wide of range of financial sectors.

The approach in this study draws on the terrorist resourcing model (TRM), whose remit is more comprehensive than that of the money laundering/terrorist financing (ML/TF) model

conventionally used by FIUs (O'Halloran et al, forthcoming). The TRM incorporates all assets that are deemed resources, including modes of financial transactions. As a result, the TRM generates more information about all value moved by financial intermediaries to terrorist organizations. The research in this study and the way it is coded is based on the five stages of TRM.

The TRM is distinguishes between two types of terrorist resources: 1) resources raised and 2) resources transferred. First, resources raised refers to individuals who are intent on to sending cash or goods to a terrorist organization but are apprehended before the transfer is complete. Second, resources transferred refers to the successful transfer of funds from a financial intermediary to a terrorist organization. The patterns that emerge suggest that terrorist organizations adopt a fairly uniform approach to fund themselves through transnational networks. While the cases differ in terms of the amount of money and transfer of resources, it appears that the investors and their financial intermediaries use relatively similar networks to transport resources to terrorist's organizations. The primary data includes more than twenty-eight independent variables to map terrorist resourcing networks. Collectively, the data points follow from the initial transfer to the resource destination (the terrorist group). This research performs a cross-sectional small-*n* analysis to cross-reference major nodes in cases to find patterns and similarities in terrorist groups' operations, independent of size or location. The cases were chosen for their relevance to and emphasis on terrorist resourcing. Each case follows the same independent variables which are listed and described in the coding.

The starting node is the primary investor – a person or organization responsible for raising funds. All financial intermediaries are listed along with the type of financial intermediary mechanism. The financial intermediary mechanism displays the use of the method to transfer the resources such as hawala, wire transfer, etc. We also identify those banks that wire transfer funds that consequently enable terrorist attacks. Similarly, we list organizations along with any terrorist affiliates receiving the funds. We also classify the ideology and location of the terrorist organization. The investigating agencies for the case and the investigating agencies' country are also listed. Finally, we provide the total number of victims of terrorist financing cases.

A. Stage 1 of the TRM: Acquisition and Exchange

Stage one of the TRM is the "acquisition of funds and end-use goods and exchange goods", also known as the 'investor'. Many "investors" in the cases in our study raised monetary funds with the intention of funding a terrorist organization. However, only a few cases manifest resourcing rather than financing. *USA v Mehdi et al* (2010) involved the movement of over 2000 PlayStation 2's along with $200,000, while *United States of America v Sriskandarajah* (2012) involved a submarine, warfare technology, and weapons being accumulated with the intention of being transferred to a terrorist organization. Across all cases in this study, the most common form of raising resources for terrorist organizations was by collecting cash. The research illustrates the many ways in which investors raised money, from funneling donations to charities, personal fundraising, or smaller door-to-door donations. Many investors used charities as their method for acquiring funds. The legal cases either cited the defendant as the charity, or the bank that provided services to the charity, as investors raised donations to send to financial intermediaries, who would send the money to terrorist organizations. This is in line with the literature on charities and terrorist fundraising, and indicative of the broader problem associated with terrorist resourcing where it ends up being difficult to parse whether funding is being used for legitimate or terrorist purposes: some charities may have a wholesome purpose, but divert funding to terrorist groups (Levitt, 2007).

B. Stage 2 of the TRM: Aggregation of Resources

One might expect tax havens to figure prominently in transnational terrorist financing networks. Later in this paper we speculate why this expectation was not met. Tax havens would be an ideal addition for Stage 2 of the TRM, which is "the pooling or aggregation of those resources". Although tax havens per se do not figure in the data, techniques commonly associated with tax evasion were used, such as a multitude of banks to store funds either through individuals or organizational cells. Many of the cells were mission-specific, actively transferring funds through international financial networks (Bantekas, 2003). Many banks in the study were used to move funds from a financial intermediary to a terrorist-organization client. Some were used frequently to store funds, including the use of sleeper cells (Bantekas, 2003). In one case, the National Westminster Bank situated in the UK was found to be a primary account holder for the

Palestinian Relief and Development Fund – a British-based charity providing funds to Hamas. Arab Bank PLC was the defendant in two separate cases accused of providing banking services to organizations that directly financed Hamas. The former contrasts with *International Relief Fund for the Afflicted and Needy (Canada) v Canadian Imperial Bank of Commerce* (2013) where the charity (IRFAN) felt their account was wrongfully terminated by the bank (CIBC). The case notes that once IRFAN was added to the terrorist watch-list in Canada, the bank immediately terminated its services to avoid providing financial services to a known terrorist financing organization by a designated organization to aggregate resources. The case *United States of America v Mehdi et al* (2010) transported over 2000 PlayStations to a subsidiary of a mall that was formally owned and operated by Hezbollah. This case shows how terrorist resourcing transports value and aggregates resources in subsequent ways, such as through a designated mall, in a way that would otherwise elude strict conventional understandings of terrorist financing. Cases involving the legal transport of funds through a financial institution shows how illicit activity can disguise itself as seemingly legal, or how illicit exports can be falsely legitimized through fraudulent documentation, and appear like a perfectly legitimate export.

C. Stage 3 of the TRM: Movement of Resources

Stage 3 of the TRM is "the transmission of resources to a terrorist organization". It comprises the largest part of the research conducted, stemming from the financial intermediary, next transferring funds to the terrorist organization, tracking how funds were transferred and what process was used to transfer the funds. The financial intermediary distinguishes itself as first and foremost executing the transfer of funds. The financial intermediary may also be the investor if they also raised funds, but generally holds a transactional position. The financial intermediary need not be a person but can take the form of an organization as in *Chaim Kaplan et al v Central Bank of the Islamic Republic of Iran* (2013). In this case, Bank Saderat acted as the financial intermediary transferring funds from London through to Beirut to support Hezbollah. Bank Saderat had formally been designated by the US Treasury Department under EO 12334 for previously facilitating the delivery funds to Hamas, PLO, and Hezbollah (US Department of the Treasury, 2008). The TRM accounts for the fact that transfers frequently traverse more than one country.

D. Stage 4 of the TRM: Transmission to Terrorist Organization

Navigating the exact route of funds from an investor to a terrorist organization is difficult through court cases since only facts relevant to the case are included in the reports and not necessarily the full causal mechanism. Stage 4 seeks to fill the network link by looking to "their transmission to a terrorist or operational cell". While many of the cases merely indicate financial transfers in the formal documents through secondary research, the findings show that funds are not the only asset that reaches a terrorist organizations. In the case of *USA v Qureshi* (2005), Mohammad Salman Farooq Qureshi lied to the FBI about his involvement with the NGO 'Help Africa People' and his affiliation with Al-Qaeda. Named as the main financial intermediary, Qureshi funneled $30,000 to an al-Qaeda affiliate.

E. Stage 5 of the TRM: Purpose of the Resources

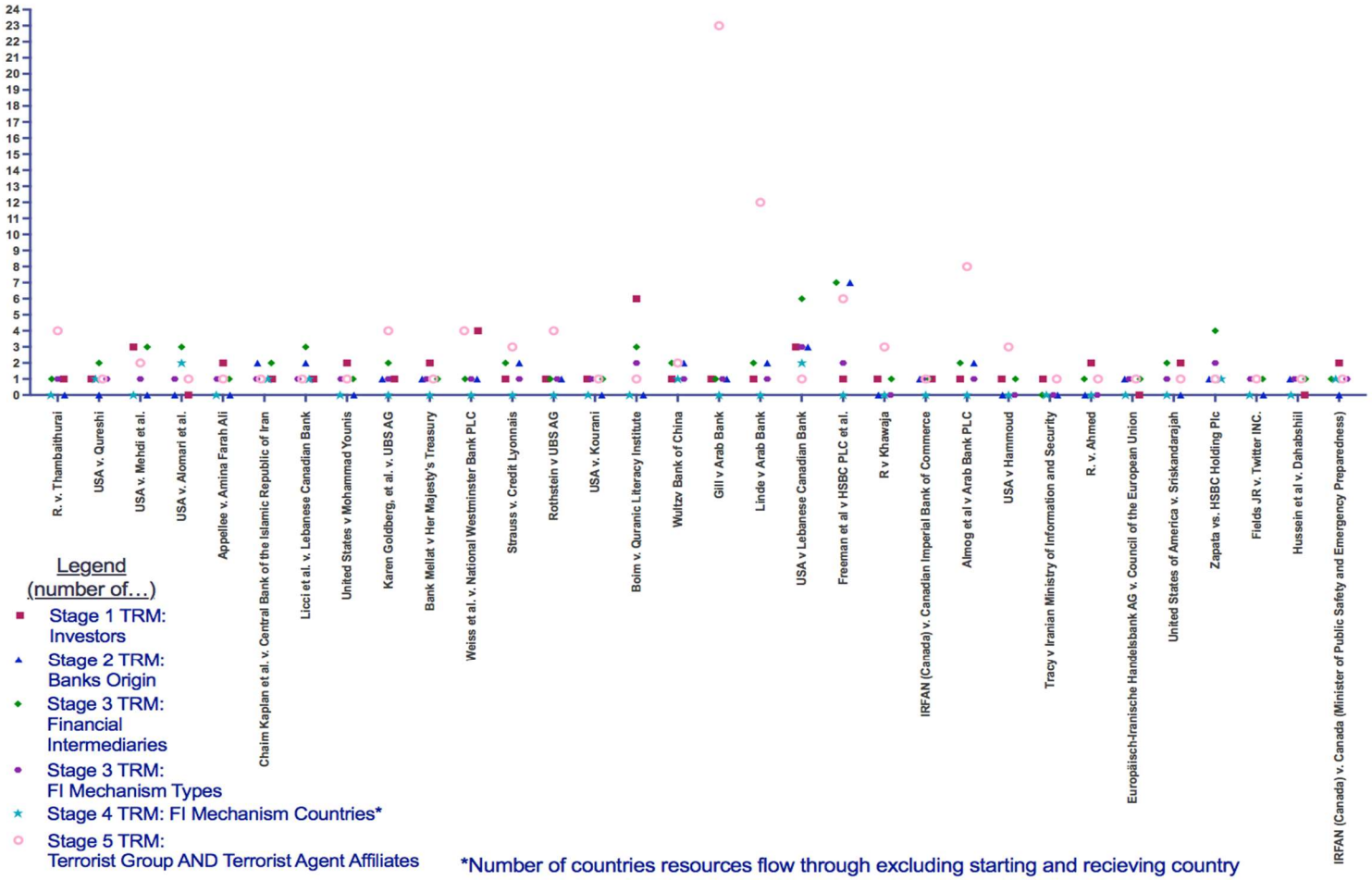
Finally, Stage 5 of the TRM entails "their [the resources] transmission to a terrorist or operational cell; and their conversion to goods and services to support the organization activities, including for an act of terrorism". Stage 5 justifies using case law to map financial networks instead of the terrorist organization case studies that are prevalent in the literature on terrorist financing. Many of the cases are brought by family members of victims, or victims themselves, who want justice from banks for abetting an attack that ultimately killed their loved ones. For example, in the case of *Almog et al v Arab Bank,* over 1,600 plaintiffs brought an action against Arab Bank for providing financial services leading to suicide bombings in Israel. The suit alleges that the bank provided financial services to organizations that were designated as terrorists by the US government, resulting in the death of innocent civilians.

IV. Observations

The 32 cases, listed on the x axis in Figure 1, shows that most cases include investors, banks, financial intermediaries, mechanism type (transfers), mechanism countries, and terrorist groups. Although most cases only involve a couple of these nodes at each stage of the TRM, the majority of cases include all the stages of the TRM. The reason "mechanism countries" appear to be low is that the starting and receiving country are not counted in this category, just the countries

through which money flows between the starting and ending transfer points. Figure 1 illustrates the pattern that emerges by evaluating terrorist networks using the five stages of the TRM.

Figure 1. Shows the frequency of TRM stages used in each case.



The cases predominantly reflect jurisdictions in the United States and Canada, as shown in Table 1. Although there are only a couple of cases in Europe, that may simply be a function of the preliminary scan of European cases. In sum, of 33 terrorist financing cases, 21 hail from the USA, seven from Canada, one from Europe, and one from the UK. The results show nine investors from the USA, five from Canada, four from Iran, four from Lebanon, and one from the UK, Switzerland, France, Netherlands, Israel, and Syria.

Table 1. Case jurisdictions, number of investors, and number of financial intermediaries by country

Countries	Case Jurisdictions	Number of Investors	Number of Financial Intermediaries
USA	23	15	18
Canada	7	7	7
Lebanon		4	10
UK	1	1	9
Iran		4	2
Switzerland		1	3
France		1	1
Germany			2
Netherlands		1	
Mexico			2
Yemen		1	
Togo			1
Kenya			1
UAE			1
Palestine			1
Israel		1	
Syria		1	
China			1
**EU	1		

As per Table 2, three banks stand out for using more than one location and appearing in more than one case for aiding/transferring resources intended for terrorism: Arab Bank PLC, HSBC, and UBS AG. Finally, the three major terrorist groups and countries identified as the recipient of the most terrorist resources transactions are Hamas, Hezbollah, and Iran. Seventeen banks were used and the locations that investors and financial intermediaries worked from/through centred on three major hubs for terrorist resourcing activity in London, Beirut, and New York. Although Canada has the second greatest number of investors and the third most financial intermediaries, the cases show the transactions took place in separate Canadian cities. The cities are spread out across the country, with no discernable pattern for Canadian cities as a terrorist resourcing hub. Table 2 shows the number of investors and financial intermediaries who used these hubs either to raise or transfer funds. The final column identifies the terrorist organizations to which the funds were ultimately transferred, and contrasts the locations of terrorist organizations with the locations of the investors and financial intermediaries.

Table 2. Locational hubs for terrorist resourcing

City	Investors	Financial Intermediaries	Terrorist Organization(s) Funded
London	(2) in (2) Different Cases: **Defendants** in R. v. Khan **Interpal** in Weiss et al. v. National Westminster Bank PLC	(7) in (4) Different Cases: **Bank Saderat** PLC in Chaim Kaplan et al. v. Central Bank of the Islamic Republic of Iran **National Westminster Bank PLC** in Weiss et al. v. National Westminster Bank PLC **HSBC Group** in Freeman et al v HSBC PLC et al. **Barclays Bank** in Freeman et al v HSBC PLC et al. **Standard Chartered Bank** in Freeman et al v HSBC PLC et al. **Bank Saderat** in Freeman et al v HSBC PLC et al. **HSBC Group** in Zapata vs. HSBC Holding PLC	Funded (4) in (5) Cases: **Hamas** in Palestine (National Westminster Bank Case) **Hezbollah** in Lebanon (Freeman & Chaim Kaplan) **Al-Qaeda** in Saudi Arabia (R v Khan) **Mexican Cartels** (Zapata)
Beirut	(2) in (2) Different Cases: **Hassan Ayash Exchange Company** in USA v. Lebanese Canadian Bank **Shahid Foundation** in Licci et al. v. Lebanese Canadian Bank	(11) in (6) Different Cases: **Lebanese Canadian** Bank in USA v Lebanese Canadian Bank **Arab Bank PLC** in Gill v Arab Bank **Arab Bank PLC** in Linde v Arab Bank **BLOM Bank** in USA v Lebanese Canadian Bank **Arab Bank PLC** in Almog et al v Arab Bank PLC **Sheik Abbas Harake** in USA v Hammoud **Sahid Foundation** in Licci et al v Lebanese Canadian Bank **Middle East and Africa Bank** in USA v Lebanese Canadian Bank **Lebanese Canadian Bank** in Licci et al v Lebanese Canadian Bank **Federal bank of Lebanon** in USA v Lebanese Canadian Bank	Funded (2) in (6) Cases: **Hezbollah** in Lebanon (Lebanese CB & Licci) **Hamas** in Palestine (Linde, Gill, & Almog) **Hezbollah** in Lebanon (Hammoud)

New York	(2) in (1) Case: **Mohammad Younis, and Faisal Shahzad** in United States v Mohammad Younis	(8) in (6) Different Cases: **Mohammad Younis** in United States v Mohammad Younis **Credit Lyonnais** in Strauss v. Credit Lyonnais **Arab Bank PLC** in Linde v. Arab Bank PLC **Arab Bank PLC** in Almog et al. v. Arab Bank PLC **HSBC Bank** in Zapata et al. v. HSBC Holding PLC **American Express Bank** in Licci et al. v. Lebanese Canadian Bank	Funded (4) in (6) Cases: **Hezbollah** in Lebanon (Licci) **Hamas** in Palestine (Linde & Almog) **Mexican Cartels** (Zapata) **Individual** in New York (Younis)

Since New York is the financial hub of the world, its frequency in Table 2 is not all that surprising. Similarly, most terrorism resources cases have been brought in US jurisdictions in general, and in New York State in particular. Yet, London and Beirut match or outnumber New York in investors and financial intermediaries. That may be a function of more robust financial regulations in the United States, especially with regards to terrorist financing. Another initial observation is the reoccurrence of global banks. A few banks appear more than once, for instance, the Lebanese Canadian Bank, HSBC Holding, and Arab Bank PLC. The data suggests that global banks are more popular for terrorist resourcing and thus appear more often in court cases. Table 2 also includes patterns for locations. Some banks may use more remote locations and appear multiple times, for example, HSBC. Some banks mainly contribute to a particular terrorist organization. For example, Arab Bank PLC seems involved only in transfers funds to Hamas and Hamas affiliates according to the data set. The Lebanese Canadian Bank only transferred funds to Hezbollah. In contrast, HSBC seems to transfer resources to Mexican Cartels and Hezbollah.

Table 3. Reoccurring banks in the dataset

Bank	Location	Number of Terrorist Groups Funded
Arab Bank PLC	(2) Locations in (3) different cases: **New York** in Almog et al. v Arab Bank **Beirut** in Almog et sl. V. Arab Bank **New York** in Linde v. Arab Bank **Beirut** in Linde v. Arab Bank **Beirut** in Gill v. Arab Bank	Terrorist groups funded (1): **Hamas** in Palestine (Gill) **Hamas** in Palestine (Linde) **Hamas** in Palestine (Almog)
UBS AG	(1) Location in (2) different cases: **Zurich** in Karen Goldberg v. UBS AG **Zurich** in Rothstein v. UBS AG	Terrorist groups funded (2): **Hamas** in Palestine (Goldberg) **Hezbollah & Hamas** in Iran (Rothstein)
HSBC Group PLC	(3) Locations in (2) different cases: **London** in Zapata vs. HSBC Holding PLC **London** in Freeman et al v HSBC PLC et al. **New York** in Zapata vs. HSBC Holding PLC **Mexico City** in Zapata vs. HSBC Holding PLC	Terrorist groups funded (2): **Hezbollah** in Lebanon (Freeman) **Mexican Cartels** (Zapata)

Table 3 shows the involvement of international banks in terrorism resourcing cases. Step 2 of the TRM model emphasizes the location where the terrorist resources are accumulated. As such, Arab Bank PLC appears in Beirut and New York. Step 3 focuses on the transfer of resources to a terrorist organization. Table 3 identifies banks that had a direct link in funding terrorist organizations. Table 3 corresponds to Table 2 which indicates the financial intermediaries' direct match with the resource transfers to terrorist organizations. Mapping a single network by utilizing the TRM model for the case of *Linde v. Arab Bank PLC*, step 1 identifies the investor as The Saudi Committee in Support of the Intifada Al Quds. The network then shows a transfer of resources to the next node - the financial intermediaries were Arab Bank PLC in New York and Arab Bank PLC in Beirut. In this case, step 2 and 3 of the TRM model work in tandem, showing that Arab Bank PLC collected and transferred terrorist resources. Next, step 4 of the TRM indicates how the resources in this case were transmitted through bank transfer. Finally, step 5 of the TRM model shows the transmission and use of resources by the recipient terrorist organization Hamas. A visual display of this network is shown below in Diagram 1. Furthermore, *Almog et al. v Arab Bank PLC* also appear twice in the above dataset following a very similar network trend as the Linde case.

For example, the investor is Popular Committee for Assisting the Palestinian Mujahideen and the Saudi Committee in Support of the Intifada Al Quds. The financial intermediary is Arab Bank PLC in New York and Beirut while Hamas is the recipient of the bank transfer (Diagram 2). To show the scale of these cases, secondary research for *Almog et al. v. Arab Bank PLC* indicates that $194,123,924 USD was transferred to the Saudi Committee in Support of the Intifada Al Quds, with a secure $40,000,000 being deposited with Arab Bank PLC (United States Senate, 2005). By contrast, in *Linde v. Arab Bank PLC* $90,000,000 USD was successfully transferred through Arab Bank to fund Hamas terror attacks.

Diagram 1. Showing all stages of the TRM, using one case of network of terrorist resourcing.

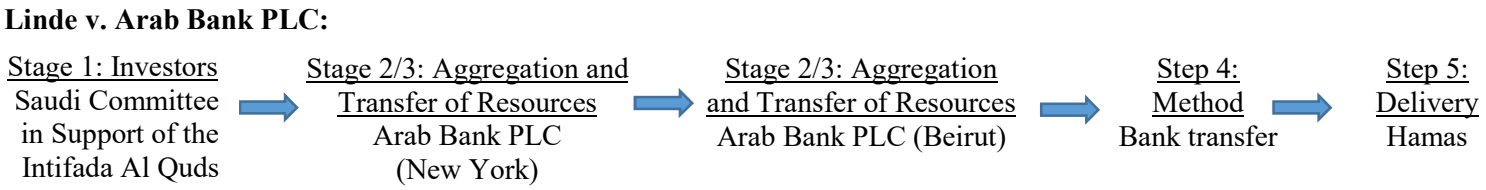
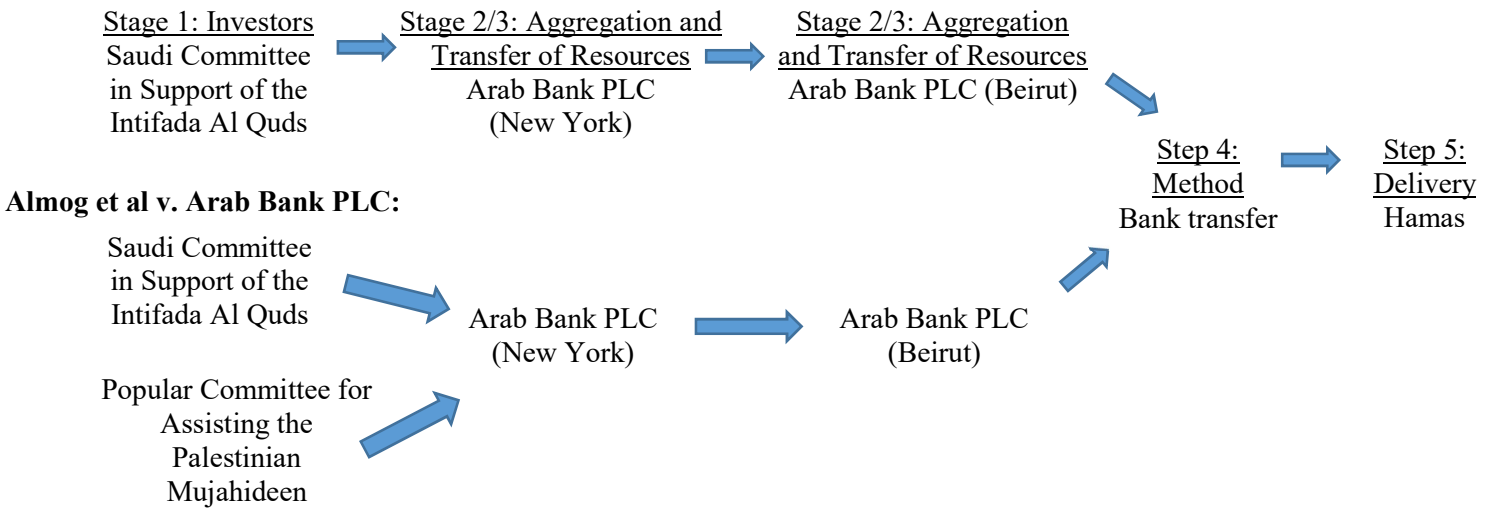


Diagram 2. Showing all stages of the TRM using two cases of network of terrorist resourcing.



The above diagram illustrates the complex network of terrorist financing. Were this paper to map the network for each case, the same pattern would emerge for every resourcing incident. The difference seems to be merely a matter of scale: the number of investors, financial intermediaries, and recipients.

Table 4. Resourced terrorist organizations

Terrorist Organization	Locational Nodes and Banks Used to Transfer Resources in Stated Location
Hezbollah	(6) Locations with (13) different Banks: **Iran (2):** Bank Sedat, Central Bank of Iran** **Lebanon (6):** Lebanese Canadian Bank x 3, Federal Bank of Lebanon, Middle East and Africa Bank, BLOM Bank **UK (6):** HSBC Group, Bank Sedat PLC x2, Barclays Bank PLC, Standard Chartered Bank, Royal Bank of Scotland N.V. **USA (1):** American Express Bank **Switzerland (1):** Credit Suisse AG **Germany (1):** Commerzbank PLC
Hamas	(5) Locations with (6) different Banks: **Switzerland (1):** UBS AG **UK (1):** National Westminster Bank PLC, **USA (3):** Credit Lyonnais, Arab Bank PLC x2 **Lebanon (3):** Arab Bank PLC x3 **Canada (1):** CIBC **France (1):** Credit Lyonnais
Iran	(2) Locations with (3) different banks: **Germany:** Bundesbank, Europaisch-Iranische Handelsank AG **Switzerland:** UBS AG
	**Central Bank of Iran in this instance did not transfer resources, but raised resources, thus the only node acting as an investor and not financial intermediary.

As shown by the table above, the top resourced terrorist organizations were Hezbollah and Hamas, with the state of Iran trailing in acquired resources with only two locations and three banks. The data shows that funds were predominately transferred to Hezbollah using Lebanese and British banks. Each country had six cases of transfers from a financial intermediary, with the Central Bank of Iran as the only one that was also acting as an investor in *Chaim Kaplan et al. v. Central Bank of the Islamic Republic of Iran*. *Kaplan et. al. v. Central Bank* explains two of the

three appearances of Banks Saderat PLC with transfers to Hezbollah. The causal mechanism Bank Saderat employed to transfer the funds is illustrated in the case:

> "Specifically, plaintiffs claim that BSI [Bank Sederat Iran] received Iranian funds from defendant Central Bank of Iran, transferred those funds to BSPLC [Bank Sederat PLC] in London who then transferred them to accounts controlled by Hezbollah in branches of defendant BSI [Bank Sederat] in Beirut." (Chaim Kaplan et al. v. Central Bank of the Islamic Republic of Iran)

Bank Saderat also appears in *Freeman et al. v. HSBC PLC,* specifically Bank Saderat London. *Freeman et al. v. HSBC* accounted for most of the locational nodes, including five different banks from the UK used to transfer resources, one bank in Germany, and one in Switzerland. Resources to Hamas seem to originate with banks in the USA and Lebanon. Arab Bank PLC transfers resources to Hamas most frequently: five times in three different cases: *USA v Lebanese Canadian Bank, USA v Hammoud,* and *Linde v Arab Bank.* In both *USA v Labanese Canadian Bank* and *USA v. Hammoud*, the two locational nodes of Arab Bank PLC are in Lebanon and the US. This may insinuate a working relationship between these two branches, with the third case, *Linde v. Arab Bank* just noting the Lebanese location. By contrast, the same bank does not recur in funding destined for Iran. That may be a function of necessity due to heightened vigilance as a result of international sanctions. Iran also does not use the US or Lebanon as locational nodes, but instead seems to rely exclusively on banks in Germany and Switzerland.

A. Case Studies

To illustrate the analysis this section will discuss three coded cases[4] that reveal the number of financial intermediaries, countries, transactions, funding/resources amount and other variations from the independent variables. Although the cases differ, the patterns that emerge are scalable to show a similar pattern among most terrorist financing cases.

Zapata et al v HSBC Holding Plc (2016) is a relatively large case in the study, spanning three terrorist organizations and $881,000,000 USD in financing. The case involves three of

[4] Space constraints make it impossible to explain and analyze every case in-depth in this working paper. They will, however, be featured in detail in a future book-length manuscript as will metrics for evaluation and how they are to be interpreted.

Mexico's most powerful drug cartels, the Sinaloa, Juarez, and Los Zetas. The plaintiffs in the case are the families of the four victims, who brought HSBC to court for reckless banking operations. HSBC reportedly accepted large amounts of money from individuals with no identifiable source of income. The money was taken to the banks in designed boxes that fit the precise dimensions of the teller windows. The case notes that HSBC admitted and accepted criminal liability for laundering $881 millions of the drug cartel proceeds. The source of the funds came from a variety of activities: The cartels account for 90% of illicit drug imports and activities such as human trafficking, extortion enterprises, and weapons trafficking. The cartels amalgamate the criminal and terrorist aspect of their organization through these activities for financial gain (Curtis & Karacan, 2002).

Step 2 (aggregation) and Step 3 (movement of funds) of the TRM model work in tandem in this HSBC case. HSBC possessed cartel money and transferred the funds to suspicious investors. HSBC's reckless protocols allowed the cartels to launder money through a legitimate institution. After the money was raised through illicit means, it is delegated to financial intermediaries, who exist on both ends of the transactions. In many cases, financial intermediaries will transfer the funds to or from the financial institution while another intermediary will complete the transaction to the terrorist organization. *Zapata et al* specifically cites a three-step approach to money laundering used by the cartels known as placing, layering, and integrating. The first step places the money into the international financial system. Second, illicit funds in the financial system are layered into a series of different accounts to conceal their origin. This is supposed to create a 'façade of legitimacy' making the funds untraceable. Integration, the final step, brings the illegitimate funds back into society by turning it into legitimate funds. Illegitimate funds enter the legal economy through a series of purchases and investments (Cassara, 2015).

The case notes two ways that funds were placed, layered, and integrated from the US banking system to the international economy and turned into legitimate funds. The first is casas de cambio, also known as 'exchange houses' – a currency exchange method to circulate illicit money in Mexico. This method allows for the exchange of one currency to another. Casas de Cambio does not operate the same as banks and the value of the currency remains the same. For example, the value of 1 peso is equivalent of 1 USD. Casas de Cambio allows businesses to transfer or exchange illicit money to different bank accounts, including in the United States. Another type of

money laundering is called the Black-market peso exchange (BMPE). This method is mainly used when cocaine is sold in USDs, then converted to other currencies such as Colombian pesos to compensate the cartels who produce cocaine in Colombia. In this case, the funds travelled from HSBC branches in the US to HSBC New York, and HSBC Mexico, and Casa de Cambio Puebla S.A de C.V in Puebla, Mexico; exchange house and chief money launderer for the cartels. Peso brokers received the USDs from drugs sold in the United States. The peso brokers then sold the USDs in Colombian pesos at a discounted rate.

The money is difficult to track once it reaches the recipient, especially through the three-step money laundering process, but the activities of the cartels may provide some insight. Illegal methods of funding are generally advantageous for all of the organization and can accomplish the task successfully (Freeman, 2011). Dart finds:

> ""money laundering is essential to the cartels' prosperity because without the ability to place, layer, and integrate their illicit proceeds into the global financial network, the cartels' ability to corrupt law enforcement and public officials, and acquire personnel, weapons, ammunition, vehicles, planes, communication devices, raw materials for drug production, and all other instrumentalities essential to their operations would be substantially impeded" (Dart, 2016)

Step 4 of the TRM model shows how the cartels use the money to ensure that their organization grows, remains stable, and that the operations continue to be profitable. Laundered money gives the cartels the resources to conduct more gruesome attacks as seen in the final TRM stage.

Four families brought HSBC to court over four separate instances regarding the murders of US family members by the cartels. Two federal US agents, victims Jaime Zapata, and Victor Avila Jr., were attacked in broad daylight and shot dead by two car loads of Los Zetas militants on a highway outside of San Luis Potosi. The case notes that the cartels had military grade weapons, and had over 100 rounds for their AK-47s. The next victims were leaving with their seven-month-old baby after a child's birthday party and were followed by an SUV full of Juarez Cartel members. The pregnant mother, Leslie, was shot in the head. The final assault was on victim Rafael Morales Valencia who exited the church on his wedding day to face 16 assassins from the Sinaloa Cartel.

The cartel forced the wedding party to the ground and kidnapped Rafael, his brother, and his uncle. The Sinaloa Cartel first tortured and then killed them by asphyxiation. These cartels have risen as the largest threat to Mexican national security and are similarly menacing to the US. Since 2006, the cartels have claimed over 100,000 lives.

In *Karen Goldberg et al v UBS* (2009), a suicide bombing on a Jerusalem Bus killed the husband of Karen Goldberg. The victim, Stuart Goldberg, was a dual citizen of Israel and Canada. The Goldberg family, Karen and her seven children, brought the suit against UBS bank for providing services to the Association de Secours Palestine (ASP), a known funder of Hamas. The plaintiffs alleged that UBS was fully aware that they were providing services for the ASP, and indirectly Hamas. UBS is a financial institution headquartered in New York. The court found UBS guilty and held UBS liable under the *Anti-Terrorism Act*. The investor in the case was the Association de Secours Palestinian (ASP), a Swiss-based bank that belongs to an umbrella organization, the 'Union of Good', also known as the 'Charity Coalition' (Levitt, 2007). The founder of the Union of Good, Sheikh Yusef Qardawi is a radical Islamist with an anti-American agenda, who called for suicide bombings against Israeli citizens and attacks on Americans. The Comité de Bienfaisance et de Secours (CBSP), of which ASP is a subsidiary also operates under the Union of Good (Levitt, 2007). CBSP collaborates with more than a dozen humanitarian organizations based in the West Bank, Gaza, Jordan, and Lebanon. Khalid Al-Shuli, who is designated a terrorist under US executive order 13224, presided over CBSP and ASP at the time. ASP was identified as a Hamas fundraising entity by President Bush on October 22, 2003 and was placed on the Office of Foreign Assets Control (OFAC) list as a Specially Designated Global Terrorist (SDGT).

In this case, UBS is represented as a financial intermediary, guilty of knowingly providing banking services to a group affiliated with Hamas. UBS accomplished this by limiting the clients' accounts enough to satisfy Swiss law despite OFAC designating the client as a terrorist threat. The case shows that 222 transactions were made on behalf of the client and failed to implement any measure restricting the client from processing transactions through the US (US Department of the Treasury, 2008). The money in *Goldberg v UBS* was transferred to Tulkarem Zakat Committee, the next financial intermediary, with which many senior members of Hamas are affiliated.

Members include Mohmammed Hamed Qa'adan, head of the Tulkarm Zakat Committee, and Ibrahim Muhammad Salim Salim Nir Al Shams, a member of both the Tulkarm Zakat Committee and the Supreme Hamas leadership in Nur Al-Shams (Levitt, 2002). Tulkarem operates in the West Bank and is not formally recognized as an SDGT but is illegal in Israel. UBS sent money to a Tulkarem account controlled by Hamas through a bank transfer. Ergo, ASP sent the money to Tulkrarem through UBS, and Tulkarem gave the money to Hamas, which completed the transfer of resources.

The funds purposefully travelled to the Tulkarem Committee to fund Hamas. In this case, $25,000 was transferred between October 3, 2003 and January 8, 2004. According to a Washington Institute report on Tulkarem Committee, the US government established that the funds are used by Hamas to support schools that indoctrinate children to become suicide bombers (Levitt, 2002: 1-2). The significance of this case rests in the lack of compliance by financial institutions and working with designated terrorist groups despite being fully aware of the repercussions. The treasury link shows that UBS settled with the US Treasury for 1.7 million USD.

Fields v Twitter (2016) ultimately exposes resources that terrorist organizations have at their disposal that are less common but just as effective to conducting operations. An American citizen, Tamara Fields, based in Florida, brought a lawsuit against Twitter for providing a platform for ISIS and supporting the terrorist organization in carrying out several attacks, including a shooting massacre in Amman, Jordan that killed her husband Lloyd Carl Fields Jr on November 9, 2015. The perpetrator was Abu Zaid, a 28-year-old Jordanian police captain studying at the International Police Training Centre (IPTC). Zaid fired 120 rounds of bullets from an assault rifle and handguns inside the IPTC, where Fields and four other Americans were shot dead while having lunch. ISIS claimed responsibility for the attack and tweeted “the killing shall continue and not stop” shortly after. Twitter has been operating since 2010 and did not block or remove official ISIS twitter accounts on the premise of freedom of expression.

The case of *Fields v Twitter* does not have any identifiable investor(s), which will be discussed in the financing portion of this case study. Twitter is the vehicle for intangible services to propagate and ultimately recruit, inspire, and finance ISIS. TRM does not need to be followed step by step to represent the flow of terrorist financing. Rather, it needs to display the necessary

components. In this case, the transfer of knowledge was a resource to recruit individuals, inspire attacks, and raise funds. This case highlights the use of media as a resource and the implications for new-age propaganda and impact of widespread information dissemination.

This section will attempt to connect the resources moved from the tweets sent out by the various ISIS accounts to collecting resources for perpetrating violent acts or acquiring assets for the terrorist organization. In this case, the aggregation of resources is the value-added of the tweets themselves. These intangible propaganda messages are a necessary component for recruitment – informing individuals on how to carry out attacks.

A. Recruitment

ISIS has many media outlets to aggregate propaganda. Al-Furqan is responsible for ISIS media and has 19,000 followers on Twitter, while Al-Hayat, the official ISIS public relations group has approximately 20,000 followers. Al-Furqa's account is responsible for the dissemination of ISIS' egregious act of brutalities including beheading videos, pictures, and various other multimedia tools of propaganda. The Al-Hayat Media Center operated at least six Twitter accounts that focused on recruiting Westerners. After the tweets are posted, Twitter is used as a core recruiting tool. ISIS recruiters first communicate with prospective individual recruits through Twitter's direct private messaging tools. Online communication allows ISIS to interact directly with individuals from anywhere in the world via direct message. ISIS has recruited about 30,000 foreign fighters via Twitter, including at least 4,500 westerners, among them 250 US citizens.

B. Propaganda

The Dawn of Glad Tidings is an ISIS Twitter App monitored by its social media branch and reportedly reached up to 40,000 tweets in one day when Mosul was captured by ISIS in Iraq. This example shows the ease of propagation through mediums such as social media. ISIS also uses Twitter to post instructional guides and promotional videos which are called "mujatweets." ISIS members, for instance, tweeted English guidelines in June 2014 to instruct Westerners how to travel and join the "fight" in the Middle East. In summary, once individuals follow the account and show interest, they are provided with the necessary tools disseminated through the tweets from

ISIS accounts and Twitter's direct message function to aid the terrorist organization in executions (such as lone-actor attacks), recruiting, or funding.

C. Funding

ISIS has been using Twitter to accumulate funds from sympathizers and organizers, promising rewards for the number of 'Dinars' donated. Advocates and donors then get in touch with the legitimate ISIS accounts and set up private donation systems. The user @jahd_bmalk announced that 26,000 Riyals or $7000 was donated through one campaign, promising donors 'silver and gold status' depending on how much an individual was willing to donate. Not only does this engage willing donors, but also provides alternate ways for individuals to involve themselves with the ease of an app.

Fields v Twitter draws important conclusions in advocating for combatting terrorist resourcing over financing, especially with mediums such as Twitter that encourage wolf-actor attacks. Even without the explicit financing component, the case of *Fields v Twitter* would still involve resources to carry out terrorist attacks. Propaganda is as dangerous as moving funds: it is seen by some 4,500 Westerners sympathizers who were knowingly recruited via Twitter joined ISIS. The transfer of resources also remains largely the same, allowing anonymous investors to communicate with the official ISIS accounts through direct messaging. ISIS saturation of information through Twitter accounts has peaked at 'over 40,000' tweets per day. The intermediaries are those who either collect the funds through one of many accounts and transfer it to ISIS branches or those who join ISIS as a result of its propaganda messages.

V. Discussion

Terrorist resourcing is a collective-action problem that necessitates collaboration to contain terrorist financing. The court cases demonstrate how resources are transferred through various countries, to end up with terrorist organizations. This study identifies nodes to start charting the patterns that terrorist resourcing networks follow.

First, this study examines the effectiveness of FATF, which sets the international standard for countering terrorist financing.[5] The eight special recommendations are designed to prevent terrorist organizations from accessing funds from international financial institutions. However, nearly half of all the cases used at least one financial institution to transfer resources. In 19 of the 32 cases, a simple bank transfer was the method of resource transfer. The FATF is only as effective as the willingness of states to comply with and enforce the eight recommendations domestically.

As discussed, the FATF does not hold any formal enforcement power. Although member countries reformed domestic law based on the FATF recommendations, 18 different countries showed up in this study, which suggests that the FATF goal of "real denial of assets" may not be effective in combatting financial transfers in a global economy (Gardner, 2007: 342). FATF will continue to face challenges to counter various methods of resourcing, including combatting the use of unconventional methods of transferring resources, such as Twitter, as well as the potential use of the Dark Web and cryptocurrencies.

Despite being the financial hub of the global economy, New York only appeared about as often as London as a locational node, and less than Beirut. This may be attributable to the success of the FATF recommendations and the enforcement actions of FinCEN and U.S. law enforcement agencies. Like other financial intelligence units, FinCEN looks to strengthen intergovernmental and institutional sharing of information to combat terrorist financing. Although *Zapata et al. v. HSBC* shows the ineffectiveness in restricting financial institutions to prevent money laundering through placing, layering and integrating, only four banks were found to have laundered money through New York. The FBI appears seven times as the investigating agency, which demonstrates the effectiveness of FinCen to relay information to relevant enforcement agencies.

[5] Fin. Action Task Force, The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 7-8, 37, 39, 47, 55 (2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf [https://perma.cc/5WU8-XU8U]. The FATF's original mandate outlined forty recommendations for combatting money laundering in 1990. The forty recommendations were then revised in 2001 and 2003 to be accompanied by eight special recommendations, and later nine, respectively, to encompass anti-terrorist financing (ATF) measures. The eight special recommendations were revoked in the 2012 amendments to simply include the FATF forty recommendations. Section C of the revised forty recommendations, specifically recommendations 5-8, focus on combatting terrorist financing. Recommendation 5 reaffirms that all terrorist financing should be criminalized, while 6 focuses on the freezing of terrorists' assets in accordance with international laws and regulations. on a risk-based approach to combatting terrorist financing in NPOs.

Member states of the UN have also agreed on a mandate overcome collective-action problems by implementing counter terrorist financing recommendations. Whether the CTITF or CTED have been a driving force in countering terrorist financing, however, cannot be inferred from the evidence in this study. Yet, indications are that collective efforts may be waning: Levitt hypothesizes that as 9/11 becomes more distant, counter-terrorist financing efforts have been diminishing. The CTITF has the potential to counter such trends by promoting cooperation and information sharing to prevent designated terrorist entities from operating. Nonetheless, designated terrorist entities continue to be operational in many cases. For instance, *Goldberg et al. v. UBS* demonstrates the use of multiple financial institutions in Switzerland that are SDGT. The CTED was not mentioned in the cases, but the lapse in international coordination indicates that country reports and information dissemination could be better.

VI. Conclusion

The conventional method of identifying ML/TF FIUs has a limited remit in identifying a terrorist financing networks; conceptually it fails to address the accumulation and dissemination of all forms of resources that support terrorists: The ML/TF model is narrowly focused on a linear process in which actual funds move, neglecting other types of resources and network transactions. By contrast, the TRM accounts for resources that pass through various outlets in various ways. As the cases in this study reinforce, the TRM model offers a more comprehensive approach to identifying and thus prevent terrorist resourcing. Using the TRM, cases such as *HSBC, UBS, and Twitter* were all reduced to a set of identifiable nodes, creating a traceable network of terrorist resources, effectively following the money trail all the way through to the attack. The TRM has the advantage of revealing more nodes along the resourcing process. Nonetheless, due to limitations in available open source data, the research does not convey a robust understanding of all the facets in which resourcing is used by terrorist organizations. Though the research shows the multiple ways in which resources are raised and transferred, the ultimate purpose of funds is usually difficult to attribute. The ability to reverse-engineer the resourcing process from the actual terrorist purpose would likely convey a better understanding of the resourcing network. This approach would likely reveal a greater variety of channels and specific commodities that support

terrorist resourcing, rather than the prevailing approach that is limited strictly to financing per se (Miklaucic & Brewer, 2013).

Some of the findings that emerge from coding nodes and edges are quite instructive. First, the diversity of cases notwithstanding, a clear pattern of resourcing emerged that differs only by scale: the more funds are transferred, the more financial institutions and intermediaries are involved. It is not clear why that is. It is possible that greater sums of money require more financial institutions to disguise the objective of the transfer. Or that greater sums need to be divvied up, which requires more people, each of whom has their own preferences and connections for how to transfer resources successfully, which would explain the greater number of financial institutions involved. Second, the evidence and approach in this study demonstrated that financial hubs, financial institutions, and recipients of resources are not randomly distributed. This raises interesting questions.

That New York and London as global financial hubs show up in the data is not surprising. Given the orders of magnitude difference in their importance to the global financial system however, one would expect to have seen more transfers through New York on the one hand, and more convictions by British authorities on the other hand. This aberration from the expected frequency suggests that US domestic enforcement mechanisms may be having a strong deterrence effect, not just on investors who intentionally circumvent the US and US-based financial institutions, but also on compliance by US financial institutions and those with US-based affiliates to avoid prosecution and fines.

Conversely, how is one to explain the lax approach to enforcement by British authorities? Perhaps the UK prefers to take an intelligence approach to terrorist resourcing: as long as transfers to not pose an imminent threat to the UK or British interests, stand back to watch and follow transfers so as to optimize the insights than can be gleaned about global terrorism. Or British authorities are so busy with kinetic threats that they simply do not have resources to devote to cases that do not pose an actual kinetic risk to the UK, British interests, or immediate allies.

The TRM makes it possible to map transnational terrorist financial networks whereas methods used by the UN, FATF, and FIUs are regionally limited in scope. The conclusion drawn from the coded cases are merely a sample that is intended to question the uniformity of terrorist

financing laws and raise concerns about the various approaches taken by individual countries compared to their regional and transnational counterparts.

In either case, the difference in findings for the US and the UK suggests that countries may be taking difference strategies to terrorist resourcing. This may also explain why different countries are taking different approaches to complying with the FATF and UN efforts: strategy may be driving compliance, rather than compliance driving strategy. The same appears to hold for banks. Relative to the number of banks in the world, especially ones that operate on a global scale, relatively few show up in the dataset; so, the frequency with which some banks recur in the data is all the more significant. This may suggest that intentional or inadvertent non-compliance may be part of a systematic business strategy by a small subset of banks: their global approach doing business may mean that it is simply easier and efficient to risk having to pay the odd US fine, amounts notwithstanding, than to forego the profits that illicit transactions generate. Prosecutions, fines and reputational risk may amount to a way for some banks to position and promote their institution for certain types of transactions that other banks would rather avoid. Alternatively, it may be less of a deliberately strategy, than a cost of doing business: for whatever reason, they feel that their business strategy requires them to take the good with the bad, and incur manageable financial and reputational cost along the way. Since illegal activity is estimated to comprise 3-4% of the global economy, and that activity requires banking services, that speculation is not all that far-fetched.

Equally instructive is the counter-intuitive lack of cases that avail themselves of tax havens. This may be a function of selection bias; or the need for tax havens may be negated by anonymous transactions conducted through offshore financial service providers. Although the research does reveal many instances of Hawala, the movement of resources through non-compliant states whose financial institutions enable more covert methods of resourcing for terrorist organizations (Miklaucic & Brewer, 2013).

To be sure, the n=32 cases is a small subset of cases and thus necessarily marred by possible selection bias and omitted variables. For instance, the notable lack of tax havens could mean that only the stupid or careless ones show up in our sample, and that the smart ones simply do not get caught, or are just too complex, difficult and onerous to prosecute, with no realistic prospect of securing a conviction. That hurdle may explain the relative dearth of convictions for transnational

terrorist financing, money laundering, and tax evasion. In other words, it may be unclear how representative or robust the data is. Still, the data is more systematic and methodical than what has hitherto been on offer in the open-source literature on terrorist financing, and it is replicable. Moreover, the findings in terms of comparable patterns, financial hubs, financial institutions, and recipients suggest that the novelty of the approach this paper posits improves out empirical, conceptual, methodological and theoretical understanding of the phenomenon of terrorist resourcing, how to curb it, and evaluating the efficiency and effectiveness of international and domestic efforts currently underway.

Appendices

Appendix 1. Coding Variables

Jurisdiction and type of legal case: Name of the legal case, where the case was brought to court, and whether it was a criminal or civil lawsuit.

Investor: Initial node whose funds are being transferred to the financial intermediary. Investors who do not possess the means/mechanism to send money to the target organization are not financial intermediaries.

Investor location: Where the investor lived or commenced operation of raising funds.

Bank origin: Name of the bank that transferred the funds.

Bank origin Country: The location of the bank where the transfer of funds took place.

Financial intermediaries: The agent (individual or organization) that facilitated the channelling of funds between the investors (source of funds) and the terrorist organization.

Financial intermediaries' location: All the countries where funds/goods passed through between origin and destination. This does not include the country of the origin (investor) nor the country that the funds/goods ultimately arrive to (terrorist).

Financial intermediary mechanism type: How the funds/goods were transferred from the financial intermediary to the terrorist organization, for example, in the form of bank transfer, hawala, etc.

Financial intermediary mechanism Country: The names of countries where the goods/funds passed through from the financial intermediary to the terrorist organization.

Tax haven name: The name of the tax haven.

Tax haven Country: The tax haven country where the money was deposited.

Terrorist agent: The terrorist organization that was funded including individuals if they have no known ties to an existing terrorist organization.

Terrorist agent affiliates: The organizations directly affiliated or controlled by the terrorist agent through which funding flows.

Terrorist agent Country: Most notable country in which the terrorist organization occupies.

Terrorist agent ideology: The ideology that encapsulates the message of terror extruding from the organization.

Investigating agency name: The name of the committee that investigated the investors and financial intermediaries in the case.

Investigating sub-agency: The sub-agency responsible for the indictment of the individuals.

Investigating agency Country: The country that launched the investigation.

Victims Country: The country the terrorist attacks took place.

Victims count: The number of people murdered, or seriously injured in the terrorist attack.

Cash transferred: Amount of cash successfully transferred from the financial intermediary to the terrorist organization.

Value of non-cash goods transferred: Non-cash assets successfully transferred from the financial intermediary to the terrorist organization.

Transfer start and finish date: The date of the cash transfer, and the date when the cash was received.

Cash raised: Amount of cash raised by the financial intermediary to transfer, but was ultimately unsuccessful in getting the cash to the destination.

Value of non-cash goods raised: Amount of non-cash assets raised by the financial intermediary to transfer, but was ultimately unsuccessful in getting the cash to the destination.

Cash raised start and finish date: The date of the cash transfer, and the date when the cash was received.

Appendix 2. Cases (In no particular order)

1. R. v. Thambaithurai
2. USA v. Qureshi
3. USA v. Mehdi et al.
4. USA v. Alomari et al.
5. Appellee v. Amina Farah Ali
6. Chaim Kaplan et al. v. Central Bank of the Islamic Republic of Iran
7. Licci et al. v. Lebanese Canadian Bank
8. United States v Mohammad Younis
9. Karen Goldberg, et al. v. UBS AG
10. Bank Mellat v Her Majesty's Treasury
11. Weiss et al. v. National Westminster Bank PLC
12. Strauss v. Credit Lyonnais
13. Rothstein v UBS AG (must get second opinion)
14. USA v. Kourani
15. Boim v. Quranic Literacy Institute (very complex)
16. Wultz v Bank of China
17. Gill v Arab Bank
18. Linde v Arab Bank
19. USA v Lebanese Canadian Bank
20. Freeman et al v HSBC PLC et al.
21. R v Khawaja
22. International Relief Fund for the Afflicted and Needy (Canada) v. Canadian Imperial Bank of Commerce
23. Almog et al v Arab Bank PLC
24. USA v Hammoud
25. Tracy v Iranian Ministry of Information and Security
26. R. v. Ahmed
27. Europäisch-Iranische Handelsbank AG v. Council of the European Union
28. United States of America v. Sriskandarajah
29. Zapata vs. HSBC Holding Plc
30. Fields JR v. Twitter INC.
31. Hussein et al v. Dahabshiil
32. International Relief Fund for the Afflicted and Needy (Canada) v. Canada (Minister of Public Safety and Emergency Preparedness)

Works Cited

Bantekas, I. (april 2003). CURRENT DEVELOPMENT: The International Law of Terrorist Financing. *The American Journal of International Law , 97*(2). doi:https://doi.org/10.2307/3100109

Barber, S. (2011, Winter). The "New Economy of Terror:" The Financing of Islamist Terrorism. *Global Security Studies, 2*(1), 1-13. Retrieved April 25, 2017, from http://globalsecuritystudies.com/Barber.pdf

Berger, M. A. (2010). Interdicting Terrorist Financing with Coercion: Strategies for Policy-Makers to Cut the Cash Flow of Terrorist Organizations. *Defence Studies, 10*(3), 387-404. doi:10.1080/14702436.2010.503681

Cassara, John A. (2006) Hide and seek: intelligence, law enforcement, and the stalled war on terrorist finance. Washington, DC: Potomac Books.

Cassara, J. A. (2015). Trade-Based Money Laundering. Print. doi:10.1002/9781119125389

Chaim Kaplan et al. v. Central Bank of the Islamic Republic of Iran, No. 10-43 (RCL) (United States District Court for the District of Columbia August 20, 2013).

Clunan, A. L. (2006). The Fight against Terrorist Financing. *Political Science Quarterly, 121*(4), 569-596. doi:10.1002/j.1538-165x.2006.tb00582.x

Cockfield, Arthur J. (2016). Big Data and Tax Haven Secrecy. *Florida Tax Review, Vol. 18*, pp. 483-539. Available at SSRN: https://ssrn.com/abstract=2757268

CTITF. (2017). About the Task Force - Counter-Terrorism Implementation Task Force. Retrieved May 18, 2017, from https://www.un.org/counterterrorism/ctitf/en/about-task-force

Curtic, G. E., & Karacan, T. (2002, December). The Nexus Among Terrorists, Narcotics Traffickers, Weapons proliferators, and organized Crime Networks in Western Europe. *Library of Congress - Federal Research Division,* 1-33. Retrieved April 25, 2017, from http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf

Dart, T. (2016, February 11). Families of Americans killed by Mexican cartels sue HSBC for laundering billions. Retrieved April 25, 2017, from https://www.theguardian.com/business/2016/feb/11/families-of-americans-killed-by-mexican-cartels-sue-hsbc

ENFORCEMENT INFORMATION FOR August 27, 2015. (2015, August 27). Retrieved April 25, 2017, from https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150827_ubs.pdf

FATF - About. (2017). Retrieved April 25, 2017, from http://www.fatf-gafi.org/about/

Financial Transactions and Reports Analysis Centre of Canada. (2015, May 30). Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Retrieved April 26, 2017, from http://www.fintrac-canafe.gc.ca/act-loi/1-eng.asp

FINCEN. (2017). FINCEN - About. Retrieved April 26, 2017, from https://www.fincen.gov/what-we-do

Freeman, M. (2011). The Sources of Terrorist Financing: Theory and Typology. *Studies in Conflict & Terrorism, 34*(6), 461-475. doi:10.1080/1057610x.2011.571193

Gardner , K. L. (2007). Fighting Terrorism the FATF Way. *Global Governance, 13*(3), 325-345. Retrieved from http://www.jstor.org/stable/27800665.

Gordon, R. K. (2012). Terrorism financing indicators for financial institutions in the United States. *Case Western Reserve Faculty Publication,577*, 765-801. Retrieved June 1, 2017, from http://scholarlycommons.law.case.edu/faculty_publications

Gouvin, E. J. (2003). Bringing out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism. *Baylor Law Review , BO-55*(3), 955-989. Retrieved from http://digitalcommons.law.wne.edu/cgi/viewcontent.cgi?article=1075&context=facschol

Grossman , L., & Newton-Small, J. (2013). The Secret Web: Where Drugs, Porn and Murder Live Online. Retrieved July 28, 2017, from http://time.com/630/the-secret-web-where-drugs-porn-and-murder-live-online/.

Gruber, Sarah M. (2013). Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion? *32 Quinnipiac L. Rev. 135.* Available at SSRN: https://ssrn.com/abstract=2312110

Hall, R. (2005, May). Terrorist Finance: On the Money Trail. *The World Today, 61*(5), 20-22. Retrieved April 25, 2017, from https://search.proquest.com/docview/60687938?accountid=6180.

International Relief Fund for the Afflicted and Needy (Canada) v. Canadian Imperial Bank of Commerce, No. CV-13-479658 (SUPERIOR COURT OF JUSTICE - ONTARIO July 05, 2013).

Jainski, W. (2011). New challenges in combating money laundering, terrorist financing and corruption . *Police Academy in Szczytno ,* 3(2), 181-200. Retrieved August 7, 2017, from internalsecurity.wspol.eu.

Karen Goldberg et al. v UBS, No. No. CV–08–375 (CPS) (United States District Court September 24, 2009).

Krieger, T., & Meierrieks, D. (2011, June 8). Terrorist Financing and Money Laundering. *SSRN Electronic Journal,* 1-26. http://dx.doi.org/10.2139/ssrn.1860069

Kurzrok, A., & Hund, G. (june 2014). Stopping Illicit Procurement: Lessons From Global Finance. *Arms Control Today,* 13-17. Retrieved April 26, 2017, from https://www.armscontrol.org/act/2014_06/Features/Stopping-Illicit-Procurement-Lessons-From-Global-Finance.

Latif, M., & Khan, R. (2010). United Nations global counterterrorism strategy: Achievements and challenges. Strategic Studies, Xxx(3)

Leuprecht, C., Walther, O., Skillicorn, D. B., & Ryde-Collins, H. (2015). Hezbollah's global tentacles: A relational approach to convergence with transnational organised crime. *Terrorism and Political Violence,*1-20. doi:10.1080/09546553.2015.1089863

Levitt, M. (2002, August 1). Charitable and Humanitarian Organizations in the Network of International Terrorist Financing. *The Washington Institute for Near East Policy ,* 1-8. Retrieved April 25, 2017, from http://www.washingtoninstitute.org/policy-analysis/view/charitable-and-humanitarian-organizations-in-the-network-of-international-t

Levitt, M. (2007, March 20). U.S.-Designated Hamas Front Gets Symbolic Win in France. Retrieved April 25, 2017, from http://www.washingtoninstitute.org/policy-analysis/view/u.s.-designated-hamas-front-gets-symbolic-win-in-france

Levitt, M., & Jacobson, M. (2008, Fall). The US Campaign to Squeeze Terrorists' Financing. *Journal of International Affairs, 62*(1), 67-85. Retrieved April 25, 2017, from http://www.jstor.org/stable/24358145

Lo, C. (2002). FATF Initiatives To Combat Terrorist Financing. *OECD Observer, 231*, 39-40. Retrieved April 25, 2017, from https://search.proquest.com/docview/217476250?accountid=6180.

Matfess, H., & Miklaucic, M. (2016). *Beyond Convergence: World without Order*. Washington, D.C.: Center for Complex Operations, Institute for National Strategic Studies, National Defense University.

Miklaucic, M., & Brewer, J. (Eds.). (2013). *CONVERGENCE: Illicit Networks and National Security in the Age of Globalization*. Washington, D.C.: National Defense University Press.

Millar, A., & Fink, N. C. (2013). Getting back to basics? renewing the mandate of the UN security council counter-terrorism committee executive directorate for 2014-2016 Center on Global Counterterrorism Cooperation. Retrieved from https://search-proquest-com.proxy.queensu.ca/docview/1761662656?accountid=6180

Nakhasi, S. S., (2007, January) Western Unionizing the Hawala?: The Privatization of Hawalas and Lender Liability, *Northwestern Journal of International Law & Business*, 27(2), 475-496.

O'Halloran, P. J., Ghanbar Pour Dizboni, A., Leuprecht, C., Adelstein, D., Green, A., & Porges, M. (July 2016). Research into How Resources are Acquired, Moved and Used to Support Acts of Terrorism. *TSAS,* 16-10, 1-86. Retrieved April 26, 2017, from http://tsas.ca/wp-content/uploads/2016/07/TSASWP16-10_OHalloranEtAl.pdf

Protecting Charitable Organizations: Commite de Bienfaisance et de Secours aux Palestiniens Association de Secours Palestinien. (2010, December 1). Retrieved April 25, 2017, from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/protecting-charities_execorder_13224-b.aspx

Realuyo, C. (2014). The Terror-Crime Nexus, Hezbollah's Global Facilitators. *Centre for Complex Operations. 5(1), 117-131.* from http://www.academia.edu/19545694/_The_Terror-Crime_Nexus_Hezbollah_s_Global_Facilitators_

ROMANIUK, P. (2010). Institutions as swords and shields: Multilateral counter-terrorism since 9/11. Review of International Studies, 36(3), 591-613. doi:http://dx.doi.org.proxy.queensu.ca/10.1017/S0260210510000653

Rose, G. (2017). Regulating Australian Charities Operating Overseas to Deter Funding of Political Violence. Article in preparation.

Shelley, Louise I. (2014). *Dirty Entanglements: Corruption, Crime, and Terrorism*. Cambridge: Cambridge University Press.

Sriskandarajah v. United States of America (Supreme Court of Canada December 14, 2012).

Solin, M., & Zerzan, A. (2010, January). Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks. *GSMA: Mobile Money for the Unbanked: GSMA Discussion Paper,* 1-35. Retrieved April 25, 2017, from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/amlfinal35.pdf

Stringer , K. (2011). Tackling Threat Finance: A Labor for Hercules or Sisyphus? *Parameters: US army War College* , 41(1), 101-118. Retrieved from http://ssi.armywarcollege.edu/pubs/parameters/articles/2011spring/stringer.pdf

TAMARA FIELDS, et al., Plaintiffs, v. TWITTER, INC., Defendant., No. 16-cv-00213-WHO. (United States District Court, N.D. California. August 10, 2016).

UN. (1994, December 9). A/RES/49/60. Measures to eliminate international terrorism. Retrieved April 26, 2017, from http://www.un.org/documents/ga/res/49/a49r060.htm

United States Senate. (2005, November) *Saudi Arabia: friend or foe in the war on terror?: hearing before the Committee on the Judiciary, United States Senate, One Hundred Ninth Congress, first session, November 8, 2005*. (2007). Retrieved May 7, 2017, from https://archive.org/stream/gov.gpo.fdsys.CHRG-109shrg34114/CHRG-109shrg34114_djvu.txt

US Department of the Treasury. (2008, November 6). Fact Sheet: Treasury Strengthens Preventive Measures Against Iranp1258. Retrieved April 26, 2017, from https://www.treasury.gov/press-center/press-releases/Pages/hp1258.aspx

US State Department. (2015). Chapter 3: State Sponsors of Terrorism Overview. Retrieved May 18, 2017, from https://www.state.gov/j/ct/rls/crt/2015/257520.htm

USA v. Mehdi, Samer, et al., No. 09-20852 CR-GOLD (United States District Court, Southern District of Florida February 24, 2010).

USA v. Qureshi, No. 04-60057-01 (United States District Court, Western District of Louisiana, Lafayette-Opelousas Division February 11, 2005).

Viles, T. (2008, January). Hawala, hysteria and hegemony. *Journal of Money Laundering Control*, 11(1), 25-33. doi 10.1108/13685200810844479

Vlcek, W. (2008). A Leviathan Rejuvenated: Surveillance, Money Laundering, and the War on Terror. *International Journal of Politics, Culture, and Society*, 20(1-4), 21-40. doi:10.1007/s10767-007-9020-6

Winer, J. M. (2008). Countering Terrorist Finance: A Work, Mostly in Progress. *The ANNALS of the American Academy of Political and Social Science*, 618(1), 112-132. doi:10.1177/0002716208317696

Zapata et. al. v. HSBC Holdings PLC et. al., No. 1:16-cv-00030 (UNITED STATES DISTRICT COURT, SOUTHERN DISTRICT OF TEXAS, BROWNSVILLE DIVISION September 02, 2016).

Zdanowicz, J. S. (2004, May). Detecting money laundering and terrorist financing via data mining. *Communications of the ACM, 47*(5), 53-55. doi:10.1145/986213.986239