TRACKING TRANSNATIONAL TERRORIST RESOURCING NODES AND NETWORKS

CHRISTIAN LEUPRECHT, ARTHUR COCKFIELD, PAMELA SIMPSON, AND MASEEH HASEEB*

ABSTRACT

In light of persistent terrorist attacks in Europe and elsewhere, the study of terrorist resourcing and financing has attracted renewed attention. How are terrorists' 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? Answers to these and other questions can help law enforcement investigate, disrupt, and neutralize cross-border terrorist resourcing. Evidence and data on this phenomenon is scarce, of questionable quality, irreplicable, and can be difficult to come by. This study is the first comprehensive effort to collect, code, analyze, and compare available open-source case law data on transnational terrorist resourcing networks. Under the study's methodology, the conventional yet strict focus on financing is broadened to resources, which includes forms other than cash, including trade-based fraud and online social networks. The analysis reveals common cross-border resourcing patterns and usage of financial intermediaries such as banks. It thus contributes to the ongoing optimization of anti-terrorist resourcing laws, policies, and risk-management practices.

---

* Christian Leuprecht is Class of 1965 Professor in Leadership at the Royal Military College, Department of Political Science and Economics, Canada, cross-appointed to Queen's University and Adjunct Research Professor at Charles Sturt University and Flinders University; Arthur Cockfield is a Professor with Queen's University Faculty of Law, Canada; Pam Simpson is an M.A. candidate, Queen's University, Department of Political Studies; and Maseeh Haseeb is a candidate for a Ph.D., Queen's University Faculty of Law. An earlier version of this Article was presented at the Stanford University Law School symposium 'What's Law Got to do With It? Examining Law in a Changing World' on November 3, 2017. The Article was also presented twice at workshops for the Canadian Network for Research on Terrorism, Security, and Society (TSAS). The authors are grateful for the many helpful comments received. They would also like to thank Bharbara Parken, JD candidate at Queen's University Faculty of Law, for her helpful research assistance.

I. INTRODUCTION

On February 15, 2011, two U.S. federal agents were attacked in broad daylight by Mexican narco-terrorists, killing one of the agents while severely wounding the other; three days later, the same group tortured and killed three members of a wedding party.[1] A lawsuit later alleged that terrorists were funded through the purportedly intentional actions of HSBC bank.[2] On January 29, 2004, a suicide bombing on a Jerusalem bus killed a Canadian Israeli resident; subsequent litigation showed that UBS bank was supplying funds to a group affiliated with a designated terrorist organization.[3]

In a different case, a lawsuit against Twitter reveals how the platform has been used to solicit donations to raise resources and recruits for terrorist attacks.[4] In 2014, the Islamic State of Iraq and Syria (ISIS), a terrorist group, harnessed the power of Twitter to recruit new members and spread propaganda throughout its network.[5] Through a Twitter software application called "Dawn of Glad Tidings," ISIS members produced up to 40,000 tweets in one day, which gradually helped to recruit about 30,000 foreign fighters, including at least 4,500 individuals from North America and Europe.[6] About US$300,000 was also funnelled through U.S. banks to carry out the September 11th attacks without being detected.[7] In all of these cases, litigation provided a wealth of information concerning how terrorists plan, finance, and execute their attacks.[8]

---

1. *See* Complaint at 1-3, Zapata v. HSBC Holdings Plc, No. 1:17-cv-06645 (E.D.N.Y. Nov. 14, 2017).

2. *See id.* at 1-5.

3. *See* Goldberg v. UBS AG, 660 F. Supp. 2d 410 (E.D.N.Y. 2009).

4. *See* Fields v. Twitter, Inc., 200 F. Supp. 3d 964 (N.D. Cal. 2016).

5. Complaint at 1, Fields v. Twitter, Inc., 200 F. Supp. 3d 964 (N.D. Cal. 2016) (No. 16-cv-00213-WHO).

6. *See id.* at 5, 7-8.

7. *See* Kevin E. Davis, *The Financial War on Terrorism*, *in* GLOBAL ANTI-TERRORISM LAW AND POLICY 205 (Victor V. Ramraj et al. eds., 2d ed. 2012); Matthew Levitt, *Charitable and Humanitarian Organizations in the Network of International Terrorist Financing*, WASH. INST. (Aug. 1, 2002), https://www.washingtoninstitute.org/policy-analysis/view/charitable-and-humanitarian-organizations-in-the-network-of-international-t [https://perma.cc/R5TR-ZMHE].

8. *See* Paul M. Barrett, *Are Credit Suisse, RBS, Standard Chartered, HSBC, and Barclays Terrorist Banks?*, BLOOMBERG BUSINESSWEEK, Feb. 23, 2015, at 52-54 (discussing U.S.

The data gleaned from contemporary cases is important because, in light of persistent terrorist attacks, the study of terrorism financing has attracted renewed attention.[9] This raises the following questions: 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 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.[10] It thus contributes to the ongoing optimization of anti-terrorist resourcing laws, policies, and risk-management practices.

This Article is organized as follows. Part II describes some key concepts surrounding terrorist financing. Part III describes international cooperative efforts, including a review of efforts to contain terrorist financing by the Financial Action Task Force (FATF), the United Nations (UN), and various government departments tasked with tracking terrorist financing (normally called Financial Intelligence Units (FIUs)). Part IV sets out the method of this study, which proposes a shift from the conventional yet strict focus on terrorist *financing* by broadening the remit to *resourcing* to include resources other than cash, such as trade-based fraud and the use of online social networks.[11]

---

civil cases where plaintiffs sued foreign banks for financing terrorism).

9. By "terrorist," we mean an individual who belongs to a group designated by the United Nations as a terrorist organization. *See Defining Terrorism*, UNITED NATIONS OFF. ON DRUG AND CRIMES (July 2018), https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html [https://perma.cc/DSV6-992L] (stating that the definition of transnational terrorism exists within customary law as: "(i) the perpetration of a criminal act (such as murder, kidnapping, hostage-taking, arson, and so on), or threatening such an act; (ii) the intent to spread fear among the population (which would generally entail the creation of public danger) or directly or indirectly coerce a national or international authority to take some action, or to refrain from taking it; (iii) when the act involves a transnational element"); *see also* G.A. Res. 49/60, *Measures to Eliminate International Terrorism* (Dec. 9, 1994), http://www.un.org/documents/ga/res/49/a49r060.htm [https://perma.cc/9RPL-7VJ6] (highlighting that the United Nations declares terrorism as: "Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.").

10. An earlier study by the Department of Homeland Security conducted a similar review of U.S. case law. For discussion, see Richard Gordon, *Terrorism Financing Indicators for Financial Institutions in the United States*, 44 CASE W. RES. J. INT'L L. 765 (2012). The underlying data is not available to the public; hence, the study is not replicable.

11. *But see* Muhamet Aliu et al., *A Review of Sources on Terrorist Financing*, 13 ACTA UNIVERSITATIS DANUBIUS: JURIDICA 97 (2017). In contrast, our study relies on primary

To this effect, this study introduces a five-step approach, dubbed the Terrorist Resourcing Model (TRM).[12] Combined with the basic premise of Social Network Analysis—an analytical tool used by political scientists and others to discern relationships among data points[13]—TRM provides insights into the relationships among facts through coding analysis.[14]

Part V presents the results of thirty-two transnational cases of terrorist resourcing—the universe of known transnational terrorist resourcing cases for which sufficient open-source data exists (see Appendix A). These cases consist largely of civil and criminal cases. Not all of these cases have been prosecuted; some were settled out of court while some are still winding their way through the court system. The sample is affected by obvious selection bias, as many of these cases were brought before U.S. courts, several by a specific subset of plaintiffs and law firms. Since some of the matters may settle, and since the burden of proof in civil cases is lower than in criminal cases, not all data are equally robust.[15]

Nonetheless, these cases are a good starting point—better, in any event, than the proliferation of anecdotal evidence and single narrative case studies whose conclusions are often conjectural.[16] Although these thirty-two cases differ markedly, they show surprisingly similar patterns that differ only in scale. They also reveal indicative findings

---

sources based on case law to explore data that reveals the nodes and networks of terrorist resourcing.

12. For a preliminary working paper version of the TRM, see Patrick J. O'Halloran et al., *Research Into How Resources are Acquired, Moved and Used to Support Acts of Terrorism* (Can. Network for Research on Terrorism, Sec. and Soc'y, Working Paper No. 16-10, 2016) [hereinafter O'Halloran et al., *Research on Resources*], https://www.tsas.ca/wp-content/uploads/2018/03/TSASWP16-10_OHalloranEtAl.pdf [https://perma.cc/J9JH-49LV]; Patrick J. O'Halloran et al., *The Terrorist Resourcing Model Applied to Canada*, 21 J. MONEY LAUNDERING CONTROL 33 (2018) [hereinafter O'Halloran et al., *Terrorist Resourcing Model*], https://doi.org/10.1108/JMLC-12-2016-0050.

13. *See* Christian Leuprecht et al., *Hezbollah's Global Tentacles: A Relational Approach to Convergence with Transnational Organized Crime*, 29 TERRORISM & POL. VIOLENCE 902 (2017); *see also* THE SAGE HANDBOOK OF SOCIAL NETWORK ANALYSIS (John P. Scott & Peter J. Carrington eds., 2011).

14. *See* O'Halloran et al., *Terrorist Resourcing Model*, *supra* note 12.

15. In countries such as the United States, Canada, and other common law countries, prosecutors must prove beyond a reasonable doubt that the mental and physical elements of a crime have been committed. For civil cases, a party must establish on a balance of probabilities that the other side has engaged in tortious acts. *See* James Q. Whitman, *The Origins of "Reasonable Doubt"*, YALE L. SCH. LEGAL SCHOLARSHIP REPOSITORY (Mar. 2005), http://digitalcommons.law.yale.edu/fss_papers/1 [https://perma.cc/B66Z-B45P]; *see also* Donald A. Dripps, *The Constitutional Status of the Reasonable Doubt Rule*, 75 CALIF. L. REV. 1665 (1987).

16. *See, e.g.*, Shima Baradaran et al., *Funding Terror*, 162 U. PA. L. REV. 477, 519 (2014) (describing the usage of tax havens for terrorist financing purposes despite the fact that no such evidence exists).

with regards to financial hubs, banks, and entities. Following this analysis, the study delves deeper into three case studies to illustrate the broader findings in terms of: 1) the patterns used to raise and transfer resources; 2) the added value of broadening the remit from financing to resourcing; and 3) the vexing problem of attribution of the purpose of funds. Part VI reviews the findings and offers a preliminary assessment of international and domestic progress in curbing terrorist resourcing. Finally, this Article concludes that the TRM provides a comprehensive framework that reveals many of the nodes and networks of terrorist resourcing.

II. OVERVIEW OF TERRORIST FINANCING

A. Using Legal Monies to Fund Terrorism

In the aftermath of the September 11th terrorist attacks, the grafting of anti-terrorist financing laws onto existing anti-money laundering laws created an awkward fit in some situations.[17] The main difference between the two is that money laundering, by definition, involves taking illicit proceeds (for example, profits from the sale of illegal narcotics) and making these proceeds seem as if they came from a legal source. Hence the term "laundering," which suggests that the dirty money appears to have been sufficiently legitimated and placed within the conventional banking system. Terrorist financing, by contrast, tends to emanate from perfectly legal sources but is subsequently used for the criminal purpose of financing terrorists.[18]

In other words, 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.[19] 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 France with the use of international calling cards.[20] However, the goal of terrorist organizations is also to conceal the money trail, for which the techniques of money laundering are well-developed.[21]

---

17. *See* Bruce Zagaris, *The Merging of the Anti-Money Laundering and Counter-Terrorism Financial Enforcement Regimes After September 11, 2001*, 22 BERKELEY J. INT'L L. 123 (2004) (critiquing this approach).

18. *See* Tim Krieger & Daniel Meierrieks, *Terrorist Financing and Money Laundering* 2 (Ctr. for Int'l Econ., Working Paper No. 2011-07, 2011), http://dx.doi.org/10.2139/ssrn.1860069 [https://perma.cc/8KR3-NV98].

19. *See id.* at 2.

20. *See* Shanaka Jayasekara, LTTE Fundraising and Money Transfer Operations (October 2007) (unpublished paper presented at the International Conference on Countering Terrorism held in Colombo), https://www.linct-aa.org/app/download/18844999/Tamil.Tiger.Fundraising.pdf [https://perma.cc/3QU3-CDKJ].

21. *See* Kathryn L. Gardner, *Fighting Terrorism the FATF Way*, 13 GLOBAL GOVERNANCE

One way terrorist groups raise money is by operating a legitimate business and not reporting all of its income to the government.[22] For example, Al-Qaeda operated many legitimate businesses in South Sudan, hosting farms, trading companies, a tannery, furniture companies, a bakery, and an investment company.[23] Because all of the businesses operated legally under domestic laws, the state was unable to detect the criminal activity.[24]

Other legitimate means of transferring money include legal donations, funds from charities, fundraising, and private investors.[25] Charities that support relief missions in conflict-prone regions of the world, using a multitude of transfer mechanisms in a globally linked economy, weave networks that veil the destination of the funds and their ultimate purpose.[26] Misuse of funds can even originate with high profile charities such as World Vision's Australian branch, which donated to relief efforts in Gaza that were found to be diverting sixty percent of donations to Hamas.[27] The transfer of funds is difficult to audit because resources are diverted and channeled through licit and illicit networks.

Cash can also be funneled through bank transfers or transferred manually. Financial institutions can divide customers using the service to fund illegal activities into two types of consumers: 1) "mission specific," referring to active terrorist cells on the one hand; and 2) inactive groups, or "sleeper cells," on the other.[28] For example, the nineteen hijackers involved in the September 11th attacks opened twenty-four domestic bank accounts with amounts ranging between US$3,000-$5,000, and they gave infrequent addresses and no social security numbers.[29]

---

325 (2007). The fact that terrorists want to conceal their assets is implied. *See also* Krieger & Meierrieks, *supra* note 18, at 13-14 (although it focuses on the difference, it also discusses the similarities between terrorism financing and money laundering, including structural similarities).

22. *See* Michael Freeman, *The Sources of Terrorist Financing: Theory and Typology*, 34 STUD. CONFLICT & TERRORISM 461, 469 (2011).

23. *Id.*

24. *See id.*

25. *See, e.g.*, Anita I. Anand, *Combating Terrorist Financing: Is Canada's Legal Regime Effective?*, 61 U. TORONTO L.J. 59, 59-61 (2011) (recommending further scrutiny of the legal framework on terrorist financing).

26. *See* Aviv (Cohen) Dekel, *The Unique Challenge of Dual-Purpose Organizations: Comparative Analysis of U.S. and Israel Approaches to Combating the Finance of Terrorism*, 35 LOY. L.A. INT'L & COMP. L. REV. 389, 400-01 (2013) (arguing for a more aggressive pursuit of the connection between charities and terrorist financing).

27. Gregory Rose, *Regulating Humanitarian Assistance by Australian Charities: Legal Tools to Deter Funding of Terrorism Abroad*, 92 AUSTL. L.J. 273, 277 (2018).

28. Ilias Bantekas, *The International Law of Terrorist Financing*, 97 AM. J. INT'L L. 315, 320 (2003).

29. *Id.* at 321.

Such dormant accounts hold small sums of money that can easily be withdrawn and transferred.[30]

Importantly, even though funds may emanate from legal sources, individuals who transfer monies across borders for terrorist financing purposes may be engaging in offshore tax evasion if they purposely do not disclose income or assets to their governments.[31] In addition, efforts to avoid detection of legal sources of monies that are subsequently transferred across borders may also constitute the crime of international money laundering.[32] In other words, even if funds come from legal activities, subsequent cross-border transfers of these monies—especially if hidden from local authorities—can trigger crimes and potential interventions from tax and law enforcement authorities.[33]

B. Using Illegal Monies to Fund Terrorism

While terrorists can rely on legal sources of monies for funding, they also rely on illegally-raised resources. Under one view, the methods of terrorism and criminal resourcing are converging.[34] Illegal methods of terrorist financing encompass an array of activities, from petty crime, extortion, and kidnapping to trade-based money laundering.[35] John Cassara identifies "familiar relations" as a pattern among trade-based money laundering networks.[36] This is replicated by Christian Leuprecht and others' study of Hezbollah's networks, where trade-

---

30. *Id.*

31. *See, e.g.*, 26 U.S.C. § 7201 (2012) ("Any person who willfully attempts in any manner to evade or defeat any tax imposed by this title or the payment thereof shall, in addition to other penalties provided by law, be guilty of a felony and, upon conviction thereof, shall be fined not more than $100,000 ($500,000 in the case of a corporation), or imprisoned not more than 5 years, or both, together with the costs of prosecution."). The penalties under the Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. § 5311 (2012) (commonly referred to as the Bank Secrecy Act (BSA)) for failure to file a foreign bank account report (FBAR) are more severe than the ones imposed by the Internal Revenue Code. For instance, a U.S. person who lives outside of the United States and fails to file an FBAR for one year can attract a penalty of up to fifty percent of the value of any undisclosed taxpayer assets. Two years of noncompliance with FBAR requirements can result in a penalty equaling 100 percent of the taxpayer's undisclosed assets. *Id.* § 5321. For discussion of these laws and penalties, see ARTHUR COCKFIELD & DAVID KERZNER, INTERNATIONAL TAXATION CORE CONCEPTS 149-70 (2d ed. 2017).

32. Arthur J. Cockfield, *Big Data and Tax Haven Secrecy*, 18 FLA. TAX REV. 483, 492-95 (2016) [hereinafter Cockfield, *Big Data*].

33. *Id.*

34. *See* Leuprecht et al., *supra* note 13; *see also* CONVERGENCE: ILLICIT NETWORKS AND NATIONAL SECURITY IN THE AGE OF GLOBALIZATION (Michael Miklaucic & Jacqueline Brewer eds., 2013) [hereinafter CONVERGENCE].

35. *See* Freeman, *supra* note 22, at 469.

36. *See* JOHN A. CASSARA, TRADE-BASED MONEY LAUNDERING: THE NEXT FRONTIER IN INTERNATIONAL MONEY LAUNDERING ENFORCEMENT 51-52 (2016) [hereinafter CASSARA, TRADE-BASED].

based cigarette smuggling and fraud in Michigan and North Carolina flowed through familiar connections.[37] Such informal value-transfer systems makes trade-based money laundering incredibly difficult for financial intelligence to detect and stop.[38]

The illicit economies of trade, such as money laundering, can contribute extensively to the formal economy.[39] There are also informal ways to transfer money covertly, such as through *hawala*.[40] *Hawala* is an informal means for individuals to transfer money among entities or individuals (often family members) outside of the country.[41] *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, transfers the money, and takes the commission.[42] Nakhasi observes that

> [T]he *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 the series of transactions, which eventually equalize the position of one *hawaladar* against another.[43]

An estimated US$200 billion per year enters the international financial system through the method of *hawala*.[44] The *hawala* system is not a perfect vehicle 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 transmit money to their home countries, and terrorist financing flows may be concealable within this, typically larger, existing set of flows.[45] As our case law analysis reveals, *hawala* has been used between countries such as the United States and Somalia, and it involves individuals and controversial money transfer businesses.[46] *Hawala* leaves behind few records and remains unregulated; thus, it is ripe for potential abuse, including terrorist financing.

---

37. *See* Leuprecht et al., *supra* note 13, at 907-09.

38. *See* JOHN A. CASSARA, HIDE & SEEK: INTELLIGENCE, LAW ENFORCEMENT, AND THE STALLED WAR ON TERRORIST FINANCE 215-18 (2006) [hereinafter CASSARA, HIDE & SEEK].

39. *See* Jonathan M. Winer, *Countering Terrorist Finance: A Work, Mostly in Progress*, 618 ANNALS AM. ACAD. POL. & SOC. SCI. 112, 121 (2008).

40. *Id.* at 116-17.

41. CASSARA, TRADE-BASED, *supra* note 36, at 51-54.

42. *See* CONVERGENCE, *supra* note 34, at 117.

43. Smriti S. Nakhasi, *Western Unionizing the* Hawala*?: The Privatization of* Hawalas *and Lender Liability*, 27 NW. J. INT'L L. & BUS. 475, 477-78 (2007) (citations omitted).

44. *See* Robert Hall, *Terrorist Finance: On the Money Trail*, WORLD TODAY, May 2005, at 20, 21.

45. *Id.* at 21.

46. *See* United States v. Ali, 799 F.3d 1008 (8th Cir. 2015); United States v. Ali, 682 F.3d 705 (8th Cir. 2012).

III. GLOBAL COOPERATION AGAINST TERRORIST FINANCING

This study uses case law and the TRM to map and detect terrorist resourcing patterns. Because one of the objectives of this study is to gauge the effectiveness of current legislation, regulation, and policy, this Part surveys international and domestic laws and policies that govern terrorist financing. It begins by setting out academic perspectives that support the need for international cooperation. Next, it provides an overview of the complex international laws and policies striving to inhibit terrorist financing. As subsequently discussed, the most important international fora for cooperative measures against terrorist financing are the United Nations and the Financial Action Task Force. These bodies develop laws and policies that are implemented by participating nations and typically enforced by government agencies that are called financial intelligence units (such as FinCEN within the United States). This Part then reviews the limits of collective action by international organizations and their respective members.

A. The Need for Global Cooperation

1. Academic Perspectives

Collaboration among international and domestic actors is normally viewed as indispensable to contain terrorist resourcing.[47] The general consensus is that financing is the lifeblood of these organizations, actively enabling terrorist organizations to operate and execute attacks.[48] The prevailing approach to combatting terrorist financing is through collective action.[49] International organizations forge a collective-action strategy to ensure allied states comply with international standards.[50] 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

47. *See* Michael A. Berger, *Interdicting Terrorist Financing with Coercion: Strategies for Policy-Makers to Cut the Cash Flow of Terrorist Organizations*, 10 DEF. STUD. 387, 392 (2010); Anne L. Clunan, *The Fight Against Terrorist Financing*, 121 POL. SCI. Q. 569 (2006); *see* Gardner, *supra* note 21, at 328; Anja P. Jakobi, *Governing Illicit Finance in Transnational Security Spaces: the FATF and Anti-Money Laundering*, 69 CRIME L. & SOC. CHANGE 173 (2018); Levitt, *supra* note 7.

48. *See* Freeman, *supra* note 22, at 461; *see also* CONVERGENCE, *supra* note 34.

49. *See* Berger, *supra* note 47, at 392; Clunan, *supra* note 47; Gardner, *supra* note 21, at 335.

50. Gardner, *supra* note 21, at 335.

country.[51] As such, domestic organizations are heavily invested in transnational intelligence sharing and building measures to confront international terrorist resourcing collectively.[52]

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), government financial intelligence units (FIUs), the Financial Crimes Enforcement Network (FinCEN) in the United States, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and the Australian Transaction Reports and Analysis Centre (AUSTRAC).[53] The United Kingdom has a more complex set of organizations with oversight of money laundering, but it has a new Office for Professional Body Anti-Money Laundering Supervision (OPBAS).[54]

2. 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.[55] Terrorist financing gained international notoriety after Al-Qaeda's bombing of the U.S. embassies in Tanzania and Kenya.[56] The UN continues to build on the original "International Convention for the Suppression of the Financing of Terrorism" (Convention), which is an initiative specific to countering terrorist financing.[57] Following the September 11th attacks, the UN Security Council (UNSC) introduced Resolution 1373, which actively worked to "suppress the financing of terrorism."[58] This resolution specifically criminalizes the "collection and provision of funds for terrorist purposes" through established measures for member states to freeze the funds of persons involved in terrorism and terrorist organizations.[59] Further, adopted in 2014, Resolution 2178 emphasizes the importance of information-sharing between domestic member states and international organizations, the suppression of involvement of individuals in

51. *See id.* at 341; Hall, *supra* note 44, at 21.

52. *See* Clunan, *supra* note 47; O'Hallaran et al., *Research on Resources*, *supra* note 12.

53. *See* Bantekas, *supra* note 28; Berger, *supra* note 47, at 392; Clunan, *supra* note 47; Jakobi, *supra* note 47, at 173; Rose, *supra* note 27.

54. *Office for Professional Body Anti-Money Laundering Supervision (OPBAS)*, FIN. CONDUCT AUTH., https://www.fca.org.uk/opbas [https://perma.cc/D89G-A97Q].

55. *See* Bantekas, *supra* note 28.

56. *See* Clunan, *supra* note 47.

57. *Id.* at 575.

58. *Terrorism Financing*, SEC. COUNCIL COUNTER-TERRORISM COMM., https://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/ [https://perma.cc/XM4Z-RAEK].

59. *Id.*

terrorist organizations from travelling abroad, and increasing profiling of individuals travelling, especially suspected foreign fighters.[60] Although UN member states are encouraged to adopt updated measures "combatting the financing of terrorism" (CTF), member states' compliance has been waning as the September 11th attacks become more distant.[61]

The UN formal counter-terrorism branches include the Counter Terrorism Implementation Task Force (CTITF), the United Nations Counter-Terrorism Center (UNCCT), operating within the CTITF, the UN Global Counter Terrorism Strategy, the 1267 Monitoring Team, the United Nations Office on Drugs and Crime (UNODC), the Counter Terrorism Committee Executive Directorate (CTED), and the UN Office of Counter-Terrorism.[62]

The CTITF was established in 2005 by the Security General to coordinate the counter-terrorism efforts of the General Assembly and the Security Council's cohesive global counter-terrorism strategy.[63] The CTITF manifests a common approach by member states against terrorism, focusing on strengthening individual and collective capacities of countries alongside the UN to prevent and counter terrorism. Main tenets of the strategy include increased coordination among states, especially in combatting money laundering.[64] 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.[65] The UNCCT, working within the CTITF, focuses on three main objectives: 1) implementing the four pillars of the UN Global Counter-Terrorism Strategy through national and regional development goals; 2) fostering a cooperative international community and promoting counter-terrorism centres; and 3) member states' capacity to strengthen

60. S.C. Res. 2178 (Sept. 24, 2014), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2178%20%282014%29 [https://perma.cc/8X4E-QCSA].

61. *See* Matthew Levitt & Michael Jacobson, *The U.S. Campaign to Squeeze Terrorists' Financing*, 62 J. INT'L AFF. 67, 73 (2008).

62. *See UN Global Counter-Terrorism Strategy*, UNITED NATIONS OFF. COUNTER-TERRORISM, https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy [https://perma.cc/89XE-XEHR].

63. *See* Peter Romaniuk, *Institutions as Swords and Shields: Multilateral Counter-Terrorism Since 9/11*, 36 REV. INT'L STUD. 591 (2010).

64. *Coordination and Coherence of the Counter-Terrorism Efforts of the United Nations*, UNITED NATIONS OFF. COUNTER-TERRORISM, https://www.un.org/counterterrorism/ctitf/en/about-task-force [https://perma.cc/2BRT-GUH7].

65. *See* Muhammad I. Latif & Rehman A. Khan, *United Nations Global Counterterrorism Strategy: Achievements and Challenges*, 30 STRATEGIC STUD. 1 (2010), http://issi.org.pk/wp-content/uploads/2014/06/1299823784_75120807.pdf.

counter-terrorist capability.[66] The UN Global Counter Terrorism Strategy was adopted in September 2006 and acts as "a unique global instrument to enhance national, regional and international efforts to counter terrorism."[67] The four pillars are: 1) to address conditions conducive to the spread of terrorism; 2) to prevent and combat terrorism; 3) to build states' capacity and build the role of the UN; and 4) to ensure human rights and the rule of law.[68]

A subsidiary organ of the UNSC pursuant to Resolutions 1526, 2253, and 2368 is the Monitoring Team, which is responsible for assisting two security council committees: the ISIL (Da'esh) & Al-Qaida Sanctions Committee and the 1988 Committee.[69] Aside from assisting various bodies within the organization with carrying out mandates, the Monitoring Team submits reports on sanctions and the changing nature of the ISIL, al-Nusrah Front, Boko Harem, Taliban, and Al Qaeda threats.[70] The Monitoring Team also works in information collection and collaboration with various UN branches, including UNODC and separately with the FATF. The current mandate of the Monitoring Team was extended in 2017 to continue until December 2021.[71]

The UNODC works at the nexus of terrorism and drug-related crime. Extensive research addresses the connected global network of illicit activities, reflecting the conclusions of the latest UNODC reports.[72] Using the various reports and findings, the UNODC has the capability to employ AML/CTF tactics to mitigate the networks of drug trafficking in an attempt to finance terrorism. Some of these tactics include freezing funds, travel bans, and arms embargos on various terrorist organizations, all included in relevant UNSC decisions and universal anti-terrorist instruments.[73] Understanding the intricacy of

66. *About UNCCT*, UNITED NATIONS OFF. COUNTER-TERRORISM, https://www.un.org/counterterrorism/ctitf/en/uncct/about [https://perma.cc/W92G-38Y6].

67. *UN Global Counter-Terrorism Strategy*, *supra* note 62.

68. *Id.*

69. *Security Council Committee Pursuant to Resolutions 1267 (1999) 1989 (2011) and 2253 (2015) Concerning ISIL (Da'esh) Al-Qaida and Associated Individuals Groups Undertakings and Entities (2017a)*, UNITED NATIONS SEC. COUNCIL, https://www.un.org/securitycouncil/sanctions/1267#work%20and%20mandate [httpe://perma.cc/M9TP-PLXW].

70. *Id.*

71. *Id.*

72. *See* CONVERGENCE, *supra* note 34; *see Drug Trafficking and the Financing of Terrorism*, UNITED NATIONS OFF. ON DRUGS & CRIME, http://www.unodc.org/unodc/en/frontpage/drug-trafficking-and-the-financing-of-terrorism.html [https://perma.cc/X7MM-TCQ4].

73. *Drug Trafficking and the Financing of Terrorism*, *supra* note 72.

these linked networks allows the UN to create effective countermeasures to disrupt these crimes.[74] Included in the UNODC is the Terrorism Prevention Branch (TPB), which specifically looks to counter-terrorist financing, ratify universal legal instruments to prevent CML, and create an international standard for CML.[75] In recent years, the TBP has been focused on new technologies for combatting terrorist financing.[76]

The CTED was established in 2004 under Resolution 1535 to "monitor, facilitate and promote Member States' implementation of resolution 1373 (2001) and subsequent resolutions and decisions of the Council" on all counter-terrorism related matters.[77] From 2008 to 2010, the organizational plan of the CTED intended to strengthen communication and coordination among member states in forging consistent counter-terrorist measures.[78] The CTED's mandate has been extended until the end of 2021, with the goal of "assist[ing] the work of the CTC and coordinat[ing] the process of monitoring the implementation of resolution 1373 (2001)."[79] The CTED accumulated detailed information about countries' counter-terrorist efforts, such as freezing assets, preventing terrorist groups from receiving aid, etc., and it frequently collaborates with the CTITF.[80] Its interventions are based on national and regional threats, as well as collaboration with a plethora of international, regional, and sub-regional organizations.[81] Developing a greater understanding of regional threats will help combat the asymmetric nature of global conflict.[82]

---

74. *Countering Terrorist Financing*, UNITED NATIONS OFF. ON DRUGS & CRIME, https://www.unodc.org/unodc/en/terrorism/news-and-events/terrorist-financing.html [https://perma.cc/JSV6-5E45].

75. *Id.*

76. *Id.*

77. *Frequently Asked Questions (FAQs)*, SEC. COUNCIL COUNTER-TERRORISM COMM., https://www.un.org/sc/ctc/about-us/frequently-asked-questions-faqs/ [https://perma.cc/Q4MG-QGPQ].

78. Briefing by CTED Exec. Dir. Mike Smith to UN Sec. Council (Mar. 19, 2008), https://www.un.org/sc/ctc/wp-content/uploads/2017/01/2008_03_19_cted_brief.pdf [https://perma.cc/6HDH-XVF3].

79. *About the Counter-Terrorism Committee*, SEC. COUNCIL COUNTER-TERRORISM COMM., https://www.un.org/sc/ctc/about-us/ [https://perma.cc/6FCT-C6L6].

80. Latif & Khan, *supra* note 65.

81. *See* ERIC ROSAND ET AL., THE UN GLOBAL COUNTER-TERRORISM STRATEGY AND REGIONAL AND SUBREGIONAL BODIES: STRENGTHENING A CRITICAL PARTNERSHIP (2008), http://www.globalcenter.org/wp-content/uploads/2008/10/strengthening_a_critical_partnership.pdf [https://perma.cc/XWY6-WFM4].

82. *See* ALISTAIR MILLAR & NAUREEN C. FINK, GETTING BACK TO BASICS?: RENEWING THE MANDATE OF THE UN SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE FOR 2014-2016 (2013), http://www.globalcenter.org/wp-content/uploads/2013/12/13Nov26_CTED-Policy-Brief_CGCC.pdf [https://perma.cc/NSB7-UXVU].

The new UN Counter-Terrorism Office is the most recent counter-terrorism measure by the UN. Under this new office, the CTITF, and subsequently the UNCCT, will be transferred from the Department of Political Affairs (DPA) to the UN Counter-Terrorism Office.[83] The new office will have five main functions: 1) "to provide leadership on General Assembly . . . mandates"; 2) to enhance coordination across the 38 CTITF entities to ensure a coherent strategy; 3) to assist member states in capacity building; 4) to "improve visibility, advocacy[,] and resource mobilization"; and 5) to ensure counter-terrorism measures are a priority across the UN systems, and that the prevention of extremism is rooted in the strategy.[84]

CTED's reporting on member states' implementation of Resolution 1373 shows the emerging risks that member states must combat, including new usage of Information Communication Technology (ICT) by terrorist organizations, the rise of foreign terrorist fighters, and women as perpetrators of terrorism. The report calls for member states to "ensure that any person who participates in the financing, planning, preparation[,] or perpetration of terrorist acts, or in supporting terrorist acts, is brought to justice," and asks member states to adopt specific methods within their domestic justice system to combat terrorism and terrorist financing.[85] For instance, terrorist financing is a criminal offense in Canada under the federal Criminal Code. As of January 2019, Canada had listed fifty-four terrorist entities under the Criminal Code and thirty-six terrorist entities under the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.[86] 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.[87]

---

83. *Counter Terrorism*, UNITED NATIONS OFF. COUNTER-TERRORISM, http://www.un.org/en/counterterrorism/ [https://perma.cc/N7FE-NNXF].

84. *General Assembly Approves Creation of New UN Counter-Terrorism Office*, U.N. NEWS (June 15, 2017), https://news.un.org/en/story/2017/06/559582-general-assembly-approves-creation-new-un-counter-terrorism-office [https://perma.cc/SA7F-UTV4].

85. UNITED NATIONS SEC. COUNCIL, COUNTER-TERRORISM COMM. EXEC. DIRECTORATE (CTED), GLOBAL SURVEY OF THE IMPLEMENTATION OF SECURITY COUNCIL RESOLUTION 1373 (2001) BY MEMBER STATES (2016), https://www.un.org/sc/ctc/blog/document/global-survey-of-the-implementation-of-security-council-resolution-1373-2001-by-member-states-2016/ [https://perma.cc/L9BU-EV3N].

86. Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism, SOR/2001-360 (Can.); *Currently Listed Entities*, PUB. SAFETY CAN., https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx [https://perma.cc/SA59-G8H6].

87. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

3. Financial Action Task Force (FATF)

FATF is an intergovernmental body that was originally established in 1989 to combat the global drug trade but evolved to combat money laundering and terrorist financing.[88] It has thirty-five member jurisdictions 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.[89] FATF does not formally possess enforcement power but makes recommendations for countering both transnational money laundering and terrorist financing.[90] These recommendations set out international standards to prevent terrorist financing and money laundering.[91]

Importantly, FATF Recommendation 6 focuses on proactively freezing funds used for terrorist purposes.[92] The International Best Practices report—evaluating the effects of Recommendation 6—highlights how vital sanctions are in addressing and combating terrorist financing. Essentially, Recommendation 6 acts as a prophylactic measure instead of a reactive tool, and it promotes the importance of effectively freezing funds. By adding a deterrent to terrorist financing, FATF hopes that individuals will be less likely to finance terror, and the individuals that are caught may lead to more financiers through the money trail. Moreover, terrorists are then forced to use more costly

88. *See Who We Are*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/about/ [https://perma.cc/P72U-FYDG]; *see also* FIN. ACTION TASK FORCE, 25 YEARS AND BEYOND: THE FINANCIAL ACTION TASK FORCE SETTING THE STANDARDS TO COMBAT MONEY LAUNDERING AND THE FINANCING OF TERRORISM AND PROLIFERATION 1 (2014), http://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF%2025%20years.pdf [https://perma.cc/5VNM-W2N4]; Gardner, *supra* note 21, at 326.

89. *FATF Members and Observers*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/trash/aboutfatf/membersobservers/fatfmembersandobservers.html [https://perma.cc/Z7F8-453A].

90. *See* Gardner, *supra* note 21, at 342.

91. 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. *Id.* at 6-7.

92. *Id.* at 39.

and obscure methods of fund transfer, making the individuals or organization more susceptible to detection.[93]

Many countries have amended their domestic AML/CTF laws on terrorist financing pursuant to FATF recommendations.[94] Moreover, FATF engages in peer review, creating reports that identify areas of noncompliance with FATF recommendations. For instance, peer reviews from the United States and Canada note that both countries lack laws that identify the beneficial owners of business and legal entities.[95] In other words and as subsequently discussed, these countries have corporate laws that allow the real, human owners of business entities such as corporations to hide their identities.[96] Kathryn Gardner suggests that it is important to continue with FATF's international collective action and make it as adaptable as possible.[97] There may be evidence to suggest success in many of FATF's geostrategic locations, such as the Middle East and North Africa (MENA).[98] The expansion into the MENA region in 2004 was thought necessary, as terrorism transcends national boundaries.[99]

4. Financial Intelligence Units

Governments that pursue global cooperation generally adopt measures advocated by the UN or FATF by implementing them under domestic law. In the United States and many other countries, a complex legal environment governs offshore tax evasion, international money laundering, and financing of global terrorism. U.S. federal stat-

93. FIN. ACTION TASK FORCE, INTERNATIONAL BEST PRACTICES: TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING (RECOMMENDATION 6) 1, 4 (2013), www.fatf-gafi.org/media/fatf/documents/recommendations/BPP-Fin-Sanctions-TF-R6.pdf [https://perma.cc/23QR-TT42].

94. *Topic: High-Risk and Other Monitored Jurisdictions*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate) [https://perma.cc/BLS2-MUW6].

95. *See* Jenik Radon & Mahima Achuthan, *Beneficial Ownership Disclosure: The Cure for the Panama Papers Ills*, COL. J. INT'L AFF. (Sept. 22, 2017), https://jia.sipa.columbia.edu/beneficial-ownership-disclosure-%C2%A0cure%C2%A0-panama-papers-ills%C2%A0 [https://perma.cc/5HRP-RU68]; *see also* Client Memorandum from David Mortlock et al., Wilkie Farr & Gallagher LLP, FinCEN Issues Long-Anticipated Requirements for AML Due Diligence on Beneficial Owners (May 24, 2016), https://www.willkie.com/~/media/Files/Publications/2016/05/FinCEN_Issues_Long_Anticipated_Requirements_for_AML_Due_Diligence.pdf.

96. *See infra* discussion accompanying footnotes 149 & 150.

97. *See* Gardner, *supra* note 21, at 342.

98. *Overview*, MENAFATF, http://www.menafatf.org/about [https://perma.cc/R3JA-BXER].

99. Gardner, *supra* note 21, at 340.

utes include the Internal Revenue Code, the Money Laundering Control Act, the Bank Secrecy Act, and the USA Patriot Act.[100] FIUs administer and, in some countries, are also mandated to enforce these laws. The Financial Crimes Enforcement Network (FinCEN) is the U.S. FIU under the Department of the Treasury that combats money laundering and terrorist financing by overseeing and disseminating financial data to enforcement agencies.[101] Based on anti-money laundering standards developed by the FATF, FinCEN recommended new regulations whereby U.S. financial institutions will need to identify, on a current basis, the ultimate (or beneficial) owners of corporations and accounts, whether or not there is any suspicion of a crime.[102]

FinCEN also uses reports from the Department of Commerce—through the Bank Secrecy Act—to track unusual transactions and to delegate extreme cases to relevant authorities to investigate.[103] This model is known as the money laundering and terrorist financing

100. 18 U.S.C. § 1956 (2012); 31 U.S.C. § 5311 (2012); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272; JOHN MADINGER, MONEY LAUNDERING: A GUIDE FOR CRIMINAL INVESTIGATORS 24-26, 28, 30-33, 35-42, 44-45, 52, 57, 62 (3d ed. 2012) (reviewing relevant laws and regulations).

101. *What we do*, FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/what-we-do [https://perma.cc/TYV4-8UWQ]. 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 Bank Secrecy Act in 1970, which enabled banks to "create audit trails of large bank transactions and to allow law enforcement access to such information." *See* Clunan, *supra* note 47, at 585; Matthew Levitt & Michael Jacobson, *The Money Trail: Finding, Following, and Freezing Terrorist Finances*, 89 WASH. INST. FOR NEAR EAST POL'Y 1, 18 (2018), https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus89.pdf [https://perma.cc/66QY-6FVN]; Eric J. Gouvin, *Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism*, 55 BAYLOR L. REV. 955, 969 (2003) (noting that originating from a joint proposal in 1998 from U.S. 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). In contrast, Cassara testified that suspicious activity reports (SARs) are consistently unsuccessful in detecting terrorist activity. SARs fail at detecting small amounts of illicit behavior, and of the millions filed, many are not acted upon. *Terrorist Financing Since 9/11: Assessing an Evolving Al-Qaeda and State Sponsors of Terrorism: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the H. Comm. On Homeland Sec.* 9-11 (2012) (statement of John A. Cassara, Private Citizen).

102. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45151 (Aug. 4, 2014) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 2024, 1026). These reforms have been promoted under the view that more regulation is needed to curtail apparent abuses, such as the UBS Swiss Bank scandal. *See* discussion *infra* Part III.A. The United States and other members of the Egmont Group of Countries have agreed to implement FATF reforms as a way to coordinate international efforts. For critique, see Richard Gordon & Andrew P. Morriss, *Moving Money: International Financial Flows, Taxes, and Money Laundering*, 37 HASTINGS INT'L & COMP. L. REV. 1, 3-4 (2014).

103. Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. § 5311 (2012) (commonly referred to as the Bank Secrecy Act (BSA)).

(ML/TF) approach.[104] FinCEN investigates how money laundering groups place, layer, and integrate money through various transactions. 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.[105] FinCEN disseminates intelligence information from financial institutions, and in less common cases the Commerce Department, to law enforcement agencies who can then inspect the inquiry.[106] Identifying suspicious activity is a key feature in blocking terrorist financing and money laundering.

Other countries also deploy their own FIUs, often with subtle differences in mandate and enforcement authority. 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."[107] Akin to FinCEN, FINTRAC is responsible for collecting financial intelligence in order to uphold the integrity of financial networks in Canada, thereby acting as a vehicle to transmit financial intelligence to relevant law enforcement agencies to penalize illegitimate financial practices.[108] Similar to FinCEN, FINTRAC employs the ML/TF model.[109]

Unlike FinCEN, FINTRAC does not have any powers to investigate; rather, it can only report information to partners such as the

---

104. *See* O'Hallaran et al., *Terrorist Resourcing Model*, *supra* note 12.

105. *See* Andrew Kurzrok & Gretchen Hund, *Stopping Illicit Procurement: Lessons from Global Finance*, ARMS CONTROL ASSOC., https://www.armscontrol.org/act/2014_06/Features/Stopping-Illicit-Procurement-Lessons-From-Global-Finance [https://perma.cc/KW4B-9NPB].

106. *FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing*, FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing [https://perma.cc/H3W7-TJKG].

107. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, FIN. TRANSACTIONS & REPS. ANALYSIS CTR. CAN., http://www.fintrac-canafe.gc.ca/act-loi/1-eng.asp [https://perma.cc/NK7C-EDZ8].

108. *See Financial Transactions and Reports Analysis Centre of Canada*, GOV. CAN., https://www.canada.ca/en/financial-transactions-reports-analysis.html [https://perma.cc/XZ4U-ZESH].

109. *See* FIN. TRANSACTIONS AND REPORT ANALYSIS CTR. OF CAN., MONEY LAUNDERING AND TERRORIST FINANCING (ML/TF) TYPOLOGIES AND TRENDS FOR CANADIAN MONEY SERVICES BUSINESSES (MSBS) (2010), https://www.justice.gov.il/Units/HalbantHon/docs/cana.pdf [https://perma.cc/9FR9-L6Q3].

RCMP.[110] Moreover, FINTRAC is only empowered to collect Suspicious Transaction Reports (STRs), which arguably have a narrower ambit compared to Suspicious Activity Reports (SARs) collected by FinCEN (because STRs are normally only triggered by a suspicious transaction, such as a deposit of $10,000 in cash, whereas a SAR can focus exclusively on a suspicious activity, such as a shady character checking her bank account, even though no transaction has been conducted).[111]

B. Limits of Collective Action

1. Non-Compliant States

States' intergovernmental role is imperative to prevent and deter terrorist financing. States are divided into two categories: compliant states and noncompliant states.[112] Compliant states are members of internationally recognized organizations and implement appropriate measures to counter terrorist financing. In contrast, noncompliant states are not members of an internationally recognized organization.[113] These states are likely to have terrorist organizations' financial intermediaries operating within their borders.[114]

Similarly, states that are considered a target of terrorism or a base for terrorist activity experience more transactions intended for the commission of terrorist acts.[115] For example, Iran is a noncompliant state and known for financially supporting the UN-designated terrorist organization, Hezbollah.[116] 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.[117] Iran spends an estimated US$200 million annually on

110. *See Money Laundering*, ROYAL CAN. MOUNTED POLICE, http://www.rcmp-grc.gc.ca/poc-pdc/launder-blanchim-eng.htm [https://perma.cc/435V-JFSN].

111. Under FINTRAC's broadened definition of an STR, however, it seems to capture suspicious activities in some circumstances. For instance, a transaction includes an "attempted transaction" for terrorist financing purposes. *See What Is a Suspicious Transaction Report?*, FIN. TRANSACTIONS & REP. ANALYSIS CTR. OF CAN., http://www.fintrac.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp#s3 [https://perma.cc/5SJS-YBWW]; *see also id.* (listing examples of Common Indicators).

112. *See* Jakobi, *supra* note 47; *Topic: High-Risk and Other Monitored Jurisdictions*, *supra* note 94.

113. Rainer Hülsse & Dieter Kerwer, *Global Standards in Action: Insights from Anti-Money Laundering Regulation*, 14 ORGANIZATION 625 (2007).

114. *Topic: High-Risk and Other Monitored Jurisdictions*, *supra* note 94.

115. *See* Christian Leuprecht & Arthur Cockfield, Global Financial Networks and Anti-Terrorist Financing Laws 17 (2018) (unpublished manuscript) (on file with authors).

116. *See id.*

117. *See* Levitt & Jacobson, *supra* note 61, at 76.

funding terrorist organizations, such as Hezbollah and Hamas.[118] Syria is also on the international radar for extensive state-sponsored terrorism, providing weapons and a safe haven for Hezbollah. The country largely operates on a cash economy that is not integrated with, or reliant on, the international monetary system.[119] Some noncompliant states, such as Iran, have been subject to sanctions.[120]

Furthermore, under the 1994 UN General Assembly Seminal Declaration on Measures to Eliminate International Terrorism, states are prohibited from financing terrorism.[121] 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.[122] Miklaucic and Brewer suggest that international cooperation is critical to defeat illicit networks and operations arising from noncompliant states.[123] 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.[124] These fixers rely on shadow facilitators who operate in the international realm to move resources to organizations or through states.[125] In this study, fixers translate to "investors" and shadow facilitators as "financial intermediaries." These reoccurring nodes show how important it is for states to cooperate to identify criminal supply chains and networks to make law enforcement agencies more effective in countering terrorist financing.[126]

Terrorism is also linked to organized crime.[127] For example, narcoterrorism is encouraged by states' failure to prevent illegal activities, contributing to terrorist financing.[128] In many cases, terrorist and criminal financing activity are indistinguishable from one another. Due to the interconnectedness of globalization, cartels and terrorist

---

118. *See id.*

119. *See id.*

120. *See id.*

121. *See* Bantekas, *supra* note 28, at 316.

122. G.A. Res. 49/60, Measures to Eliminate International Terrorism (Dec. 9, 1994), http://www.un.org/documents/ga/res/49/a49r060.htm [https://perma.cc/8DFZ-C3TZ].

123. *See* CONVERGENCE, *supra* note 34.

124. *Id.*

125. *Id.*

126. *See* BEYOND CONVERGENCE: WORLD WITHOUT ORDER (Hilary Matfess & Michael Miklaucic eds., 2016); *see also* CONVERGENCE, *supra* note 34.

127. GLENN E. CURTIS & TARA KARACAN, FED. RESEARCH DIV., LIBRARY OF CONG., THE NEXUS AMONG TERRORISTS, NARCOTICS TRAFFICKERS, WEAPONS PROLIFERATORS, AND ORGANIZED CRIME NETWORKS IN WESTERN EUROPE 1-4 (2002), http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf [https://perma.cc/K7WY-KPBM].

128. *See* Celina B. Realuyo, *The Terror-Crime Nexus: Hezbollah's Global Facilitators*, 5 PRISM 117 (2014).

groups thrive on cooperation, transcending international borders to fulfill criminal needs.[129] Aside from illicit drug smuggling, cigarette smuggling also earns a significant portion of revenue for terrorist groups.[130] It is difficult to distinguish between terrorist and criminal financing when narcotics or cigarettes are transported and sold illegally.[131] It is also difficult for states to track terrorist groups when they use legal means to fund their organization. When groups launder through legitimate businesses, this deceives the protocol in place for detecting terrorist activity.[132] Challenges for the state in combating terrorist financing include: knowledge about the terrorist organization, denying the terrorist organization assets, and executing robust state compliance.[133] State knowledge about organizational networks is critical to implement any freezes or barriers to the terrorists' funds.[134] In some instances, states do not intentionally fail to comply but lack the institutional capacity to implement best practices.[135]

Finally, certain countries, normally called "tax havens," can, at times, facilitate global crimes, such as offshore tax evasion, international money laundering, and potentially terrorist financing.[136] Tax havens are countries that impose little or no income taxes on cross-border transactions and provide tax benefits of which multinational firms take advantage through legal tax planning.[137] While there is now significant literature in law, politics, economics, and other disciplines that examine tax havens and offshore tax evasion, there is little information on what tax haven intermediaries—offshore service providers such as finance and trust companies—*actually do* to facilitate offshore evasion.[138]

---

129. *See* CONVERGENCE, *supra* note 34, at ix.

130. *See* LOUISE I. SHELLEY, DIRTY ENTANGLEMENTS: CORRUPTION, CRIME, AND TERRORISM (2014); Bantekas, *supra* note 28, at 319.

131. *See* Freeman, *supra* note 22; Leuprecht et al., *supra* note 13.

132. *See* Matthew Levitt, *U.S.-Designated Hamas Front Gets Symbolic Win in France*, WASH. INST. (Mar. 20, 2007), http://www.washingtoninstitute.org/policy-analysis/view/u.s.-designated-hamas-front-gets-symbolic-win-in-france [https://perma.cc/57QQ-2DX7].

133. *See* Leuprecht & Cockfield, *supra* note 115.

134. *See* Steve Barber, *The "New Economy of Terror": The Financing of Islamist Terrorism*, 2 GLOBAL SECURITY STUD. 1, 4 (2011), http://globalsecuritystudies.com/Barber.pdf [https://perma.cc/UG2H-9RRZ].

135. *See* Clunan, *supra* note 47, at 572.

136. Cockfield, *Big Data*, *supra* note 32, 488-93.

137. *Id.* at 489-90.

138. For other efforts to assess financial dealings within tax havens, see, e.g., *Tax Haven Abuses: The Enablers, the Tools and Secrecy: Hearing Before the Permanent Subcomm. on Investigations of the Comm. on Homeland Sec. and Gov't Affairs*, 109th Cong. 161 (2006); Dmitry Gololobov, *The Yukos Money Laundering Case: A Never-Ending Story*, 28 MICH. J. INT'L L. 711 (2007); Jeffery Simser, *Tax Evasion and Avoidance Typologies*, 11 J. MONEY LAUNDERING CONTROL 123 (2008); Douglas J. Workman, *The Use*

The gap in the literature can be largely explained by the secretive nature of tax haven activities that shields them from outside scrutiny. This environment changed as a result of a series of tax haven data leaks, including the 2016 Panama Papers leak.[139] For example, the first major financial data leak of over 2.5 million papers revealed that offshore service providers were often not complying with international "know your customer" standards,[140] which creates information problems that make it difficult for law enforcement authorities to enforce tax and criminal laws governing offshore tax evasion and other global financial crime. In other words, businesses within tax havens—often in cooperation with tax haven governments—actively subvert efforts to promote global fiscal transparency. While tax havens often serve as conduits for global financial activities, open-source evidence did not reveal any instances where they were used to finance terrorism.[141]

2. Non-Compliance with Know Your Customer Rules

FIUs track financial information collated by banks and other financial intermediaries. The "know your customer" (KYC) principle is the main international approach to enlist these intermediaries to combat money laundering and terrorist financing. Under this principle, the 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.[142] Countries such as Canada and the United Sates focus on these financial intermediaries to detect and prevent terrorist financing. For instance, through the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, Canada extends its enforcement over approximately

---

of Offshore Tax Havens for the Purpose of Criminally Evading Income Taxes, 73 J. CRIM. L. & CRIMINOLOGY 675 (1982).

139. *See* Shu-Yi Oei & Diane Ring, *Leak-Driven Law*, 65 UCLA L. Rev. 532 (2018) (discussing various tax haven data leaks); Gerard Ryle et al., *Secret Files Expose Offshore's Global Impact*, INT'L CONSORTIUM INVESTIGATIVE JOURNALISTS (Apr. 2, 2013), https://www.icij.org/investigations/offshore/secret-files-expose-offshores-global-impact/ [https://perma.cc/3U8V-HZLL].

140. For instance, employees of offshore service providers at times tried to identify the source of deposited funds and questioned sources with superiors, but there was often either no follow-up or ongoing delays by depositors for periods that potentially could go on for decades. *See* Cockfield, *Big Data*, *supra* note 32, at 485-86.

141. *See* discussion *infra* Part VI.

142. *See* John Hunt, *The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments are Trying to Stop Them*, 20 INFO. & COMM. TECH. L. 133, 138 (2011).

31,000 reporting entities, including money services businesses, casinos, life insurance, and banks.[143] These reporting entities include financial institutions and designated nonfinancial institutions and professions. Still, their remit only covers a minority of global financial transactions. A majority of transactions eludes FIUs; they flow through informal mechanisms such as the *hawala* system.

FATF embraces the KYC principle, and it forms one of its most important recommendations to track and inhibit terrorist financing.[144] 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, make gathered information available to central financial institutions, and eliminate anonymous accounts.[145] The international goal is to identify trends in the money laundering market and to create a robust framework to counter money laundering. Different countries have adopted approaches that differ in some cases. As mentioned, in the United States banks must track SARs, whereas Canadian banks must file STRs, which give them a slightly narrower reporting ambit.[146] Under the KYC principle, banks and other financial institutions are supposed to report to their national FIUs, SARs, STRs, and other information.

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.[147] For FATF to be successful in counter-terrorist financing efforts, its focus needs to shift to the way terrorist groups adapt their financial operations.

FATF seeks compliance with KYC standards in part by "blacklisting" uncooperative countries.[148] Recently, FATF recommended that countries adopt AML/CTF laws that allow financial institutions to identify individuals who are the ultimate (or beneficial) owners of

---

143. DEPT. OF FIN. CAN., REVIEWING CANADA'S MONEY LAUNDERING AND ANTI-TERRORIST FINANCING REGIME (2018), https://www.fin.gc.ca/activty/consult/amlatfr-rpcfa-eng.pdf [https://perma.cc/36A3-CCWW].

144. *See* Kevin D. Stringer, *Tackling Threat Finance: A Labor for Hercules or Sisyphus?*, 41 PARAMETERS 101, 110 (2011).

145. *See* Hall, *supra* note 44, at 22.

146. *See supra* discussion in the text accompanying footnote 111; *see also* Richard Gordon, *Terrorism Financing Indicators for Financial Institutions in the United States*, 44 CASE W. RES. J. INT'L L. 765, 766 (2012).

147. *See* Leuprecht et al., *supra* note 13.

148. *See* Mark T. Nance, *The Regime That FATF Built: An Introduction to the Financial Action Task Force*, 69 CRIME L. & SOC. CHANGE 109, 116 (2018).

corporations and accounts, irrespective of any suspicion of a crime. At present, Canadian federal and provincial corporate laws, as well as U.S. state corporate 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 (for example, a corporation or a limited liability company).[149] 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.[150] As shareholders are never registered on a share registry, bearer shares allow for anonymous ownership. Canada and the United States, therefore, fail to comply with recent FATF reforms.

As a result of similar concerns, some observers question the effectiveness of collective action and maintain that international efforts to combat terrorist resourcing during the post-September 11th era was largely superficial.[151] Domestic bureaucratic interests may also undermine the effectiveness of international cooperation and information sharing with foreign institutions.[152]

3. Assimilating Technology

In addition to ever-evolving terrorist networks, technology developments also present challenges to law enforcement.[153] Recent global financial crimes were aided by quasi-anonymous forms of digital cash over the Internet.[154] The current, most popular cryptocurrency—a form of digital cash generated by the application of cryptography—is Bitcoin.[155] Presumably, cryptocurrencies are mainly used for legal purposes, but their illegal use is reportedly on the rise.[156] 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.

---

149. *See* Arthur J. Cockfield, *Examining Canadian Offshore Tax Evasion*, 65 CAN. TAX. J. 651 (2017).

150. *Id.*

151. *See* Clunan, *supra* note 47, at 579.

152. *See id.* at 589; *see also* William Vlcek, *A Leviathan Rejuvenated: Surveillance, Money Laundering, and the War on Terror*, 20 INT'L J. POL. CULTURE & SOC'Y 21, 23 (2008).

153. *See* Cockfield, *Big Data*, *supra* note 32, at 524.

154. *See* Joshua Bearman, *Silk Road: The Untold Story*, WIRED (May 23, 2015, 6:00 AM), https://www.wired.com/2015/05/silk-road-untold-story/ [https://perma.cc/CN5B-6U44].

155. *See* Sarah Gruber, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*, 32 QUINNIPIAC L. REV. 135, 141 (2013).

156. *See* Lev Grossman & Jay Newton-Small, *The Secret Web: Where Drugs, Porn and Murder Live Online*, TIME (Nov. 11, 2013), http://content.time.com/time/magazine/article/0,9171,2156271-6,00.html [https://perma.cc/MED6-ZLLA].

Cryptocurrencies help anonymize cross-border financial dealings and can potentially facilitate terrorist financing. Anonymity is promoted because cryptocurrencies are not backed by any financial institution or government, and there is no central control; it is not clear how governments will be able to monitor, track usage, and identify the relevant taxpayer. Moreover, cryptocurrencies are used for criminal purposes on a part of the Internet sometimes referred to as the "Dark Web"—websites accessed via an anonymizing network that decouples both ends of transactions, including financial dealings.[157] While there does not appear to be any evidence of terrorist financing via cryptocurrencies in either tax haven data leaks or our open-source cases, to the extent that terrorist financiers become more technologically sophisticated they are likely to assimilate these developments to achieve their goals.

IV. CASE LAW AND STUDY METHODOLOGY

Data from the thirty-two court cases, listed in Appendix A, 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: 1) by exploring primary sources (legislation) and secondary sources (scholarly journals and government documents); and 2) by searching electronic online legal databases, including Westlaw, LexisNexis-Quick Law, CanLII, and EUR-Lex—access to European Union law.[158] The study relies on legislation, scholarly journals, and government documents to explore the essential vocabulary on terrorist financing and to identity case names and citations. In the process, we compiled a list of the *terms* and *categories* to narrow our focus.[159]

---

157. *See id.*

158. 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 Westlaw using different connectors. Both databases provide a list of connectors to search within cases.

159. 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 Westlaw are effective search tools to explore domestic cases, while QuickLaw is better equipped 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 to directives by the European Parliament to explore data

The list of *terms* includes "charity," "finance," "donation," "funds," "alms," "money laundering," "transaction," "informal transfer," etc. The list of *categories* includes "online," "social media," "*hawala*," "bank," "money transfer business," etc. The *terms* and *categories* narrowed our focus to track international, transnational, and cross-border transactions of monetary and other formal and informal financial proceeds used to resource terrorist financing. These criteria also set the scope conditions 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 the circulation of currency for the purpose of terrorism. Cases included jurisdictions in North America and Europe.

The approach in this study draws on the Terrorist Resourcing Model (TRM), which is a tool used by social scientists to analyze data concerning the contribution of resources to terrorists.[160] Here, data is drawn from published cases that involve terrorist financing, and then it is coded and analyzed via software. The TRM's focus on resources is more comprehensive than that of the ML/TF model conventionally used by FIUs.[161] The TRM incorporates all assets that are deemed resources, including modes of financial transactions, trade-based fraud, and online social media.[162] As a result, the TRM is thought to generate 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 the TRM.

The TRM distinguishes between two types of terrorist resources: resources raised and resources transferred.[163] First, resources raised refers to individuals who intend to send cash or goods to a terrorist organization but are apprehended before the transfer is complete.[164] Second, resources transferred refers to the successful transfer of funds from a financial intermediary to a terrorist organization.[165] The patterns that emerge suggest that terrorist organizations adopt a fairly uniform approach to fund themselves through transnational networks. While these cases differ in terms of the amount of money and transfer

---

that help us understand how terrorist funds are channelled through a wide range of financial sectors.

160. *See* O'Halloran et al., *Terrorist Resourcing Model*, *supra* note 12, at 35. The TRM has five stages: acquisition of resources, aggregation of resources, transmission to a terrorist organization, transmission to a terrorist cell, and conversion. *Id.*

161. *See id.* at 34.

162. *See id.* at 58-59.

163. *See id.* at 35.

164. *Id.*

165. *Id.*

of resources, it appears that the investors and their financial intermediaries use relatively similar networks to transport resources to terrorist organizations.

The primary data includes more than twenty-six independent variables to map terrorist resourcing networks.[166] 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 that are listed and described in the coding manual.

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 enabled terrorist attacks. Similarly, we list organizations, along with any terrorist affiliates, that received 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 "[a]cquisition of free or stolen funds and exchange and end-use goods," the role of someone defined as the "investor."[167] Many "investors" in the cases raised monetary funds with the intent to fund a terrorist organization. However, only a few cases manifest resourcing rather than financing. *United States v. Mehdi*[168] involved the movement of over 2,000 PlayStation 2 game consoles along with US$200,000, while *United States v. Sriskandarajah* involved a submarine, warfare technology, and weapons being accumulated with the intent to transfer them to a terrorist organization.[169] Across all cases in this study, the most common form of raising resources for terrorist organizations was to collect cash.

---

166. *See infra* Appendix 1.

167. *See* O'Halloran et al., *Terrorist Resourcing Model*, *supra* note 12, at 35 (emphasis omitted).

168. Indictment, United States v. Mehdi, No. 1:09-cr-20852-ASG (S.D. Fla. Feb. 24, 2010), ECF No. 3.

169. United States v. Sriskandarajah [2012] 3 S.C.R. 609 (Can.).

The research also 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 named the defendant as the charity or the bank that provided services to the charity as investors who raised donations to send to financial intermediaries who would then send the money to terrorist organizations. This is in line with the literature on charities and terrorist fundraising, and it is indicative of the broader problem associated with terrorist resourcing: the difficulty parsing whether funding is being used for legitimate or terrorist purposes. Some charities may have a wholesome purpose but nevertheless divert some funding to terrorist groups.[170]

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 pooling resources, either in select financial institutions (for money) or select locales (for goods).[171] Although tax havens per se do not figure in the data, techniques commonly associated with tax evasion were used, such as using multiple banks to store funds either through individuals or organizational cells. Many of the cells were mission-specific, actively transferring funds through international financial networks.[172]

Many banks were also used to move funds from a financial intermediary to a terrorist-organization client. Some were even used frequently to store funds, including the use of sleeper accounts.[173] In one case, the National Westminster Bank in the United Kingdom was an account holder for the Palestinian Relief and Development Fund—a British-based charity providing funds to Hamas.[174] Arab Bank PLC was the defendant in two separate cases accused of providing banking services to organizations that directly financed Hamas.[175] The former contrasts with *International Relief Fund for the Afflicted and Needy (Canada) v. Canadian Imperial Bank of*

170. *See* Levitt, *supra* note 132.

171. *See* O'Halloran et al., *Terrorist Resourcing Model*, *supra* note 12, at 35.

172. *See* Bantekas, *supra* note 28, at 320.

173. *See id.* at 319.

174. Weiss v. Nat'l Westminster Bank PLC, 936 F. Supp. 2d 100, 104 (E.D.N.Y. 2013), *vacated*, 768 F.3d 202 (2d Cir. 2014).

175. Linde v. Arab Bank, PLC, 269 F.R.D. 186, 192, 201, 205 (E.D.N.Y. 2010); Almog v. Arab Bank, PLC, 471 F. Supp. 2d 257, 261 (E.D.N.Y. 2007).

Commerce where the charity (IRFAN) felt their account was wrongfully terminated by the bank (CIBC).[176] The case notes that IRFAN's charity registration was cancelled after being audited twice by the Canada Revenue Agency (CRA), supplemented by evidence from an investigation tying IRFAN to funding Hamas. CIBC then immediately terminated its services to avoid providing financial services to a known terrorist financing organization.[177]

In *United States v. Mehdi*, the defendant transported over 2,000 PlayStations to a subsidiary of a mall that was formally owned and operated by Hezbollah.[178] This case shows how terrorist resourcing transports value and aggregates resources in subsequent ways—such as through the shopping center Galeria Page located in Paraguay—in a way that would otherwise elude strict conventional understandings of terrorist financing.[179] Cases involving the legal transport of funds through a financial institution shows how illicit activity can be disguised as seemingly legal, as well as how illicit exports can be falsely legitimized through fraudulent documentation and appear as a perfectly legitimate export.

C. Stage 3 of the TRM: Movement of Resources

Stage 3 of the TRM is the "[t]ransmission [of resources] to a terrorist organization."[180] It comprises the largest part of the research conducted, describing the flow from a financial intermediary, transferring funds to the terrorist organization, tracking how funds were transferred, and what processes were used to transfer funds. The financial intermediary is the entity that initiates the transfer of funds. The financial intermediary may also be the investor if they also raised funds, but it generally holds a transactional position.

The financial intermediary can also be an organization in a country where resources are not planned to be used within that country, as in *Kaplan v. Central Bank of the Islamic Republic of Iran*.[181] In this case,

176. Int'l Relief Fund for the Afflicted and Needy (Can.) v. Can. Imperial Bank of Commerce, [2013] ONSC 4612. *See also* Int'l Relief Fund for the Afflicted and Needy (Can.) v. Minister of Nat'l Revenue, [2013] FCA 178 (discussing the decision by Canadian tax authorities to cancel the charitable status of the organization).

177. *Id.*

178. Factual Proffer at 1-2, United States v. Mehdi, No. 1:09-cr-20852-ASG-1 (S.D. Fla. Aug. 20, 2014); MATTHEW LEVITT, HEZBOLLAH: THE GLOBAL FOOTPRINT OF LEBANON'S PARTY OF GOD 48 (2015).

179. Factual Proffer, *supra* note 178, at 1.

180. *See* O'Halloran et al., *Terrorist Resourcing Model*, *supra* note 12, at 35 (emphasis omitted).

181. Kaplan v. Cent. Bank of the Islamic Republic of Iran, 961 F. Supp. 2d 185 (D.D.C. 2013), *aff'd in part*, *vacated in part*, 896 F.3d 501 (D.C. Cir. 2018).

Bank Saderat acted as the financial intermediary transferring funds from London to Beirut to support Hezbollah.[182] Bank Saderat had formally been designated by the U.S. Treasury Department under EO 12334 for previously facilitating the delivery funds to Hamas, PLO, and Hezbollah.[183] 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 to do through court cases because only facts relevant to the case are included in the reports, and the full causal mechanism is not necessarily described. Stage 4 seeks to fill in the network links by looking at their "[t]ransmission to a terrorist or operational cell."[184] Many of the cases merely indicate financial transfers in the formal documents, secondary research highlights that funds are not the only asset that reaches a terrorist organization. In one specific case, Mohammad Salman Farooq Qureshi lied to the FBI about his involvement with the NGO "Help Africa People" and his affiliation with Al-Qaeda.[185] Named as the main financial intermediary, Qureshi funneled US$30,000 to an Al-Qaeda affiliate.[186]

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

Finally, Stage 5 of the TRM is "conversion" and entails " 'exchanging funds or goods for end-use goods. For example, money may be used to buy a vehicle'. Conversion also includes the exchange of funds or goods for services."[187] This stage hence tries to identify the purpose of the resources. Many of the cases are brought by the kin 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 v. Arab Bank*, over 1,600 plaintiffs brought an action against Arab Bank for providing financial services

---

182. *Id.* at 190.

183. *See* Press Release, U.S. Dep't of the Treasury, Fact Sheet: Treasury Strengthens Preventive Measures Against Iranp1258 (November 6, 2008), https://www.treasury.gov/press-center/press-releases/Pages/hp1258.aspx [https://perma.cc/RER4-BYL4].

184. *See* O'Halloran et al., *Terrorist Resourcing Model*, *supra* note 12, at 35 (emphasis omitted).

185. INTRODUCTION TO THE NATIONAL SECURITY DIVISION'S CHART OF PUBLIC/UNSEALED INTERNATIONAL TERRORISM AND TERRORISM-RELATED CONVICTIONS FROM 9/11/01 TO 12/31/16, Feb. 10, 2017, at 7, http://www.humanrightsfirst.org/sites/default/files/NSD-Terrorism-Related-Convictions.pdf [https://perma.cc/KZ67-SR86].

186. *Id. See also* Bill of Information, United States v. Qureshi, 6:04-cr-60057-RFD-CMH (W.D. La. Oct. 13, 2004).

187. *See* O'Halloran et al., *Terrorist Resourcing Model*, *supra* note 12, at 35.

that ultimately led to suicide bombings in Israel.[188] The suit alleged that the bank provided financial services to organizations that were designated as terrorists by the U.S. government, resulting in the death of innocent civilians.[189] In other words, the purpose of gathering the resources was allegedly to generate violence for political purposes.

V. OBSERVATIONS

This Part first provides an overview of the TRM analysis by focusing on three case studies before providing more general observations concerning the patterns detected.

A. Case Studies of Terrorist Financing

To illustrate how we approached the TRM analysis, this Section discusses three coded cases that reveal the number of financial intermediaries, countries, transactions, funding and 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 v. HSBC Holdings PLC is a relatively complex case in our study, as it encompasses three terrorist organizations that raised US$881,000,000.[190] The case involves five of Mexico's most powerful drug cartels: the Sinaloa, Juarez, Gulf, Los Zetas, and Norte del Valle.[191] Families of four victims sued HSBC for reckless banking operations.[192] The defendants (HSBC and affiliates) reportedly accepted large amounts of money from individuals with no identifiable source of income.[193] The money was taken to the banks in custom-made boxes

188. Almog v. Arab Bank, PLC, 471 F. Supp. 2d 257, 259-60 (E.D.N.Y. 2007).

189. *Id.*

190. Complaint ¶ 144, Zapata v. HSBC Holdings plc, No. 1:16-cv-00030 (S.D. Tex. filed Feb. 9, 2016).

191. Zapata v. HSBC Holdings PLC, Civil Action No. 1:16-cv-30, 2017 WL 6939209, at *1 (S.D. Tex. 2017).

192. *Id.* The plaintiffs in this case are Mary M. Zapata (Individually and as Administrator of the Estate of Jaime J. Zapata); Amador Zapata, Jr.; Amador Zapata III (Individually and as Administrator of the Estate of Jaime J. Zapata); Carlos Zapata; Jose Zapata; E. William Zapata; Victor Avila, Jr. (Individually and as Guardian for S.A. and V.E.A.); Claudia Avila (Individually and as Guardian for S.A. and V.E.A.); Victor Avila; Magdalena Avila; Magdalena Avila Villalobos; Jannette Quintana; Mathilde Cason (Individually and as Administrator of the Estate of Arthur and Lesley Redelfs, and as Guardian for R.R.); Robert Cason; Reuben Redelfs; Paul Redelfs; Katrina Redelfs Johnson; Beatrice Redelfs Duran; Rafael Morales (Individually and as Administrator of the Estate of Rafael Morales Valencia); Maria Morales; Moraima Morales Cruz (Individually and as Guardian for G.C., A.C., and N.C.); and Juan Cruz.

193. Complaint, *supra* note 190, ¶ 147. The defendants are HSBC Holdings plc; HSBC Bank U.S.A., N.A.; HSBC México S.A., Institución de Banca Múltiple, Grupo Financiero HSBC; and Grupo Financiero HSBC, S.A. de C.V.

that fit the precise dimensions of the teller windows.[194] The case highlights that HSBC admitted and accepted criminal liability for laundering US$881 million of the drug cartel's proceeds.[195]

Funds came from a variety of sources: in Mexico, the cartels account for US$18 billion and US$29 billion in cash smuggled from the United States to Mexico for drug sales, with additional revenue originating from activities such as human trafficking, extortion enterprises, and weapons trafficking.[196] The cartels amalgamate the criminal and terrorist aspect of their organization through these activities for financial gain.[197] Ergo, the plaintiffs claimed that HSBC is liable for the terrorist attacks against their family members under the Anti-Terrorism Act (ATA), Section 2333 of 18 U.S.C.[198] *Zapata* demonstrates how large-scale money laundering operations can be conducted using relatively simple means: a program was created to allow individuals to deposit cash without detection as part of a much larger operation.

Step 2 (aggregation) and Step 3 (movement of funds) of the TRM work in tandem in this HSBC case. HSBC possessed cartel money and transferred the funds to suspicious organizations. HSBC's allegedly reckless protocols allowed the cartels to launder money through its legitimate institution. After the money was raised through illicit means, it was delegated to financial intermediaries on either end of each transaction. 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.[199] The defendants in *Zapata*, according to the Complaint, promoted a three-step approach to money laundering, used by the cartels, known as placing, layering, and integrating.[200] The first step places the money into the international financial system.[201] Second, illicit funds in the financial system are layered into a series of different and smaller amounts to conceal their origin.[202] This is supposed to create

194. *Id.*

195. *Id.* ¶ 244.

196. *Id.* ¶ 37; CONVERGENCE, *supra* note 34, at 69-70.

197. CURTIS & KARACAN, supra note 127, at 1, 22.

198. *See* 18 U.S.C. § 2333(a) (2006); *see generally* CURTIS & KARACAN, *supra* note 127, at 1, 22.

199. *See* O'Halloran et al., *Terrorist Resourcing Model*, *supra* note 12, at 38. While some organizations possess the capability to acquire and aggregate funds (such as charitable organizations), the transfer of funds and collection by a terrorist entity may be completed by a different actor. *See* Int'l Relief Fund for the Afflicted and Needy (Can.) v. Minister of Nat'l Revenue, [2013] FCA 178 (discussing the charity IRFAN).

200. Complaint, *supra* note 190, ¶ 110.

201. *Id.*

202. *Id.*

a "façade of legitimacy," making the funds untraceable.[203] Integration, the final step, brings the illegitimate funds back into the conventional banking system by turning it into legitimate funds.[204] Illegitimate funds enter the legal economy through a series of purchases and investments.[205]

The Complaint notes two ways that the funds were placed, layered, and integrated from the U.S. banking system to the international economy and turned into legitimate funds. The first money laundering method is called *Casas de Cambio*, also known as "exchange houses"—a currency exchange method to circulate illicit money in Mexico.[206] This method allows for the exchange of one currency to another.[207] *Casas de Cambio* do not operate the same as banks, and the value of the currency remains the same. In other words, the *Casas de Cambio* do not exchange currencies at typical foreign exchange rates. *Casas de Cambio* allow businesses to transfer or exchange illicit money to different bank accounts, including in the United States.[208] The second type of money laundering is called the black market peso exchange (BMPE).[209] This method is mainly used when cocaine is sold in U.S. dollars and converted to other currencies, such as Colombian pesos, to compensate the cartels who produce cocaine in Colombia.[210] In this case, the funds travelled from HSBC branches in the United States to HSBC US, HSBC Mexico, and *Casas de Cambio* Puebla S.A de C.V in Puebla, Mexico, which served as the exchange house and chief money launderer for the cartels. Peso brokers received the U.S. dollars from the drugs sold in the United States. These brokers then sold the U.S. dollars in Colombian pesos at a discounted rate.[211]

The case provides insight into a cartels' three-step money laundering process. Tom Dart, a reporter with *The Guardian*, finds:

> [M]oney 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,

203. *Id.*
204. *Id.*
205. *See* CASSARA, HIDE & SEEK, *supra* note 38, at 36-37.
206. Complaint, s*upra* note 190, ¶ 119.
207. *Id.*
208. *Id.* ¶ 119.
209. *Id.* ¶ 121.
210. *Id.* ¶ 121.
211. *Id.* ¶¶ 121-25.

> ammunition, vehicles, planes, communication devices, raw materials for drug production, and all other instrumentalities essential to their operations would be substantially impeded.[212]

Step 4 of the TRM shows how the cartels use the money to ensure that their organization grows, remains stable, and that 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 took HSBC to court over four separate instances regarding the murders of U.S. family members by the cartels. Two federal U.S. agents—victims Jaime Zapata and Victor Avila Jr.—were attacked in broad daylight by two cars full of Los Zetas militants, killing agent Zapata while severely wounding his partner on a highway outside of San Luis Potosi.[213] The Complaint notes that the cartels had military grade weapons and over 100 rounds for their AK-47s.[214] The next two 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.[215] The pregnant mother, Leslie, was shot in the head.[216] The final assault was on victim Rafael Morales Valencia who exited the church on his wedding day to face sixteen assassins from the Sinaloa Cartel.[217] 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 all three by asphyxiation.[218] The cartels have risen as the largest threat to Mexican national security and are similarly menacing to the United States. Since 2006, cartels have claimed over 100,000 lives.[219] It is important to note that this case and all others are coded based on variables as shown in Appendix 1.

In *Goldberg v. UBS*, a suicide bombing on a Jerusalem bus killed the Karen Goldberg's husband, Stuart Goldberg.[220] Stuart was a Canadian citizen and Israeli resident.[221] The Goldberg family—Karen and her seven children—brought a civil suit in a United States District Court under the Anti-Terrorism Act (ATA) against UBS Bank for

---

212. Tom Dart, *Families of Americans Killed by Mexican Cartels Sue HSBC for Laundering Billions*, GUARDIAN (Feb. 11, 2016, 3:16 PM), https://www.theguardian.com/business/2016/feb/11/families-of-americans-killed-by-mexican-cartels-sue-hsbc [https://perma.cc/3YCP-X429] (internal quotation marks omitted).

213. Complaint, *supra* note 190, ¶ 2.

214. *Id.*

215. *Id.* ¶ 3.

216. *Id.* ¶ 4.

217. *Id.* ¶ 4.

218. *Id.* ¶ 4.

219. *Id.* ¶ 5.

220. Goldberg v. UBS AG, 660 F. Supp. 2d 410, 416 (E.D.N.Y. 2009).

221. *Id.* at 414.

providing services to the Association de Secours Palestine (ASP), a known funder of Hamas.[222] The plaintiffs alleged that UBS was fully aware that they were providing services for the ASP, and indirectly Hamas.[223] UBS is a financial institution headquartered in New York.[224] The court held that the plaintiffs successfully pleaded their claim under the ATA.[225] The investor in the case was ASP, a Swiss-based bank that belongs to an umbrella organization, the "Union of Good," also known as the "Charity Coalition."[226] ASP was both the financial intermediary and the investor in this case. ASP was identified as a Hamas-fundraising entity by President George W. Bush on October 22, 2003 and was placed on the Office of Foreign Assets Control (OFAC) list as a Specially Designated Global Terrorist (SDGT) entity.[227] 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.[228] The Comité de Bienfaisance et de Secours (CBSP), of which ASP is a subsidiary, also operates under the Union of Good.[229] CBSP collaborates with more than a dozen humanitarian organizations based in the West Bank, Gaza, Jordan, and Lebanon.[230] Khalid Al-Shuli, who is a designated terrorist entity under U.S. Executive Order 13224, presided over CBSP and ASP at the time.[231]

As mentioned, UBS is also represented as a financial intermediary, which allegedly knowingly provided banking services to a group affiliated with Hamas.[232] UBS provided financial support 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 that UBS failed to implement any measure restricting the client from processing transactions

---

222. *Id.* at 413-15.

223. *Id.* at 416.

224. *Id.* at 415.

225. *Id.*

226. *See* Levitt, *supra* note 132.

227. Press Release, U.S. Dep't of the Treasury, Office of Pub. Affairs, U.S. Designates Five Charities Funding Hamas and Six Senior Hamas Leaders as Terrorist Entities (Oct. 22, 2003), https://www.treasury.gov/press-center/press-releases/Pages/js672.aspx [https://perma.cc/L943-VTTN].

228. Levitt, *supra* note 132.

229. *Id.*

230. Press Release, *supra* note 227.

231. *Resource Center: Commite de Bienfaisance et de Secours aux Palestiniens Association de Secours Palestinie*, U.S. DEP'T TREASURY, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/protecting-charities_execorder_13224-b.aspx [https://perma.cc/4KBX-BKG6].

232. Goldberg v. UBS AG, 660 F. Supp. 2d 410, 416, 432-33 (E.D.N.Y. 2009).

through the United States.[233] The money in *Goldberg v. UBS* was transferred to the Tulkarem Zakat Committee, the next financial intermediary, with which many senior members of Hamas are affiliated.[234] Members include "Mohmammed Hamed Qa'adan, head of the Tulkarm [Z]akat [C]ommittee, and Ibrahim Muhammad Salim Salim Nir Al Shams, a member of both the Tulkarm [Z]akat [C]ommittee and the Supreme Hamas leadership in Nur Al-Shams."[235] Tulkarem operates in the West Bank and is not formally recognized as an SDGT but is recognized as supporting terrorist activities in Israel.[236] UBS sent money to a Tulkarem account controlled by Hamas through a bank transfer.[237] Ergo, ASP sent the money to Tulkrarem through UBS, and Tulkarem gave the money to Hamas, which completed the transfer of resources.

Transfers to the Tulkarem Committee were accordingly intended for Hamas. In this case, approximately US$25,000 was transferred between October 3, 2003 and January 8, 2004.[238] According to some remarks made by President Bush and members of his cabinet, the U.S. government established that the funds are used by Hamas to support schools that indoctrinate children to become suicide bombers.[239] The significance of this case rests in the lack of compliance by financial institutions and their collaboration with designated terrorist groups despite being fully aware of the repercussions. The Treasury Department indicated that UBS settled with the U.S. government for approximately US$1.7 million.[240]

In *Fields v. Twitter*, an American citizen in Florida, Tamara Fields, 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.[241] The perpetrator was Abu Zaid, a 28-year-old Jordanian police captain studying at

---

233. ENFORCEMENT INFORMATION FOR AUG. 27, 2015: UBS AG SETTLES POTENTIAL LIABILITY FOR APPARENT VIOLATIONS OF THE GLOBAL TERRORISM SANCTIONS REGULATIONS, [hereinafter ENFORCEMENT INFORMATION] https://www.treasury.gov/resourcecenter/sanctions/CivPen/Documents/20150827_ubs.pdf [https://perma.cc/RGT4-GPZB].

234. *Goldberg*, 660 F. Supp. 2d at 416, 433-34.

235. Levitt, *supra* note 7.

236. *Goldberg*, 660 F. Supp. 2d at 416.

237. *Id.*

238. *Id.*

239. *White House Freezes Suspected Terror Assets*, WASH. POST ONLINE (Dec. 4, 2001), http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushtext_120401.html [https://perma.cc/5SXC-L45R].

240. ENFORCEMENT INFORMATION, *supra* note 233.

241. Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1119 (N.D. Cal. 2016).

the International Police Training Centre (IPTC).[242] 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.[243] ISIS claimed responsibility for the attack and shortly after tweeted, "[t]he killing shall continue and will not stop."[244] Twitter, in operation since 2010, did not block or remove official ISIS twitter accounts on the grounds of freedom of expression.[245]

Fields does not have any identifiable investors, which will be discussed in the financing portion of this case study. Twitter is labeled here as the vehicle for intangible services to propagate and ultimately recruit, inspire, and finance ISIS. The 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 social media propaganda and impact of widespread information dissemination.

This case shows the causal nexus between the resources moved due to the tweets sent out by the various ISIS accounts with the collection of 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.

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.[246] Al-Furqan's account is responsible for the dissemination of ISIS' egregious acts of brutality—including beheading videos, pictures, and various other multimedia tools of propaganda.[247] The Al-Hayat Media Center operated at least six Twitter accounts that focused on recruiting Westerners.[248] After the tweets are posted, Twitter is used as a core recruiting tool.[249] ISIS recruiters first communicate with prospective individual recruits through Twitter's

242. Complaint, *supra* note 5, at 13.
243. *Id.*
244. *Id.* at 14.
245. *Id.* at 1121-24.
246. *Id.* at 2.
247. *Id.*
248. *Id.*
249. *Id.*

direct private messaging tools.[250] Online communication allows ISIS to interact directly with individuals from anywhere in the world via Twitter's direct messaging function. ISIS recruited about 30,000 foreign fighters via Twitter, including at least 4,500 westerners, and among them are 250 U.S. citizens.[251]

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.[252] This example shows the ease of propagation through mediums such as social media. ISIS also uses Twitter to post instructional guides and promotional videos, called "mujatweets."[253] ISIS members, for instance, tweeted English guidelines in June 2014 to instruct Westerners how to travel and join the "fight" in the Middle East.[254] Consequently, once individuals follow the account and show interest, they are provided with the necessary tools that are disseminated through the tweets from ISIS accounts and Twitter's direct messaging function to aid the terrorist organization in executions (such as lone-actor attacks), recruiting, or funding.

ISIS has also been using Twitter to accumulate funds from sympathizers and organizers, promising rewards for the number of "Dinars" donated.[255] 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 US$7000—was donated through one campaign, promising donors "silver status" and "gold status" depending on how much an individual was willing to donate.[256] Not only does this engage willing donors, but it also provides alternate ways for individuals to involve themselves with the ease of an app.

Fields shows the need for methodological approaches, such as the TRM, that accounts for a broad range of resource deployments, not just cash, especially with social media such as Twitter that can be used to encourage attacks by lone-wolf actors. Even without the explicit financing component, *Fields* would still involve resources to carry out terrorist attacks. Propaganda is as dangerous as moving funds: it was seen by some 30,000 foreign sympathizers who were

250. *Id.*
251. *Id.* at 5.
252. *Id.* at 7-8.
253. *Id.* at 4.
254. *Id.* at 4.
255. *Id.* at 5.
256. *Id.* at 5.

recruited via Twitter and joined ISIS.[257] 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 peaked at 40,000 tweets per day.[258] The intermediaries are those who either collect the funds through one of many accounts and transfer them to ISIS branches, or those who join ISIS as a result of its propaganda messages.

B. General Observations

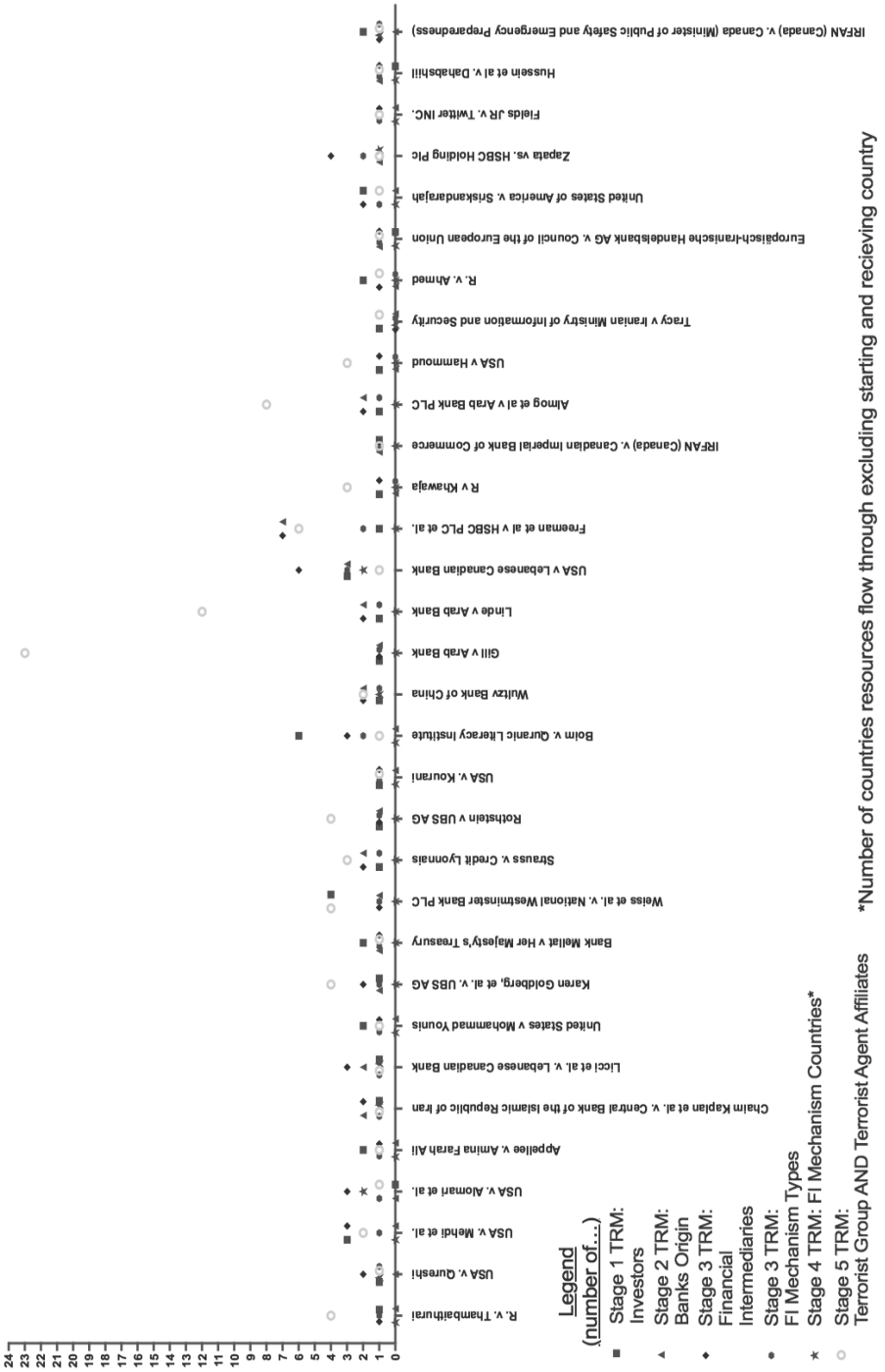
Of the thirty-two cases listed on the x-axis in Figure 1, most include investors, banks, financial intermediaries, mechanism type (transfers), mechanism countries, and terrorist groups. Although most cases only involve a couple of these nodes at each stage of the TRM, the majority of cases include all the stages of the TRM. "Mechanism countries" are low because the starting and receiving country are not counted in this category; only countries through which money flows between the starting and ending transfer points are counted. Figure 1 illustrates the pattern that emerges by evaluating terrorist networks using the five stages of the TRM.

257. *Id.* at 5.

258. *Id.* at 8.

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, this may simply be a function of the preliminary scan of European cases. In sum, of the thirty-two terrorist financing cases, twenty-one hail from the United States, seven from Canada, one from Europe, and one from the United Kingdom. The results show nine investors from the United States, five from Canada, four from Iran, four from Lebanon, and one from the United Kingdom, 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 or transferring resources intended for terrorism: Arab Bank PLC, HSBC, and UBS AG. Finally, the three major terrorist entities identified as recipients of the most terrorist resources transactions are Hamas, Hezbollah, and Iran. Seventeen banks were used, and the locations from or through which investors and financial intermediaries worked centered on three

financial hubs: London, Beirut, and New York. Although Canada runs second for the number of investors and third for financial intermediaries, the cases show that the transactions took place in separate Canadian cities. The cities are spread out across the country, with no discernable pattern for a Canadian city 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. Khawaja **Interpal** in Weiss v. National Westminster Bank PLC	(7) in (4) Different Cases: **Bank Saderat** PLC in Kaplan v. Central Bank of the Islamic Republic of Iran **National Westminster Bank PLC** in Weiss v. National Westminster Bank PLC **HSBC Group** in Freeman v. HSBC Holdings PLC **Barclays Bank** in Freeman v. HSBC Holdings PLC **Standard Chartered Bank** in Freeman v. HSBC Holdings PLC **Bank Saderat** in Freeman v. HSBC Holdings PLC **HSBC Group** in Zapata v. HSBC Holdings PLC	Funded (4) in (5) Cases: **Hamas** in Palestine (National Westminster Bank Case) **Hezbollah** in Lebanon (Freeman & Kaplan) **Al-Qaeda** in Saudi Arabia (R v. Khawaja) **Mexican Cartels** (Zapata)
Beirut	(2) in (2) Different Cases: **Hassan Ayash Exchange Company** in USA v. Lebanese Canadian Bank SAL **Shahid Foundation** in Licci v. Lebanese Canadian Bank SAL	(11) in (6) Different Cases: **Lebanese Canadian** Bank in USA v. Lebanese Canadian Bank SAL **Arab Bank PLC** in Gill v. Arab Bank **Arab Bank PLC** in Linde v. Arab Bank	Funded (2) in (6) Cases: **Hezbollah** in Lebanon (Lebanese CB & Licci) **Hamas** in Palestine (Linde, Gill, & Almog) **Hezbollah** in Lebanon (Hammoud)

City	Investors	Financial Intermediaries	Terrorist Organization(s) Funded
		BLOM Bank in United States v. Lebanese Canadian Bank SAL **Arab Bank PLC** in Almog v. Arab Bank PLC **Sheik Abbas Harake** in United States v. Hammoud **Sahid Foundation** in Licci v. Lebanese Canadian Bank SAL **Middle East and Africa Bank** in United States v. Lebanese Canadian Bank SAL **Lebanese Canadian Bank** in Licci v. Lebanese Canadian Bank SAL **Federal bank of Lebanon** in United States v. Lebanese Canadian Bank SAL	
New York	(2) in (1) Case: **Mohammad Younis, and Faisal Shahzad** in United States v. Younis	(8) in (6) Different Cases: **Mohammad Younis** in United States v. Younis **Credit Lyonnais** in Strauss v. Credit Lyonnais **Arab Bank PLC** in Linde v. Arab Bank PLC **Arab Bank PLC** in Almog v. Arab Bank PLC **HSBC Bank** in Zapata v. HSBC Holdings PLC **American Express Bank** in Licci v. Lebanese Canadian Bank SAL	Funded (4) in (6) Cases: **Hezbollah** in Lebanon (Licci) **Hamas** in Palestine (Linde & Almog) **Mexican Cartels** (Zapata) **Individual** in New York (Younis)

Because New York is the financial hub of the world, its frequency in Table 2 is not surprising. Similarly, most terrorism resource cases have been brought in U.S. 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 particular global banks. A few banks appear to recur: the Lebanese Canadian Bank, HSBC Holdings PLC, 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 Holdings PLC. Some banks mainly contribute to a particular terrorist organization. For example, Arab Bank PLC seems involved only in the transfer of funds to Hamas and Hamas affiliates. The Lebanese Canadian Bank only transferred funds to Hezbollah. In contrast, HSBC Holdings PLC 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 v. Arab Bank **Beirut** in Almog 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 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 v. HSBC Holdings PLC **London** in Freeman v. HSBC Holdings PLC **New York** in Zapata v. HSBC Holdings PLC **Mexico City** in Zapata v. HSBC Holdings 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 emphasizes the location where the terrorist resources are accumulated. As such, Arab Bank PLC appears in Beirut and New York. Step 3 also focuses on the transfer of resources to a terrorist organization. It identifies banks that had a direct link in funding terrorist organizations, and it 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 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.[259] 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, Steps 2 and 3 of the TRM work in tandem, showing that Arab Bank PLC collected and transferred terrorist resources. Next, Step 4 of the TRM indicates how resources were transmitted. Finally, Step 5 of the TRM shows the transmission and use of resources by the recipient terrorist organization, Hamas. This network is visualized in Figure 2. Furthermore, *Almog v. Arab Bank PLC* also appears twice in the dataset following a very similar network trend to 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 (Figure 3). To show the scale of these cases, secondary research for *Almog* indicates that US$194,123,924 was transferred to the Saudi Committee in Support of the Intifada Al Quds, with US$40,000,000 being deposited with Arab Bank PLC.[260] By contrast, in *Linde*, US$20,000,000 was successfully transferred through Arab Bank to fund Hamas terror attacks.[261]

259. Linde v. Arab Bank PLC, 269 F.R.D. 186, 192, 201, 205 (E.D.N.Y. 2010).

260. *Saudi Arabia: Friend or Foe in the War on Terror?: Hearing Before the Comm. on the Judiciary*, 109th Cong. (2005), https://archive.org/stream/gov.gpo.fdsys.CHRG-109shrg34114/CHRG-109shrg34114_djvu.txt [https://perma.cc/9CUG-M3KU].

261. *Linde*, 269 F.R.D. at 191-92, 202.

Figure 2

A case of network of terrorist resourcing that shows all stages of the TRM

***Linde v. Arab Bank PLC*:**

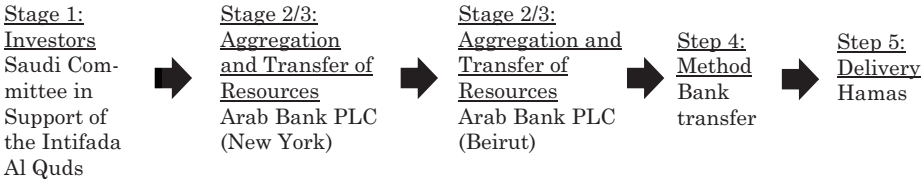
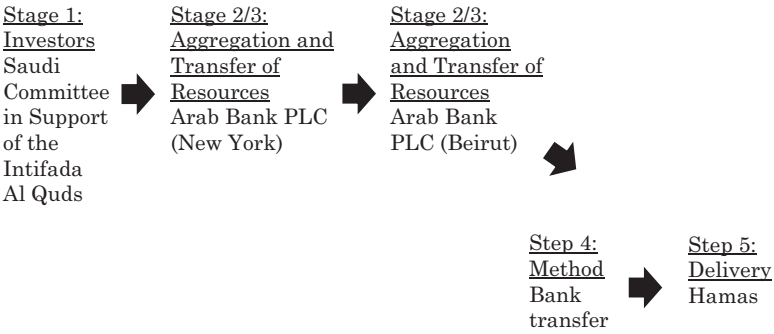


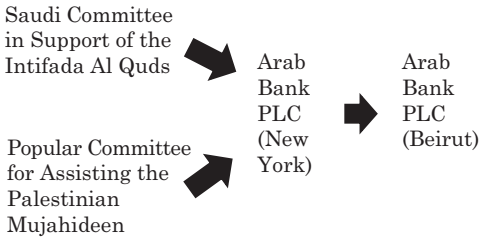
Figure 3

Two cases of networks of terrorist resourcing that show all stages of the TRM

***Linde v. Arab Bank PLC*:**



***Almog et al. v. Arab Bank PLC*:**



The above diagrams illustrate the complexity of terrorist financing. The same patterns repeat 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 SAL x3, 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 acts as an investor and not a financial intermediary.

Table 4 shows Hezbollah and Hamas as the top-resourced terrorist organizations, with 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 *Kaplan v. Central Bank of the Islamic Republic of Iran*. *Kaplan* explains two of the three appearances of Bank Saderat PLC

with transfers to Hezbollah.[262] The causal mechanism Bank Saderat employed to transfer the funds is illustrated in the case: "[s]pecifically, plaintiffs claim that BSI [Bank Saderat Iran] received Iranian funds from defendant Central Bank of Iran ("CBI") transferred those funds to BSPLC [Bank Saderat PLC] in London who then transferred them to 'accounts controlled by Hezbollah in branches of defendant BSI in Beirut."[263]

Bank Saderat also appears in *Freeman v. HSBC Holdings PLC*, specifically Bank Saderat London. *Freeman* accounted for most of the locational nodes, including five different banks from the United Kingdom used to transfer resources, one bank in Germany, and one in Switzerland.[264] Resources for Hamas seem to originate with banks in the United States and Lebanon. Arab Bank PLC transfers resources to Hamas more frequently than anyone else—five times in three different cases: *United States v. Lebanese Canadian Bank SAL*, *United States v. Hammoud*, and *Linde*.[265] In both *Lebanese Canadian Bank* and *Hammoud*, the locational nodes of Arab Bank PLC are in Lebanon and the United States. This may suggest a working relationship between these two branches, with the third case, *Linde*, noting only 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 United States or Lebanon as locational nodes, but instead seems to rely exclusively on banks in Germany and Switzerland.

VI. DISCUSSION

Terrorist resourcing is a collective-action problem that necessitates collaboration to contain terrorist financing. The court cases and accompanying documents demonstrate how resources are transferred through various countries to end up with terrorist organizations. This study identifies specific nodes in an effort 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.[266] The eight special recommendations seek to prevent terrorist organizations from

---

262. Kaplan v. Cent. Bank of the Islamic Republic of Iran, 961 F. Supp. 2d 185, 190 (D.D.C. 2013).

263. *Id.*

264. Freeman v. HSBC Holdings PLC, No. 14-cv-6601, 2018 WL 3616845, at *1-2 (E.D.N.Y. 2018).

265. United States v. Leb. Can. Bank SAL, No. 11 Civ 9186(PAE), 2012 WL 3854778, at *1 (S.D.N.Y. Sept. 5, 2012); *Linde*, 269 F.R.D. at 191-92, 205; United States v. Hammoud, 381 F.3d 316, 325-26 (4th Cir. 2004).

266. *See supra* note 70 and accompanying text.

accessing funds from international financial institutions. However, nearly half of all the cases used at least one financial institution to transfer resources. In nineteen of the thirty-two cases, a simple bank transfer was the method of resource transfer. FATF is only as effective as states prepared to comply with and enforce the eight recommendations domestically.

As discussed, FATF does not hold any formal enforcement power. Although member countries reformed domestic law based on FATF recommendations, eighteen different countries from across the globe 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.[267] FATF will continue to face challenges in countering 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.

Notwithstanding its status as the preeminent global financial hub, 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 FATF recommendations and enforcement actions by 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, in particular by amassing financial information collected by banks under KYC rules. *Zapata v. HSBC Holdings plc* shows the ineffectiveness of this approach when criminals or terrorists launder monies through placing, layering, and integrating.[268] Nevertheless, only four banks were found to have laundered money through New York. The FBI also appears seven times as the investigating agency, which demonstrates the effectiveness of FinCEN in relaying information to relevant enforcement agencies.

Member states of the United Nations have also agreed on a mandate to overcome collective-action problems by implementing counter-terrorist financing recommendations.[269] Whether the Counter-Terrorism Implementation Task Force (CTITF) or the Counter-Terrorism Committee Executive Directorate (CTED) have been a driving force in countering terrorist financing, however, cannot be inferred from the evidence in this study. Yet, indications suggest that collective efforts

267. Gardner, *supra* note 21, at 342.

268. Zapata v. HSBC Holdings PLC, No. 1:16-CV-030, 2017 WL 6939210, at *1-2, 4 (S.D. Tex. Oct. 17, 2017).

269. *Collective Action, Overcoming Information-Sharing Barriers Vital to Tackling Violent Extremism, Secretary-General Tells Counter-Terrorism Conference*, UNITED NATIONS (June 28, 2018), https://www.un.org/press/en/2018/l3282.doc.htm [https://perma.cc/3A4C-KYML].

may be waning: Levitt hypothesizes that as the September 11th attacks become more distant, counter-terrorist financing efforts have diminished.[270] The CTITF has the potential to counter such trends by promoting cooperation and information sharing to prevent designated terrorist entities from raising funds and other resources. Nonetheless, designated terrorist entities continue to be operational in many cases. For instance, *Goldberg v. UBS* demonstrates the use of multiple financial institutions in Switzerland that are SDGT.[271] CTED did not come up in these cases, but the lapse in international coordination indicates that country reports and the dissemination of information could be better.

Some of the findings that emerge from the TRM analysis are quite instructive. First, the diversity of cases notwithstanding, a clear pattern of resourcing emerged that differs only by scale: the more funds that 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 divided up, which requires more people, each of whom has their own preferences and connections for how to transfer resources successfully. This would explain the greater number of financial institutions involved. Second, the evidence and approach in this study demonstrates 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. This aberration from the expected frequency suggests that U.S. domestic enforcement mechanisms may be having a strong deterrence effect, not just on investors who intentionally circumvent the United States and U.S.-based financial institutions, but also on compliance by U.S. financial institutions and those with U.S.-based affiliates to avoid prosecution and fines.

Conversely, the apparently lax approach to enforcement by British authorities may be a function of a preference for an intelligence approach to prioritizing terrorist resourcing: as long as transfers do not pose an imminent risk to the United Kingdom or British interests, the reality of human resource constraints means standing back to watch and follow transfers while optimizing insights to be gleaned about global terrorism.

In either case, the difference in findings for the United States and the United Kingdom suggests a possible difference in strategies for

270. Levitt & Jacobson, *supra* note 61.

271. Goldberg v. UBS AG, 660 F. Supp. 2d 410, 415-16, 433 (E.D.N.Y. 2009).

combating terrorist resourcing. This may also explain why different countries are taking different approaches to complying with FATF and UN efforts—strategy may be driving compliance, rather than compliance driving strategy. The same appears to hold true 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 noncompliance 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 more efficient to risk a fine than to forego the profits that illicit transactions generate.

The low risk of prosecutions, fines, and reputational harm may enable 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 deliberate strategy than a cost of doing business: banks might feel that their business strategy requires them to take the good with the bad and incur manageable financial and reputational costs along the way. Since illegal activity is estimated to comprise three to four percent of the global economy, and that activity requires banking services, this 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: a possible difference may amount to money launderers having as their aim not just to transfer illicit gains but to hold on to them whereas terrorist resourcing is just about moving value, not about holding on to it. Nor does this study capture the movement of resources through less compliant states whose financial institutions may enable more covert methods of resourcing for terrorist organizations. In this regard, among the top twenty global financial hubs, the outliers that do not show up in this study may warrant closer scrutiny: Hong Kong, Singapore, Shanghai, Tokyo, Sydney, Beijing, Zurich, Frankfurt, Toronto, Shenzhen, Boston, San Francisco, Dubai, Los Angeles, Chicago, Vancouver, Guangzhou, and Melbourne. That none of the hubs in Asia and the Middle East show up in this study may just be happenstance of language and selection bias; or not.

VII. CONCLUSION

The conventional method of identifying Money Laundering/Terrorist Financing (ML/TF) traditionally deployed by FIUs has limited remit in identifying 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 also 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 a variety of outlets in different ways. As the cases in this study reinforce, the TRM offers a more comprehensive approach to identifying, and thus preventing, 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 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. The research shows the multiple ways in which resources are raised and transferred, but the ultimate purpose of funds is notoriously 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.

To be sure, thirty-two cases is a small subset and is thus necessarily marred by possible selection bias and omitted variables. For instance, the notable lack of tax havens could mean that only the irresponsible or careless show up in our sample, and that smarter actors 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 relatively few convictions for transnational terrorist financing, money laundering, and tax evasion.

While it is unclear how representative or robust the data is, the fact that distinct patterns emerge shore up the broader validity of the findings. Indeed, 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 Article posits improves our empirical, conceptual, methodological, and theoretical understanding of the phenomenon of terrorist resourcing. It thus contributes to the ongoing optimization of anti-terrorist resourcing laws, policies, and risk management practices.

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 or 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 or goods passed through between origin and destination. This does not include the country of the origin (investor) nor the country where the funds or goods ultimately arrive (terrorist).

Financial intermediary mechanism type: How the funds or 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 or 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 in which 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 (ALPHABETICAL ORDER)

1. Almog v. Arab Bank, PLC, 471 F. Supp. 2d 257 (E.D.N.Y. 2007).
2. Bank Mellat v. Her Majesty's Treasury [2013] UKSC 38, [2013] UKSC 39.
3. Boim v. Quranic Literacy Institute, 340 F. Supp. 2d 885 (N.D. Ill. 2004).
4. Europäisch-Iranische Handelsbank AG v. Council of the European Union [2014] C-585/13 P (appeal taken from Eng.).
5. Fields v. Twitter Inc., 881 F.3d 739 (9th Cir. 2018).
6. Freeman v. HSBC Holdings PLC, 14 CV 6601 (DLI) (CLP), 2018 WL 3616845 (E.D.N.Y. July 27, 2018).
7. Gill v. Arab Bank, 893 F. Supp. 2d 474 (E.D.N.Y. 2012).
8. Goldberg v. UBS AG, 660 F. Supp. 2d 410 (E.D.N.Y. 2009).
9. Her Majesty the Queen v. Ahmed, [2014] ONSC 6153 (Can.).
10. Hussein v. Dahabshiil Transfer Servs., Ltd., 230 F. Supp. 3d 167 (S.D.N.Y. 2017).
11. International Relief Fund for the Afflicted and Needy (Canada) v. Canadian Imperial Bank of Commerce, [2013] 220 ONSC 4612.
12. International Relief Fund for the Afflicted and Needy (Can.) v. Minister of National Revenue, [2013] FCA 178.
13. Kaplan v. Central Bank of the Islamic Republic of Iran, 961 F. Supp. 2d 185 (D.D.C. 2013).
14. Licci ex rel. Licci v. Lebanese Canadian Bank, SAL, 732 F.3d 161 (2d Cir. 2013).
15. Linde v. Arab Bank, PLC, 97 F. Supp. 3d 287 (E.D.N.Y. 2015).
16. R. v. Khawaja, [2012] 3 SCR 555 (Can.).
17. R. v. Thambithurai, [2011] BCCA 137 (Can.).
18. Rothstein v. UBS AG, 708 F.3d 82 (2d Cir. 2013).
19. Strauss v. Credit Lyonnais, S.A., 1242 F.R.D 199 (E.D.N.Y. 2007).
20. Tracy v. Iranian Ministry of Information and Security, [2016] ONSC 3759 (Can.).
21. United States v. Ali, 799 F.3d 1008 (8th Cir. 2015).
22. United States v. Alomari, 6:08-cr-06087 (W.D.N.Y. May 7, 2008).
23. United States v. Sriskandarajah, [2012] 3 S.C.R. 609 (Can.).
24. United States v. Hammoud, 381 F.3d 316 (4th Cir. 2004).
25. United States v. Kourani, 17 Cr. 417 (AKH), 2018 WL 1989583 (S.D.N.Y. April 26, 2018).

26. United States v. Lebanese Canadian Bank SAL, 285 F.R.D. 262 (S.D.N.Y. 2012).
27. United States v. Mehdi, 1:09-cr-20852 (S.D. Fla. Oct. 1, 2009) (Court Listener).
28. United States v. Qureshi, 09-CR-0102-001-CVE (N.D. Okla. Nov. 21, 2011).
29. United States v. Younis, No. 10 Cr. 813 (JFK), 2011 WL 1485134 (S.D.N.Y. April 19, 2011).
30. Weiss v. National Westminster Bank PLC, 768 F.3d 202 (2d Cir. 2014).
31. Wultz v. Bank of China, 304 F.R.D. 384 (S.D.N.Y. 2015).
32. Zapata v. HSBC Holding PLC, CIVIL ACTION NO. 1:16-CV-030, 2017 WL 6939209 (S.D. Tex. Sep. 14, 2017).