GLOBAL CENTER ON COOPERATIVE SECURITY

POLICY BRIEF

Untangling a Marriage of Convenience

Anti-Money Laundering and Countering the Financing of Terrorism

By **Tracey Durner** and **Danielle Cotter**

January 2019

Within the realm of policy discussions, anti–money laundering (AML) and countering the financing of terrorism (CFT) efforts are generally treated as a package deal. The Financial Action Task Force (FATF), the FATF Recommendations, and related guidance documents represent today's international AML and CFT standards and are mirrored in laws and initiatives around the world. Given the "obvious similarities and differences between money laundering and terrorism financing," FATF notes "the risks (of both) are often assessed and managed using the same information flows between public and private sector institutions."[1]

This convergence between the types of information and stakeholders relevant to money laundering and terrorism financing is, in part, behind the unification of AML and CFT efforts. From a policymaking standpoint, the combination makes sense. Financial intelligence units (FIUs) already analyze suspicious financial activity, including potential instances of money laundering, often triggered by reports from the private sector resulting from frontline compliance and transaction monitoring procedures. It seems logical to incorporate the deterrence, detection, and tracking of terrorism financing into existing AML frameworks. In practice, critics have argued this "marriage" places undue burden on the private sector to understand the intent of criminals behind the actual transactions.[2] Others contend that the very premise of CFT policies are misguided, resulting in ineffective and even harmful outcomes.[3]

With the rise of the Islamic State of Iraq and the Levant (ISIL) and the preponderance of low-cost, lone-actor attacks in North America and Europe, international attention once again has focused on CFT as a central tenet in the fight against terrorism. In 2016, FATF issued a consolidated strategy on CFT,[4] followed by the adoption of an operational plan in 2018.[5] CFT-specific entities such as the Counter ISIL Financing Group have emerged, and the French government in 2018 convened a high-level international conference focused on combating the financing of

1 Financial Action Task Force (FATF), *Money Laundering and Terrorist Financing Risk Assessment Strategies*, 18 June 2008, http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20Risk%20Assessment%20Strategies.pdf.

2 Gauri Sinha, "AML-CFT: A Forced Marriage Post 9/11 and Its Effect on Financial Institutions," *Journal of Money Laundering Control* 16, no. 2 (May 2013): 142–158.

3 Peter R. Neumann, "Don't Follow the Money: The Problem With the War on Terrorist Financing," *Foreign Affairs* 96, no. 4 (July/August 2017).

4 FATF, "Consolidated FATF Strategy on Combatting Terrorist Financing," 19 February 2016, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Terrorist-Financing-Strategy.pdf.

5 FATF, "Terrorist Financing," n.d., http://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html (accessed 5 December 2018).

ISIL and al-Qaida, with a second conference scheduled for Australia in mid-2019.[6]

This brief examines where and how AML frameworks are fit for purpose relative to CFT and considers where additional CFT-specific efforts are necessary. It begins with a brief summary of the evolution of money laundering and terrorism financing policies, discussing the unification of the two fields and the key differences between the motivations and typologies of money laundering and terrorism financing crimes. Against that backdrop, it explores the four objectives of CFT efforts (prevent, detect, freeze, and trace) to identify areas where existing unified AML/CFT frameworks are working and areas where more nuance is required to effectively combat threats specific to terrorism financing. Although particular attention is given to the United States and United Kingdom as international financial centers, similar approaches and convergences between AML and CFT policies and practices occur worldwide. The brief concludes with recommendations on how current CFT policy discourse and evolution can meaningfully support broader counterterrorism objectives.

AML AND CFT: A MARRIAGE OF CONVENIENCE?

The acts of misrepresenting wealth and concealing its origins or destinations from authorities long predate the emergence of the term "money laundering." Organized crime, particularly international drug trafficking, provided the impetus for many AML frameworks that are still in place today. The United States is considered to have passed the first legislation related to money laundering in 1970. The U.S. Bank Secrecy Act (BSA) introduced record-keeping and reporting requirements for banks and other financial institutions, expanding the possibility for investigation and evidence collection relating to money laundering. Sixteen years later, the United States designated money laundering as a federal crime and established penalties for BSA violations, including civil and criminal forfeiture.

Shortly thereafter, the international community followed suit via the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, which calls on signatories to adopt measures to establish money laundering as a criminal offense and to "enable competent authorities to identify, trace, and freeze or seize proceeds relating to offenses (including money laundering)."[7] In "recognition of the threat posed to the banking system and financial institutions," FATF was established in 1989 as an intergovernmental body that would focus on combating money laundering.[8]

More than a decade later, the terrorist attacks in the United States on 11 September 2001 commanded significant international attention. Almost immediately, CFT became one of the central tenets of the U.S. response, with Executive Order 13224 ordering the freezing of assets and blocking of transactions by individuals and entities associated with or supporting al-Qaida and its affiliates, including Osama bin Laden, and other listed terrorist groups.[9]

U.S. President George W. Bush made clear his expectations that the international community would join the United States in its CFT efforts. In announcing the executive order, he stated, "[I]t puts the financial world on notice. If you do business with terrorists, if you support or sponsor them, you will not do business with the United States of America…. Money is the lifeblood of terrorist operations. Today, we're asking the world to stop payment."[10]

CFT mechanisms in the United States predated these attacks; as of 1996, the United States had criminalized knowingly providing or attempting or conspiring to

6 For the communiqué from the 2018 meeting, see "Final Statement – International Conference on Combating the Financing of Daesh and Al-Qaeda," France Diplomatie, 25–26 April 2018, https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/events/article/final-statement-international-conference-on-combating-the-financing-of-daesh.

7 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 20 December 1988, 1582 U.N.T.S. 27627.

8 FATF, "History of the FATF," n.d., http://www.fatf-gafi.org/about/historyofthefatf/ (accessed 27 December 2018).

9 Exec. Order No. 13224, 66 Fed. Reg. 49079 (25 September 2001).

10 Office of the Coordinator for Counterterrorism, U.S. Department of State, "President Freezes Terrorists' Assets," 24 September 2001, https://2001-2009.state.gov/s/ct/rls/rm/2001/5041.htm.

provide material support for terrorist crimes or listed terrorist organizations.[11] Yet, the effectiveness at that time was limited. The 9/11 Commission noted that, before the 2001 attacks, the FBI considered terrorism financing cases "too difficult" to pursue due to challenges in international information sharing and a perceived "wall" between intelligence and criminal investigations.[12]

To adequately respond to political pressure for action in the aftermath of 9/11, it was expedient to add CFT to AML frameworks already operational and successful. In October 2001, the USA PATRIOT Act amended the existing Money Laundering Control Act, "allowing investigators to use the tools that were already available to investigate organized crime and drug trafficking" to "detect and prevent terrorism," including terrorism financing.[13] The USA PATRIOT Act also contains numerous assertions of its extraterritorial application.[14]

These actions by the United States had ripple effects across the international system. On 28 September 2001, the UN Security Council adopted Resolution 1373, calling for all member states to establish a system for freezing "without delay" the assets of persons who commit or attempt to commit terrorist acts or participate in or facilitate the commission of terrorist acts.[15] This represented a near-universal expansion of the U.S. approach under Executive Order 13224 and marked a shift in international law as the United Nations mandated the adoption of domestic laws. The United Kingdom, which already had enacted CFT-specific measures due to the conflict in Northern Ireland, passed a significant amendment bolstering national CFT authority in early December 2001.[16] CFT was swiftly added to FATF's mandate via Special Recommendations in October 2001, successfully cementing the global marriage between AML and CFT.

UNTANGLING MOTIVATIONS AND METHODS

Understanding the motivations for money laundering and terrorism financing is important for determining the sectors that are targeted and the most common methods or typologies used in these crimes. This information is crucial for developing adequate detection mechanisms and responses, as well as for understanding risk profiles for countries and financial sectors (box 1).

The objective of money laundering is to generate usable profit, to integrate "dirty money" generated by a predicate offense, i.e., a form of criminal activity, into the financial system and make those funds appear legitimate. Criminal activities often yield large sums of proceeds in a short period of time. Those involved must conduct a series of transactions to put distance between the funds and the crime from which they originated so they appear to have a legitimate origin. The closer the crime is to the money, the more important it is for money launderers to place the funds in sectors in which substantial transactions are unlikely to draw attention. For this reason, cash-intensive businesses, as well as those that have subjective value such as the real estate, art, and precious stones markets, are often involved in the early stages of the money laundering process. Criminals are most vulnerable during the first round of injecting illicit funds into the financial system, and international standards include a range of measures intended to detect and report any activity that may be related to the proceeds of crime.

Terrorists raise funds from criminal channels and legal ones (e.g., donation of lawfully acquired income). Contrary to money laundering, it is not necessarily the source of the funds that makes terrorism financing illegal, but rather its purpose of supporting

11 18 U.S.C. § 2339A (1994) (providing material support to terrorists); 18 U.S.C. § 2339B (1996) (providing material support or resources to designated foreign terrorist organizations).

12 John Roth, Douglas Greenburg, and Serena Wille, "Staff Report to the Commission," *Staff Monograph on Terrorist Financing*, n.d., p. 33, https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf. (report to the National Commission on Terrorist Attacks Upon the United States).

13 U.S. Department of Justice, "The USA PATRIOT Act: Preserving Life and Liberty," n.d., https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.

14 Joseph B. Tompkins Jr., "The Impact of the USA PATRIOT Act of 2011 on Non-U.S. Banks" (paper, International Monetary Fund Seminar on Current Development in Monetary and Financial Law, Washington, DC, 7–17 May 2002), https://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/tompki.pdf.

15 UN Security Council, S/RES/1373, 28 September 2001.

16 The United Kingdom criminalized negligence related to terrorism financing by expanding the conditions for failure to disclose by the regulated sector from instances when an individual "knows or suspects" of an offense to when there is "reasonable grounds for knowing or suspecting." Terrorism Act, 2000, sec. 21A, https://www.legislation.gov.uk/ukpga/2000/11/pdfs/ukpga_20000011_en.pdf.

Box 1. A Note on Risk

When considering risk for money laundering and terrorism financing, the Financial Action Task Force (FATF) focuses its attention on countries that have technical or capacity gaps relative to the implementation of anti–money laundering (AML) and countering the financing of terrorism (CFT) standards. According to FATF, weak compliance correlates with higher risks for money laundering and terrorism financing activity. This approach is based on the premise that criminals may seek jurisdictions with limited AML and CFT regimes and enforcement capabilities to minimize the likelihood of detection of their operations. Raising standards across the board would then prevent criminals from "jurisdiction shopping" to exploit the weakest link.

Yet, such jurisdictions present a double-edged sword for money laundering, as there is often a correlation between weak regulatory environments and decreased economic stability. Those involved in money laundering may therefore prefer more stable financial environments that do not jeopardize access to their funds or where large-scale transactions are more common and thus unlikely to draw attention. The failure of major banks such as Danske Bank, HSBC, and BNP Paribas to implement proper AML controls within their institutions, as well as the corresponding fines, demonstrate that even well-established organizations can be vulnerable to exploitation by criminal actors.[a]

Terrorist organizations may similarly seek to utilize high-traffic channels, hoping that the sheer volume of transactions will create a "needle in a haystack" scenario that further obscures their activity. There is often correlation between areas with a terrorist presence and weak regulatory environments, but terrorism financing transactions are frequently transnational and may include the transfer of funds to and from well-regulated jurisdictions. Further, as terrorist operations become increasingly dispersed, so too has terrorism financing, which makes risk assessments centered solely on regulatory environments less instructive.

a See Peter Levring and Frances Schwartzkopff, "Danske Bank May Face $630 Million Fine, Danish Government Says," Bloomberg, 19 September 2018, https://www.bloomberg.com/news/articles/2018-09-19/danske-bank-may-face-630-million-fine-danish-government-says; Aruna Viswanatha and Brett Wolf, "HSBC to Pay $1.9 Billion U.S. Fine in Money-Laundering Case," Reuters, 11 December 2012, https://www.reuters.com/article/us-hsbc-probe/hsbc-to-pay-1-9-billion-u-s-fine-in-money-laundering-case-idUSBRE8BA05M20121211; "BNP Paribas Fined Over Weaknesses in Anti-Money Laundering Controls," Reuters, 2 June 2017, https://www.reuters.com/article/us-bnp-paribas-moneylaundering/bnp-paribas-fined-over-weaknesses-in-anti-money-laundering-controls-idUSKBN18T2JI.

terrorist activity. Some individuals knowingly finance terrorism, for instance, motivated by an opportunity for financial gain, coercion, and ideological or political sympathies. In those instances, terrorism financiers may adopt money laundering tactics to conceal the transactions and avoid detection.

Others may not be aware that they are supporting terrorism, such as an individual sending money to a family member who is, unknown to them, a foreign fighter or an individual unwittingly donating to a charity that supports terrorist activity. This was the case with the Liberation Tigers of Tamil Eelam (LTTE), which was designated as a terrorist organization by the European Union and a number of countries, including Canada, the United Kingdom, and the United States. Particularly prior to the 9/11 attacks, the LTTE was notorious for skimming contributions to legitimate nonprofits, nongovernmental organizations, and charities in Sri Lanka by the Tamil diaspora community. At its height, the LTTE was able to secure an estimated $2 million per month in this way.[17]

This potential for illegal and legal sources of funds, plus the increasingly small transaction values involved in terrorism financing, render it nearly impossible to blindly identify a terrorism financing transaction without the context that an in-depth investigation provides. As such, most CFT cases emerge as part of broader counterterrorism investigations led by

17 Peter Chalk, "The Tigers Abroad: How the LTTE Diaspora Supports the Conflict in Sri Lanka," *Georgetown Journal of International Affairs* 9, no. 2 (Summer/Fall 2008): 97–104, 101.

intelligence, military, or law enforcement agencies. On the other hand, money laundering is more likely to be detected by a mixture of public and private sector actors. For example, a skilled accountant who noted a discrepancy or unexplained wealth in a client's records is required to furnish the FIU with a written explanation of their suspicion. The FIU will analyze this report and disseminate it to the appropriate investigative authority.[18] In some cases, the same bodies have mandates for CFT and AML investigations. In others, there is a separation between criminal (money laundering) and intelligence (terrorism and terrorism financing) investigations. There can be further dispersion among money laundering investigations when the investigative authority is determined by the predicate offense (e.g., anticorruption agencies). Although the FIU should be the nucleus of these efforts, in practice, siloes often hinder holistic responses to illicit financial flows generally and money laundering and terrorism financing specifically.

BOLSTERING EFFORTS TO COUNTER TERRORISM FINANCING

In the wake of the 9/11 attacks, CFT efforts have yielded tangible results, leading to a significant investment of counterterrorism funding in CFT measures. There are generally four core objectives in combating terrorism financing: prevent, detect, freeze, and trace. For each of these, there are areas in which existing unified AML/CFT frameworks are working and areas in which more nuance is required to effectively combat threats specific to terrorism financing.

Prevent

The ultimate CFT goal is the prevention of terrorist attacks and operations, including by identifying operatives and financiers. Historical reliance on kinetic and largely reactive counterterrorism responses have been augmented by preventing and countering violent extremism (P/CVE) efforts, which target the human, or supply, side of terrorism by addressing the underlying drivers of radicalization and recruitment to violent extremism. Prevention in the CFT context refers to efforts to cut off the supply of resources needed for terrorist attacks and operations.

Curbing the source of terrorism financing is a moving target. States continue to be significant financiers of terrorism, and many organizations benefit from close state relationships. Terrorist organizations have also proven adept at generating their own revenue. For example, the Taliban collects significant funds from criminal enterprises, namely its facilitation of drug trafficking and other smuggling networks. Kidnapping for ransom has been profitable for criminal groups in Latin America[19] and has been adopted at various times as a fundraising strategy by the Euskadi Ta Askatasuna Basque separatist group,[20] Abu Sayyaf in the Philippines,[21] Al-Qaida in the Islamic Maghreb,[22] Al-Qaida in the Arabian Peninsula,[23] and Boko Haram.[24] ISIL received attention for its sale of oil, trade in antiquities, and extortion practices. Terrorist groups that control or occupy territory, such as al-Shabaab, have been known to collect resources from taxation, robbery, black markets, and aid misappropriation.

Across the board, terrorist organizations employ a mix of these tactics as suits their needs, opportunities, and strategic objectives. Terrorist organizations that

18 In some cases, FIUs have a mandate to partake in or lead these investigations directly.

19 Hostage US, "New Kidnapping Trends on the Global Stage," n.d., https://hostageus.org/new-kidnapping-trends-on-the-global-stage/.

20 Mikel Buesa and Thomas Baumert, "Dismantling Terrorists' Economics: The Case of ETA," Universidad Complutense de Madrid, January 2012, pp. 9–12, http://webs.ucm.es/info/cet/documentos%20trabajo/DT11CET_Dism_terr_eco_case_ETA.pdf.

21 James Hookway, "Terror Grows in Southern Philippines From Militants Linked to Islamic State," *Wall Street Journal*, 18 November 2016, https://www.wsj.com/articles/terror-grows-in-southern-philippines-from-militants-linked-to-islamic-state-1479465005; UN Security Council, "Letter Dated 16 July 2018 From the Chair of the Security Council Committee Pursuant to Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) Concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals and Entities Addressed to the President of the Security Council," S/2018/705, 27 July 2018 (containing report titled *Twenty-Second Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2368 (2017) Concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities*, para. 69) (hereinafter 2018 sanctions monitoring team report).

22 David Lewis, "Al Qaeda's Richest Faction Dominant in North Mali: U.S.," Reuters, 26 July 2012, https://www.reuters.com/article/us-mali-usa-africom-idUSBRE86P1IC20120726; 2018 sanctions monitoring team report, para. 36.

23 2018 sanctions monitoring team report, para. 26.

24 FATF, the Inter-Governmental Action Group Against Money Laundering in West Africa, and the Task Force on Money Laundering in Central Africa, *Terrorist Financing in West and Central Africa*, October 2016, p. 18, http://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-West-Central-Africa.pdf.

diversify their sources of income are better able to weather the loss of any one resource stream, at least in the short term. For example, ISIL, which had an estimated annual revenue of $2 billion in 2015, was able to continue operations after a sharp decline in their access to oil reserves and the resulting proceeds, due to other funding opportunities.[25] When forced to operate on leaner budgets, terrorist organizations can execute low-cost attacks that have a high impact. According to a study of terrorist cells that plotted or carried out attacks in western Europe between 1994 and 2013, 75 percent of terrorist attacks in Europe during that period cost less than $10,000 each.[26]

As terrorist groups are adept at evolving and diversifying their revenue generation tactics, CFT policymakers and practitioners must be mindful of the "balloon effect," in which constricting one source of funding leads to an expansion in another. A deeper understanding of the scale and diversification of terrorism funding portfolios would contribute to efforts to squeeze both ends of the balloon. The current knowledge base would benefit from increased quantitative information sharing and collaborative trend analysis among intelligence agencies and counterterrorism bodies, FIUs, law enforcement, economists, academics, practitioners, and policymakers.

Regardless, governments and policymakers cannot prevent terrorism financing without addressing the ideological appeal of terrorist groups. As long as terrorist groups are able to attract supporters, there is likely to be a readily available stream of resources, whether via direct contributions, social media fundraising campaigns, or the provision of material support and human capital in the form of terrorist fighters. To date, there appears to be little overlap between P/CVE and CFT interventions, which is a glaring gap in holistic responses to terrorism. To bridge that gap, policymakers should consider better mitigation of the unintended consequences of rigid CFT frameworks that exacerbate underlying drivers of violent extremism. For example, governments have used CFT laws as a justification to target political opposition, and financial institutions have dropped perceived high-risk clients because implementing the proper risk management measures would prove too costly or challenging. Because this has had negative effects on availability of civic space,[27] the ability of nonprofits to operate,[28] and financial access for marginalized communities, [29] financial policymakers could work with P/CVE practitioners to develop and enforce more balanced and human rights–adherent CFT regulations. Additionally, P/CVE efforts and actors would do well to engage more with the financial space, examining how socioeconomic mobility, financial literacy, and economic empowerment, i.e., the ability of individuals to contribute to and benefit from economic growth, can contribute to resilience to violent extremism.

Detect

A second core objective of CFT is the detection of terrorism financing. To do this, CFT frameworks borrow from existing AML and financial integrity controls intended to make criminal engagement with the financial system more complicated and risky. More than one-third of the FATF Recommendations focus on frontline compliance, which includes measures such as know your customer (KYC), customer due diligence (CDD), and record-keeping requirements.[30] As international standards, these recommendations require

25 Camilla Schippa, "This Is How Terrorists Finance Their Attacks," World Economic Forum, 15 November 2017, https://www.weforum.org/agenda/2017/11/terror-attacks-are-increasingly-self-funded-how-can-we-stop-them/.

26 Ibid.

27 Lana Baydas and Shannon N. Green, eds., "Counterterrorism Measures and Civil Society: Changing the Will, Finding the Way," Center for Strategic and International Studies, March 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180322_CounterterrorismMeasures.pdf?EeEWbuPwsYh1iE7HpnS2nPyMhev21qpw.

28 Sue E. Eckert, Kay Guinane, and Andrea Hall, "Financial Access for U.S. Nonprofits," Charity and Security Network, February 2017, https://www.charityandsecurity.org/system/files/FinancialAccessFullReport_2.21%20(2).pdf; "At the Intersection of Security and Regulation: Understanding the Drivers of 'De-Risking' and the Impact on Civil Society Organizations," Human Security Collective and European Center for Not-for-Profit Law, March 2018, https://www.hscollective.org/wp-content/uploads/2018/05/Understanding-the-Drivers-of-De-Risking-and-the-Impact-on-Civil-Society-Organizations_1.pdf.

29 Tracey Durner and Liat Shetret, "Understanding Bank De-risking and Its Effects on Financial Inclusion: An Exploratory Study," Oxfam and Global Center on Cooperative Security, November 2015, https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/rr-bank-de-risking-181115-en_0.pdf.

30 FATF Recommendations 9 through 23 are listed as "preventative measures." FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*, October 2018, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

reporting entities to collect information on the client, source of funds, and anticipated transaction patterns.

In addition to creating an obstacle and exposure risk for terrorism financiers, the information collected is extremely useful in investigating and prosecuting terrorist networks and individuals. Information collected via compliance obligations can often provide the missing link in an ongoing investigation, placing an individual in a particular location to make a transaction, uncovering aliases, or establishing patterns of unexplained behavior that may be attributed to criminal activity. Financial information and intelligence also can be a key source of evidence to support successful terrorism or terrorism financing prosecutions.

Financial institutions and other reporting entities do more than just collect information. They also must submit reports when a transaction might be related to criminal or terrorism-related activity or organizations. FATF Recommendations 20 and 21 relate to reporting suspicious transactions, which in the United States is considered "the cornerstone of the BSA reporting system."[31]

In practice, suspicious transaction reports (STRs) have become a method by which the private sector can demonstrate compliance with AML and CFT laws. In 2003 the U.S. Financial Crimes Enforcement Network (FinCEN), the U.S. FIU, coined the term "defensive filing," referring to reports that were submitted to protect an institution rather than due to genuine concern. Then-FinCEN Director William J. Fox argued that

> if institutions begin to believe that they will routinely be targeted for criminal investigation and prosecution for failure to properly implement the [BSA] regulatory regime, it is natural that institutions will take all steps necessary to ensure they are protected from such risk. It is not a large leap to understand why institutions are beginning to report on any transaction that is at all unusual, even if it is not necessarily suspicious as that term has been defined by our regulations.[32]

The number of reports filed in the United States has almost doubled in the last 10 years, breaking the two-million mark in 2017.[33] There have been similarly drastic increases in reporting around the world. The UK FIU receives an average of roughly 1,650 reports per working day and recorded a 38 percent annual increase in reports filed from October 2016 to September 2017.[34] The Australian FIU reported a 70 percent increase in suspicious matter reports over a similar 12-month period.[35]

Underpinning effective reporting is an understanding of typologies and "red flags" for terrorism financing transactions. Red flags for terrorism financing might be as general as an unsatisfactory explanation for a significant transaction inconsistent with the account holder's typical activity or as specific as numerous ATM cash withdrawals in high-risk areas for terrorism activity, such as near the Syrian border. The Canadian FIU notes, "[A] suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both."[36]

According to the Association of Certified Anti-Money Laundering Specialists (ACAMS), "Developing terrorist financing typologies for anti-money laundering programs requires understanding. You must understand the terrorist threat environment, emerging

31 U.S. Federal Financial Institutions Examination Council, "Suspicious Activity Reporting—Overview," n.d., https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_015.htm (accessed 27 December 2018).

32 William J. Fox, remarks provided to the American Bankers Association at the American Bar Association Money Laundering Enforcement Seminar, Arlington, Virginia, 25 October 2004, https://www.fincen.gov/news/speeches/remarks-william-j-fox-director-financial-crimes-enforcement-network-united-states-0.

33 The period was July 2016 to June 2017. FinCEN, "Suspicious Activity Report Statistics (SAR Stats)," https://www.fincen.gov/reports/sar-stats (accessed 24 October 2018).

34 UK National Crime Agency, "Suspicious Activity Reports (SARs): Annual Report 2017," n.d., p. 6, http://www.nationalcrimeagency.gov.uk/publications/826-suspicious-activity-reports-annual-report-2017/file.

35 AUSTRAC for the Commonwealth of Australia, "AUSTRAC Annual Report 2017–18," 4 October 2016, p. 7, http://www.austrac.gov.au/sites/default/files/AUSTRAC_annual_report_2017-18.pdf.

36 Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), "Guideline 2: Suspicious Transactions," June 2017, http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp?wbdisable=true#s6.

terrorist trends, the funding flows terrorists rely on to sustain their operations and your institutional risk for being used to facilitate terrorist funding flows."[37] Although entities such as the Egmont Group of Financial Intelligence Units have published lists of financial and behavioral indicators for terrorism financing, identifying these red flags can still be a daunting task for many private sector companies unfamiliar with the terrorism landscape, specifically those that facilitate transactions for dozens or hundreds of jurisdictions around the world. Terrorism financing accounted for just 0.1 percent of STRs filed in the United States in 2017, a percentage that has held fairly constant in recent years.[38] In the United Kingdom, just 1,414 of the 419,451 reports received between October 2015 and September 2016 were related to terrorism finance (0.3 percent).[39]

Where reporting is most likely to be effective relative to terrorism financing are instances that involve well-established and well-organized terrorist groups. In those instances, organizations seek to manage and sustain operational expenses and function more like traditional criminal networks for which AML policies were originally developed. They need to move funds without detection, but also store assets and even maximize revenue generation from investments. Existing AML procedures are relevant in these cases, as the scale of funding is likely to approach that which organized crime networks are seeking to launder. Understanding the beneficial ownership structures, shedding light on offshore banking practices, investigating shell companies, and combating the unrecorded cross-border movement of assets can prove instructive in addressing or at least identifying terrorism financing of this scale.[40]

Where current frontline and reporting measures, such as KYC, CDD, and reporting obligations, may not be as successful are the direct transfers of funds to and among potential or suspected terrorist operatives. Transactions can be sourced from legal income and are often too small to attract attention, making them virtually impossible to distinguish and highly unlikely to be flagged in an STR. Further, terrorist attacks increasingly involve expenditures that appear innocuous when made separately and examined in a vacuum, such as a vehicle rental or everyday-item purchases such as batteries, alarm clocks, and plastic bottles.[41]

In most instances, terrorism financing is only detected once the suspect is known or after an attack. Of terrorism financing–related reports submitted in the United States in 2017, 73 percent were associated with known or suspected terrorists.[42] According to ACAMS, "It is possible to identify terrorism financing preemptively, but the likelihood is not probable until after a terrorist event takes place. We normally identify terrorist financing reactively, after the fact, through negative news. Our challenge is to improve the likelihood and thereby increase the probability of identifying suspicious activity before that activity evolves into a terrorist event."[43]

As terrorists have adapted their methodologies, so too must those charged with combating terrorism and its financing update and revise the red flags for potential terrorist activity. The unique operational expenses of modern terrorist organizations provide new and different opportunities for detection by those in the financial sector. Such transactions could include life insurance policies with provisions for coverage in areas where terrorist groups are known to be active,

37 Dennis M. Lormel, "Developing Terrorist Financing Typologies for AML Programs," *ACAMS Today*, 6 March 2017, https://www.acamstoday.org/developing-terrorist-financing-typologies-for-aml-programs/.

38 FinCEN, "Suspicious Activity Report Statistics (SAR Stats)" (accessed 24 October 2018).

39 UK National Crime Agency, "Suspicious Activity Reports (SARs)," pp. 6, 54.

40 An example of AML inquiries being used to identify actors and entities affiliated with terrorism and terrorism financing can be found in the real estate sector in the United Arab Emirates. A 2018 report notes that the Khanani Money Laundering Organization, a Pakistani entity sanctioned by the United States for laundering money for terrorist groups including al-Qaida and the Taliban, had maintained investments in real estate properties in the UAE. Per the report, these multimillion-dollar real estate holdings, along with links to unsanctioned companies in Pakistan, the United States, the United Kingdom, and the UAE, "suggest that the network maintains at least some of the infrastructure required to conduct illicit finance." C4ADS, "Sandcastles: Tracing Sanctions Evasion Through Dubai's Luxury Real Estate Market," 2018, pp. 27–31, https://static1.squarespace.com/static/58831f2459cc684854aa3718/t/5b1fd4bf575d1ff600587770/1528812745821/Sandcastles.pdf.

41 These items were purchased to carry out recent terrorist attacks. See Neumann, "Don't Follow the Money"; Dina Temple-Raston, "How Much Does a Terrorist Attack Cost? A Lot Less Than You Think," NPR, 25 June 2014, https://www.npr.org/sections/parallels/2014/06/25/325240653/how-much-does-a-terrorist-attack-cost-a-lot-less-than-you-think.

42 FinCEN, "Suspicious Activity Report Statistics (SAR Stats)" (accessed 24 October 2018).

43 Lormel, "Developing Terrorist Financing Typologies for AML Programs."

unusual periods of account dormancy and reactivation, or transactions that indicate a liquidation of all personal property and assets. Development of these red flags must prioritize human rights considerations, in particular privacy and data protections; and actions taken in response by financial institutions, such as account closures, should be rooted in context-specific evidence. Red-flag transactions do not inherently reflect affiliation with terrorism, and the parameters of further investigation should be clearly regulated by law, including the powers of appropriate authorities, oversight mechanisms, and means of recourse. Investigators should seek corroborating information and intelligence from other sources before making a determination about potential criminality.

Even with improved indicators, one must remain realistic about the limitations of reporting in proactively identifying instances of terrorism financing. There is a perception that reporting will lead to the interception of assets intended to facilitate an impending terrorist attack. Although this should remain the ultimate goal, the intrinsic value of the information that is collected from frontline compliance and reporting obligations should not be overlooked. Financial intelligence is a critical link within the criminal justice chain. Collectively, this information creates a rich database that can be mined by investigators to uncover connections between terrorist networks, as well as used to secure successful prosecutions for terrorism and terrorism financing offenses.

Existing data collection procedures may be augmented in instances of suspected terrorism financing. Current FATF standards require enhanced due diligence for transactions with jurisdictions considered high risk for money laundering or terrorism financing, as well as for those conducted by political officials to combat corruption.[44] In combination with more nuanced red-flag indicators, enhanced due diligence guidelines could be developed specific to potential instances of terrorism financing, including encouraging expanded transaction monitoring procedures. These guidelines would benefit from collaborative development among regulators, financial sectors, law enforcement, and counterterrorism bodies to ensure proper calibration among information collection, confidentiality, and overly burdensome compliance procedures. They must be drafted in close consultation with data privacy and consumer protection experts to ensure they are in line with the rule of law and compliant with national and international human rights obligations.

Freeze

The ability to freeze assets under international sanctions regimes is a core tool in combating terrorism financing. According to the UN Security Council Counter-Terrorism Committee (CTC), "The freezing of terrorist assets is a highly effective way for Member States to stem the flow of funds. It can also act as a deterrent to further engagement in terrorist activity."[45]

Economic sanctions, including trade bans and embargoes, were used as a punitive measure against state sponsors of terrorism. Questions remain regarding the extent to which these sanctions have resulted in a significant reduction in the scale of terrorism financing from state actors,[46] although they have been shown to have negative humanitarian consequences.[47] UN Security Council Resolution 1373 reflected a shift to organization- and individual-level designations and devolved terrorism financing sanctions regimes to member states. FATF Recommendation 6 on targeted financial sanctions related to terrorism and terrorism financing further reinforces this shift.[48]

Following the adoption of Resolution 1373, 166 countries and jurisdictions issued orders freezing approximately $112 million in terrorist assets in just

44 FATF Recommendation 19 indicates that enhanced due diligence should be applied to countries determined by FATF to be at higher risk for money laundering and terrorism financing activities, while Recommendation 12 addressed additional measures when handling transactions for politically exposed persons.

45 CTC, "Terrorism Financing," n.d, https://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/ (accessed 10 December 2018).

46 Gary Clyde Hufbauer, Jeffery J. Schott, and Barbara Oegg, "Using Sanctions to Fight Terrorism," *Peterson Institute for International Economics Policy Brief*, no. 01-11 (November 2011), https://piie.com/publications/policy-briefs/using-sanctions-fight-terrorism.

47 Working Group 3, High Level Review of UN Sanctions, "UN Sanctions: Humanitarian Aspects and Emerging Challenges; Chairperson's Report," 19 January 2015, http://www.hlr-unsanctions.org/HLR_WG3_report_final.19.1.15.pdf.

48 FATF Recommendation 7 addresses financial sanctions related to proliferation of weapons of mass destruction.

three months.[49] In the 18 months that followed, an additional $80 million was seized.[50] Following this initial success, the scale of asset freezing declined significantly. Further, despite global participation, the United States and three other countries were responsible for approximately two-thirds of the assets frozen during September–December 2001.[51]

Timing is a critical element in the effectiveness of financial sanctions. National laws differ regarding the use of judicial and administrative procedures to implement domestic asset-freezing procedures. Within the UN framework, asset-freezing mechanisms are triggered when an individual or entity is designated, or listed, under the criteria of each sanctions regime. As such, designation is inherently reactive, coming into effect only when the person to target is known. Further, UN designations are a public record.[52] Assets must be frozen immediately after an individual is listed to avoid circumvention by simply withdrawing or transferring funds to an untraceable account. In practice, the complex process of disseminating the list from the United Nations to individual banks often means the actual asset freeze is delayed.

According to FATF, "Measures to freeze terrorist funds or other assets may complement criminal proceedings against a designated person or entity, but are not conditional upon the existence of such proceedings."[53] Although intended to allow the freezing of assets of suspects who have not been arrested, the effect on the human rights of the individual suspects must be considered. This includes potential infringement on their rights to privacy, property, and a fair trial. Public designation also can significantly limit individuals' ability to travel and gain or maintain employment and financial access. Those listed on the UN Security Council's ISIL (Da'esh) and Al-Qaida Sanctions List can submit delisting requests to the Office of the Ombudsperson to the ISIL (Da'esh) and Al-Qaida Sanctions Committee. The ombudsperson is an impartial and independent arbitrator who considers these requests via a formal process and then makes a recommendation to the committee on whether to delist or retain an individual or entity on the list.[54] This process can be a lengthy one, typically ranging between eight and 16 months.[55]

Avenues to challenge domestic designation vary, and in some cases, domestic designation has been used to target political opposition. Further, there are practical considerations for individuals who may suffer from mistaken identity (e.g., similar but not identical names) or have the unfortunate luck of sharing a name with someone convicted of a terrorist offense or listed on a terrorism watch list.[56]

Despite these challenges, designation under a sanctions regime remains one of the core tools in combating terrorism financing, particularly given the international reach of UN designations. The UN Security Council Counter-Terrorism Committee Executive Directorate (CTED) is tasked with assessing the effective implementation of terrorism and nonproliferation financing regimes by member states. In its most recent report, CTED notes the level of state compliance remains "inadequate" and lists "many challenges faced by Member States in their efforts to establish and implement an effective freezing mechanism that is consistent with the relevant international standards

49 UN Security Council, "Letter Dated 19 September 2002 From the Chairman of the Security Council Committee Established Pursuant to Resolution 1267 (1999) Concerning Afghanistan Addressed to the President of the Security Council," S/2002/1050, 20 September 2002, pp. 9–10 (containing report titled *Second Report of the Monitoring Group Established Pursuant to Security Council Resolution 1363 (2001) and Extended by Resolution 1390 (2002)*).

50 Office of Public Affairs, U.S. Department of the Treasury, "Testimony of Samuel W. Bodman, Deputy Secretary U.S. Department of Treasury Before the Senate Committee on Banking, Housing and Urban Affairs," js1501, April 29, 2004, https://www.treasury.gov/press-center/press-releases/Pages/js1501.aspx.

51 Rensselaer Lee, "Terrorist Financing: The U.S. and International Response," *CRS Report for Congress*, RL31658, 6 December 2002, p. 2, https://burgess.house.gov/uploadedfiles/wot%20-%20terrorist%20financing%20the%20u.s.%20and%20international%20response.pdf.

52 For the designation list, see UN Security Council Subsidiary Organs, "Consolidated United Nations Security Council Sanctions List," n.d., https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list (accessed 27 December 2018).

53 FATF, *International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)*, June 2013, p. 6, http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP-Fin-Sanctions-TF-R6.pdf.

54 UN Office of the Ombudsperson of the Security Council's 1267 Committee, "The Office of the Ombudsperson to the ISIL (Da'esh) and Al-Qaida Sanctions Committee," n.d., https://www.un.org/securitycouncil/ombudsperson (accessed 30 December 2018).

55 "Procedure for Requests for Delisting Submitted to the Office of the Ombudsperson (S.C. Resolution 2368 (2017))," n.d., https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/procedure_chart.pdf.

56 Elena Servettaz, "A Sanctions Primer: What Happens to the Targeted," World Affairs, July/August 2014, http://www.worldaffairsjournal.org/article/sanctions-primer-what-happens-targeted.

and human rights obligations. Many Member States have developed domestic asset-freezing mechanisms, but their use remains limited."[57] There is need to invest in further capacity development to strengthen the ability of states to meaningfully meet the requirement to freeze "without delay" and to increase the number and diversity of states that are contributing to designations while ensuring adequate human rights protections.

Trace

"Follow the money" principles have been at the core of complex criminal investigations for decades. Tracing transactions and monitoring financial flows can similarly uncover terrorist operatives, facilitators, and their associated networks.

Under FATF Recommendation 32, law enforcement agencies should "develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing." The word "parallel" is important; per international standards, there is or should be no terrorism investigation that does not include a CFT investigation. As noted, information gathered by the financial sector as part of routine compliance measures helps investigators connect individuals or pieces of intelligence to uncover a fuller picture of the extent and breadth of terrorist operations. It provides a key source of evidence for use in the prosecution of terrorism cases, particularly in instances where suspects have not been charged or arrested in relation to a specific attack (e.g., a suspected foreign fighter).

Traditional mechanisms for tracing monetary flows often involve monitoring transactions over time, which can be politically unpalatable regarding terrorism financing. Once a terrorist suspect is identified, freezing or intercepting the funds immediately to prevent an attack is desirable. Doing so, however, will alert the individual that they have been identified as affiliated with terrorism, likely forcing them underground and ending the flow of information and intelligence.

In most countries, suspicious transaction regulations support follow-the-money objectives, including by not requiring reporting entities to halt or reject transactions and strictly prohibiting them from informing the client that an STR is being filed. Yet, increased enforcement actions related to inadequate AML frameworks are having a trickle-down effect on CFT intelligence gathering, given the unification of AML and CFT policies.

Globally, AML enforcement continues to grow at record pace. For example, the number of AML and CFT fines imposed by U.S. regulators increased 65 percent during 2010–2015, and fines rose from $161 million to more than $2.6 billion.[58] Regulators insist fines are levied only in cases where egregious and sustained offenses have occurred, but a bank may be sanctioned even when there is no evidence of criminal or terrorist activity in its ledgers. The outcome arguably has been an increasingly risk-averse financial system, as underscored by the trend of de-risking, in which financial institutions deny or close the accounts of perceived high-risk clients rather than develop effective mitigation measures.[59] This particularly impacts low-profit clients for banks, which are often already members of marginalized communities.

Beyond financial exclusion challenges, risk aversion in the financial sector affects abilities to meaningfully trace terrorism financing. As U.S. Comptroller of the Currency Thomas J. Curry said, "Transactions that would have taken place legally and transparently may be driven underground."[60] When banks deny or close accounts to avoid assuming risk, law enforcement loses all visibility into the transactions. It is a significant loss of intelligence for counterterrorism agencies in the monitoring of known actors and as one piece of information in broader trend identification and analysis on terrorism financing typologies.

Existing international standards focus on criminalizing terrorism financing as a stand-alone offense. It is critical that equal prioritization be given to the collection of financial intelligence as a tool for proactive terrorism investigations. As asserted by the FATF president in a 2017 briefing to the CTC, "Regardless

57 CTED, "Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States," S/2016/49, 20 January 2016, p. 114.

58 Clay Lowery and Vijaya Ramachandran, "Unintended Consequences of AML Policies," *Banking Perspectives* 4, no. 3 (3rd quarter, 2016): 54–60.

59 Durner and Shetret, "Understanding Bank De-risking and Its Effects on Financial Inclusion."

60 Thomas J. Curry, remarks before the Institute of International Bankers, Washington, DC, March 7, 2016, https://www.occ.treas.gov/news-issuances/speeches/2016/pub-speech-2016-25.pdf.

of their size and complexity, the financial activities and channels of terrorists are an essential source of intelligence. Financial investigation can identify terrorist cells, their associates and facilitators, and reveal the structure of terrorist groups, and their logistics and facilitation networks."[61]

To facilitate the gathering of financial information, private sector actors should be given or be assured they have the legal and operational space to serve as meaningful partners to law enforcement and intelligence networks. This includes reflecting on the calibration of regulatory enforcement actions and its effect on financial transparency related to CFT. Doing so represents a needed shift in the mentality of regulators, who increasingly see financial institutions as responsible for conducting the type of financial analysis that was historically the responsibility of law enforcement and intelligence agencies. It will also require a change in financial institutions' perceptions of and approach toward their compliance obligations. For example, the significant investments being made in compliance department staffing might be better spent on transaction monitoring capacities, data mining and information technologies, or enhanced risk-rating and management systems. Governmental actors and regulators can support this effort through policy guidance on assessment of and response to terrorism financing risks, as well as awareness raising on the use of STRs and other requests for information to support broader intelligence and counterterrorism efforts.

CONCLUSION AND RECOMMENDATIONS

Significant progress has been made to combat terrorism financing in the last two decades. The international standards provided through the FATF Recommendations and UN Security Council resolutions provide a strong, universal, and measurable framework against which to consider efforts to combat illicit and terrorism financing. The World Bank and the International Monetary Fund have provided standardized procedures for assessing national risk for money laundering and terrorism financing, and FATF deploys a universal methodology to assess compliance with its recommendations, enabling a comparative understanding of the status of AML and CFT globally. Further, the outcomes of FATF assessments and, in many cases, national risk assessments are public documents, in contrast to the classified outputs associated with the majority of counterterrorism efforts. The recent shift of FATF to focus on effective implementation in addition to mere technical compliance is poised to push significant advancements in the ability of developing AML and CFT regimes around the world to effectively identify and combat financial crimes.

There remains one clear issue with AML and CFT frameworks: they center on the formal financial system. The primacy of the formal sector is not universal in countries around the world, especially not in countries that experience the brunt of terrorist activity or operations. In those areas, so-called informal financial systems are the cornerstone of economic activity. Cash remains king due to low bank-penetration rates and weak institutional trust. Fitting the informal sector into the existing regulatory system is not the answer to improving the effectiveness of CFT measures.

Instead, creative thinking is required to build a regulatory structure focused on and specific to the informal sector. The informal financial sector should be used as the starting point and foundation on which regulatory frameworks are built. Such frameworks would do well to consider the potential technical jump that is offered by emerging mobile money and digital currency technologies.

As outlined above, there is a need for further refinement of CFT policies separate from existing AML policies. This is not a call to roll back existing AML and CFT frameworks but rather an appeal to augment them with CFT-specific policies and strategies that reflect the dynamic landscape of terrorism and terrorism financing today. From the perspective of international security assistance, this may also mean untangling the marriage of convenience of AML and CFT that has allowed donors to concurrently address development and counterterrorism objectives. Where possible, separate CFT interventions should be developed to support the institutions that have counterterrorism responsibilities, such as law enforcement and military agencies, as well as counterterrorism-adjacent entities such as intelligence and judicial bodies. Within the context of programs that combat

61 Santiago Otamendi, remarks to the CTC, 14 December 2017, https://www.fatf-gafi.org/publications/fatfgeneral/documents/briefing-otamendi-unctc-dec2017.html.

financial crime or illicit financial flows more broadly, engaging all AML and CFT actors to promote coordination is important to avoid the lack of information sharing that has been a pitfall for many terrorism financing cases.[62] To this end, the following recommendations are offered to the relevant actors.

Regulators and the financial sector

Bolster efforts to address terrorism financing as a specific crime, including the ongoing work by FATF and others to enhance detection mechanisms.

- Update and develop red-flag indicators for different reporting entities specific to terrorism financing transactions.[63]
- Explore potential applicability of enhanced due diligence measures to advance financial information gathering in support of terrorism investigations and prosecutions.
- Develop capacity on terrorism and terrorism financing for risk management teams and compliance managers.
- Establish public-private partnerships to enhance information technology solutions to risk assessments for terrorism financing.

National CFT regimes

Support reporting entities in CFT recognition and monitoring capacities while acknowledging the reality that identifying terrorism financing is like finding a "needle in a haystack."

- Promote the recruitment and hiring of dedicated forensic accountants by investigative authorities.
- Invest in enhanced transaction monitoring capacities, including the use of data mining and information technology, in line with necessary private and information security objectives.
- Develop and refine matrices relative to terrorism financing vulnerabilities and risks at the national level based on findings from national risk assessments on money laundering and terrorism financing and mutual evaluation and follow-up report processes.
- Recalibrate the regulatory framework for reporting entities to prioritize the collection of financial information.

Member states

Continue efforts to combat revenue generation by terrorist organizations.

- Support military–law enforcement cooperation and intelligence sharing to identify, investigate, and disrupt illegal revenue generation by terrorist organizations.
- Bolster multi-stakeholder analysis and collection of quantitative data to retain a dynamic understanding of terrorist revenue streams in order to constrict both ends of the balloon.
- Align CFT efforts with parallel P/CVE interventions to reduce the ideological support for terrorist organizations and the flow of resources from supporters.

UN counterterrorism-adjacent entities

Enhance effectiveness of existing financial sanctions and asset-freezing mechanisms related to terrorism and terrorism financing.

- Provide capacity development assistance to jurisdictions for effectively meeting FATF and UN standards on financial sanctions and asset freezing without delay.
- Support UN member states in preparing and submitting designations under UN sanctions regimes to ensure a broad and diverse range of contributions.
- Publish data on the effectiveness of asset-freezing measures, including case studies on the deployment of asset freezes to successfully advance criminal prosecutions or thwart attacks.

62 For further guidance on the convergence and divergence of money laundering and terrorism financing efforts, see Tracey Durner and Danielle Cotter, "Combating Money Laundering and Terrorism Financing: Good Practices for AML/CFT Capacity Development Programs," Global Center on Cooperative Security, September 2018, pp. 4–6, https://www.globalcenter.org/wp-content/uploads/2018/09/GC_2018-Sept_Combating-Money.pdf.

63 For examples, see FINTRAC, "Guideline 2: Suspicious Transactions."

ABOUT THE AUTHORS

Tracey Durner

Tracey Durner is a Senior Analyst for the Global Center on Cooperative Security. She specializes in financial inclusion issues, including anti–money laundering (AML), countering the financing of terrorism (CFT), and bank de-risking. Focusing on the Greater Horn of Africa region in particular, she has coauthored reports on countering violent extremism and AML and CFT topics and assisted in the design and implementation of regional capacity-building programs. She holds a BA in international affairs and political science from Northeastern University.

Danielle Cotter

Danielle Cotter is a Senior Analyst for the Global Center. She focuses on research and programming related to anti–money laundering (AML) and countering the financing of terrorism (CFT), particularly in the Greater Horn of Africa and the Middle East and North Africa regions. She has coauthored reports on AML, CFT, and countering violent extremism issues and works on capacity-building programs with a focus on developing economies. She holds a BA in international relations with an East Asia focus from Tufts University.

ACKNOWLEDGMENTS

The Global Center on Cooperative Security gratefully acknowledges the support for this policy brief provided by the government of Norway. The authors recognize the contributions of Neil Bennett, Shaun McLeary, Eelco Kessels, Melissa Lefas, and Jason Ipe.

The views expressed are those of the authors and do not necessarily reflect the views of the Global Center, its advisory council, or the government of Norway.

SUGGESTED CITATION: Tracey Durner and Danielle Cotter, "Untangling a Marriage of Convenience: Anti-Money Laundering and Countering the Financing of Terrorism," Global Center on Cooperative Security, January 2019.

This version contains a correction.

ABOUT THE GLOBAL CENTER

The Global Center on Cooperative Security works with governments, international organizations, and civil society to develop and implement comprehensive and sustainable responses to complex international security challenges through collaborative policy research, context-sensitive programming, and capacity development. In collaboration with a global network of expert practitioners and partner organizations, the Global Center fosters stronger multilateral partnerships and convenes key stakeholders to support integrated and inclusive security policies across national, regional, and global levels.

GLOBAL CENTER ON COOPERATIVE SECURITY

globalcenter.org
@GlobalCtr

NORWEGIAN MINISTRY OF FOREIGN AFFAIRS

© 2019 Global Center on Cooperative Security
All rights reserved.
For permission requests, write to the publisher at:
1101 14th St. NW, Ste. 900
Washington, DC 20005
Design: Studio You London