K4D | Knowledge, evidence and learning for development

Effectiveness of Different Methods to the Counter Financing of Terrorism

Iffat Idris
GSDRC, University of Birmingham
29 April 2022

Question

What is the effectiveness of the different methods to counter the financing of terrorism (CFT)?

Contents

1. Summary

Countering financing of terrorism (CFT) has been a core component of counter terrorism strategies since the 9/11 attacks on the US in 2001. Key CFT measures are criminalisation of terrorism financing; sanctions and assets freezing/seizure; and use of financial intelligence. CFT assessments focus on implementation of these measures, rather than on impact in terms of preventing terrorist activity. The limited literature on the latter suggests that, while CFT measures can hamper terrorists/terrorist groups, they cannot stop them entirely. Despite this, CFT remains a useful tool for governments in the fight against terrorism/their efforts to counter terrorism. However, the current CFT model needs to be reformed to address significant changes in both the terrorist threat and terrorism financing environment.

This rapid review looks at the effectiveness of different CFT measures. It draws on a mixture of academic and grey literature, including policy papers and reports from agencies involved in CFT implementation. While there is available literature on terrorism financing (how groups raise funds), and on the various approaches to CFT as well as implementation assessment, the review found very little on the impact of CFT in preventing terrorism. Reflecting this, it was also difficult to identify specific examples of CFT impact and effectiveness. The examples that were found are mentioned in section 5 of this review.

Key findings of the rapid review are as follows:

- **Terrorist activity is dependent on individuals/groups having the funds and resources to plan and carry out attacks, and to sustain themselves.** Terrorism financing can come from both licit and illicit sources, and entails raising, moving, storage, managing and obscuring funds. Cutting off funds is an important counter-terrorism strategy, and was especially prioritised in the wake of the 9/11 attacks in the United States.
- **Countering financing of terrorism (CFT) involves a range of measures**, key among which are criminalisation of terrorism financing, sanctions and asset freezing/seizure, and use of financial intelligence. A body of UN Security Council Resolutions, international conventions, and national legislation/regulations, as well as Financial Action Task Force (FATF) recommendations and standards make up the CFT framework.
    - **Criminalisation of terrorist financing** - entails banning all transactions with individuals or groups who commit, threaten or support terrorism. The 9/11 attacks led to this being established in the US as well as through UN resolutions, and mobilised other countries to follow suit. With a small number of exceptions, terrorist financing is now globally criminalised. However, a smaller proportion of countries have substantial or high levels of effectiveness in investigating and prosecuting terrorism finance offences.
    - **Sanctions and asset freezing/seizure** – these are often called for through UNSC resolutions and can be against individuals, groups or even states; countries are supposed to implement these without delay. They can be wide-ranging, e.g. economic sanctions, arms embargoes, travel bans, and freezing bank accounts. Evidence on effectiveness of sanctions is weak, but suggests they can do little to bring about significant policy changes, though they can constrain (make it harder) for those targeted to carry out activities. A further problem is that application of terrorism related sanctions

and asset freezing/confiscation requirements by countries is not sufficient, with frequent delays.

  - **Financial intelligence** – this refers to the collection and analysis of financial flows and transactions in order to identify activity related to terrorist financing or money laundering. It is carried out by financial intelligence units (FIUs) working in partnership with private sector entities such as banks, which must report suspicious transactions. While some argue that the full potential of financial intelligence to prevent terrorism is not being realised, there are significant difficulties, most notably that terrorism financing transactions form a tiny proportion of suspicious activity (most is money laundering, fraud, financial crime), and can be very hard to identify.

- **CFT effectiveness is primarily assessed using FATF standards** – the FATF expanded its money laundering mandate in 1989 to include CFT. It has produced a list of 40+9 recommendations covering both anti-money laundering (AML) and CFT, and provides guidance to member states on implementing these. The FATF also assesses implementation, based on 11 immediate outcomes that it has identified as resulting from an effective AML/CFT framework.
- **Lack of CFT impact assessment** – The FATF assessment has come under criticism for its focus on outputs and outcomes (essentially processes) rather than on impact in terms of preventing terrorism. However, there is acknowledgement that this is difficult to assess for several reasons, including lack of information (e.g. about terrorist attacks prevented) and challenges in establishing causality between CFT and prevention.
- **The current CFT framework has shortcomings** – even with the lack of impact assessment, the literature points to significant flaws in the current CFT framework, which was set up in the wake of the 9/11 attacks largely to stop transfer of funds to Al-Qaeda. Since then the terrorist threat has changed (with both larger, territory-controlling groups such as Al-Shabaab, and more lone operators) and also terrorism financing (less reliance on formal financial system, new funding sources and payment systems). While the basic CFT elements, such as criminalisation of terrorism financing, should be retained, reforms are needed to address the new terrorism and finance environment.
- **Examples of success that this review found make use of different CFT measures**: a) actions by the US to thwart cyber campaigns by Al-Qassam Brigades, ISIS and Al-Qaeda; b) efforts to stop ISIS financing by cutting the group off from its funding sources, and denying it access to the global financial system; and c) the Terrorist Finance Tracking Programme (TFTP) which has been a highly powerful and effective financial intelligence tool for CFT.

The evidence on CFT measures, assessment and impact was found to be both ‘gender-blind’ and ‘disability-blind'.

2. Methods to counter financing of terrorism

Terrorist financing

Terrorists (individuals or groups) need funds, e.g. for weapons and equipment, travel, accommodation, training, salaries, logistics and to sustain themselves in order to plan and carry out their attacks. Terrorist financing is defined as ‘the solicitation, collection or provision of funds

with the intention that they may be used to support terrorist acts or organisations'.[1] Terrorist financing thus involves raising, moving, storing, managing and obscuring funds. Funds can come from both licit and illicit sources. Davis (2020) identifies the following common sources of terrorist financing: i) state sponsors (e.g. Iran's support for Hezbollah); ii) wealthy donors; iii) other terrorist groups (e.g. support from Al-Qaeda to its affiliates); and iv) self-financing by raising funds through licit (e.g. profits from businesses, charitable organisations) and illicit sources (e.g. drugs and arms trafficking, extortion, human trafficking, kidnapping for ransom, burglary). One estimate puts the annual income of the world's richest terror groups at more than USD 3.6 billion, with Hezbollah's USD 1.1 billion being the highest.[2]

Countering the financing of terrorism (CFT) is therefore a vital component of counter-terrorism strategies. The Financial Action Task Force (FATF) explains that, '[d]isrupting and preventing these terrorism-related financial flows is one of the most effective ways to fight terrorism. Not only can it prevent future attacks by disrupting their material support, the footprints of their purchases, withdrawals and other financial transactions can provide valuable information for ongoing investigations'.[3] CFT deprives terrorist groups of the means to conduct terrorist acts, based on the idea that 'money is the oxygen of terrorism' (Parker & Taylor, 2010, cited in Brzoska, 2011: 7). Key CFT measures are described below.

Criminalisation of terrorist financing

Criminalisation of terrorist financing is the first step in CFT. This has been done through a body of international conventions, which are supposed to be translated into national legislation in individual countries. Most significant in this regard is the 1999 UN International Convention for the Suppression of the Financing of Terrorism, which entered into force in April 2002. As well as criminalising financing of terrorism, the Convention calls for the freezing and seizure of funds (Davis, 2020: 472).

The 9/11 attacks in the United States were followed on 25 September 2001 with Executive Order 13224 issued by President Bush. This blocked property and banned transactions with individuals who commit, threaten or support terrorism. It also set up a list of banned individuals, which is maintained by the Office of Foreign Assets Control (OFAC). Equally important, Bush's Executive Order mobilised other countries and multilateral organisations to implement similar CFT measures. On 28 September 2001 UN Security Council Resolution 1373 was passed, requiring member states to build their capacity to combat terrorism, including countering financing of terrorism (Davis, 2020: 472).

There had been strong European resistance to introducing controls on financial transfers and assets, as called for in the 1999 UN International Convention for the Suppression of the Financing of Terrorism (Brzoska, 2011). However, this dissipated after the 9/11 attacks in the US, and a further push for action in Europe came from the July 2005 terrorist attacks in London. Three months later the Council of Europe adapted its Convention 141 to criminalise terrorist financing. The EU adopted a Directive on the Prevention of the Use of the Financial System for

[1] https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm
[2] https://www.dowjones.com/professional/risk/glossary/financial-crime/counter-terrorist-financing/
[3] https://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html

the Purpose of Money Laundering and Terrorist Financing, which largely repeated the FATF standards (see below) (Brzoska, 2011).

The vast majority of countries have passed legislation criminalising terrorism financing. The FATF's latest report on effectiveness and compliance with FATF standards (see below), found that '90% of Global Network countries have criminalised terrorist financing in line with the FATF's requirements (which include supporting organisations)' (FATFb, 2022b: 43). However, in many ways, this is the easy part. In order to be effective, criminalisation has to be followed by enforcement, investigation and prosecution of those suspected of involvement in terrorism financing. The record on this is less impressive. The FATF (2022b: 43) found that. 'Over 70% of all FATF members have a substantial or high level of effectiveness for investigating and prosecuting terrorism finance offences. But the majority of FATF-style regional body members (75%) have either a low or moderate rating, with only a few demonstrating a substantial level of effectiveness'.

Asset freezing/seizure and sanctions

UN Security Council resolutions can call for sanctions to be imposed on individuals or groups for the prevention and suppression of terrorism and terrorist financing (FATF, 2022a). 'These measures have ranged from economic and trade sanctions to arms embargoes, travel bans, and financial or commodity restrictions' (Davis, 2020: 481). Countries are required to implement such sanctions without delay, and to 'freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity' designated in relation to UNSC resolutions on terrorism (FATF, 2022a: 13). Brzoska (2011) explains that asset freezing can take place if the relevant bodies believe terrorist groups or individuals might support or perform terrorist attacks, i.e. 'without the evidentiary standards required by the courts'.

Compliance with sanctions regimes and asset freezing/seizure requirements is monitored by the FATF (see below) as well as by the United Nations Security Council's Counter Terrorism Executive Directorate (CTED) and by the UN Sanctions Monitoring Committee, which frequently deals with elements of terrorist financing (Davis, 2020: 481). In its most recent assessment the FATF (2022b: 45) found that, '[c]ountries have made progress in establishing robust systems to identify and freeze terrorism related assets and apply targeted financial sanctions. However, the majority of countries have not yet reached sufficient levels of effectiveness'. It adds:

> For most [countries], there are still barriers to implementing UN targeted financial sanctions without delay. On average, countries take too long to transpose the entities or individuals designated by the UN Security Council. 40% of jurisdictions used, to varying degrees, terrorism finance targeted financial sanctions to freeze terrorist assets and fewer (22%) used terrorism finance confiscation measures in accordance with the relevant UN Security Council Resolutions.

Even if sanctions are applied fully and in a timely manner, the evidence on their effectiveness is weak. This is true not just of sanctions related to terrorism financing, but of sanctions in general. A recent review of sanctions on individuals found: '[t]here is consensus in the literature that individual and targeted sanctions have little power to coerce targets to make significant policy

changes…. However, individual and targeted sanctions can help constrain their targets' access to resources and ability to carry out policies, particularly when sanctions are used in combination with other measures' (Lucas, 2022: 2).

Keatinge and Keen (2020: 29) note that it is particularly challenging to sanction non-state actors that control territory, such as terrorist groups like ISIS, because these operate beyond the reach of any state's law enforcement:

> Opportunities for bringing terrorists to account by means of a judicial process or confiscating their property are therefore nugatory until legitimate government forces regain control and the group thus ceases to be territory-controlling. Although the use of sanctions is perhaps symbolically important, they are of limited direct effect as the freezing of assets and blocking of transactions that typically accompanies them will not impact their targets.

Financial intelligence

Criminalisation of terrorist financing, sanctions and seizure/freezing of assets are all designed to cut off funding to terrorists. Financial intelligence refers to the collection and analysis of financial flows and transactions in order to identify activity related to terrorist financing or money laundering. The FATF recommends that countries set up financial intelligence units (FIUs) to 'serve as the centre for the receipt and analysis of suspicious transaction reports as reported by the financial sector, as well as other information that would be relevant to money laundering and terrorism financing investigations and prosecutions' (Davis, 2020: 481). FIUs are independent and autonomous bodies, usually situated within law enforcement agencies or administrative bodies reporting to finance ministries.[4]

FIUs have to partner with private sector bodies, notably banks as well as money services businesses and other types of financial entities. The latter report to FIUs, notably providing suspicious transaction reports relating to money laundering or terrorist financing. Analysis of this information can help identify terrorist financing, and in coordination with other intelligence, can even provide details of planned/actual terrorist attacks and perpetrators. Keatinge and Keen (2020: 9-10) claim that the full potential of financial intelligence in terrorism investigations is not being realised, citing a senior intelligence officer who felt that:

> financial intelligence is not prioritised to the extent that it should be, notwithstanding the available technological capabilities for exploiting this form of intelligence. In the officer's view, the approach taken to the use of financial data is 'lagging', despite the fact that financial footprints are 'brighter than they have ever been', unlike communications data which is increasingly encrypted. Thus, if financial intelligence is integrated and overlaid with other intelligence, it can be transformative.

Bauer and Levitt (2020) also highlight how financial intelligence can be used to gather intelligence, and thereby serve as a powerful tool to disrupt terrorist financing. They cite 9/11 Commission report, which concluded: 'Expect less from trying to dry up terrorist money and more

[4] https://ec.europa.eu/home-affairs/counter-terrorism-and-radicalisation/fight-against-financing-terrorism_en

from following the money for intelligence, as a tool to hunt terrorists, understand their networks, and disrupt their operations' (Bauer & Levitt, 2020: 65).

However, Davis (2020: 481) points to some difficulties in using financial intelligence to prevent terrorism. The first is that the vast majority of reports received by FIUs relate to money laundering, financial crime and fraud, and only a tiny share relate to terrorist financing. Secondly, it can be hard to identify terrorist financing as there can be little to distinguish it from other types of financial activities (both licit and illicit). The international movement of funds – which has been a focus of CFT efforts – is not exclusive to terrorist financing. But the biggest problem is as follows (Davis, 2020: 481):

> Fundamentally, terrorist financing and the proactive identification of terrorist financing in financial data suffers from a small data problem. Money laundering and other financial crimes are plentiful, meaning that there is significant data from which to construct rules that can be used to train algorithms for proactive detection. Conversely, true cases of terrorist financing using the official banking systems are rare, and methods of financing terrorism are often jurisdictionally specific, meaning that any indicators or rules identified in one jurisdiction do not easily translate across countries. Further, terrorist financing activity is often highly dependent on the type of terrorist entity doing the financing; as the terrorism landscape shifts quickly, these trends and typologies can quickly become outdated, making any successful "rules" implemented to sift through transactional data quickly obsolete.

3. Assessing CFT effectiveness

International standards

In October 2001 the Financial Action Task Force, set up in 1989 to stop money laundering, expanded its mandate to include CFT. It also published nine special recommendations on terrorist financing, which were added to the 40 original recommendations (FATF, 2022a: 8). The latter were revised in 2012 to fully integrate CFT measures with AML controls (Ryder, n.d.: 7). Key FATF recommendations specific to CFT are (FATF, 2022a: 8; Davis, 2020: 475):

- Recommendation 5 - the criminalisation of terrorist financing. This includes financing of terrorist acts, as well as financing of terrorist organisations and individual terrorists, 'even in the absence of a link to a specific terrorist act or acts'
- Recommendation 6 - targeted financial sanctions related to terrorism and terrorist financing. This entails freezing funds and assets of persons designated by the UN Security Council.
- Recommendation 8 - measures to prevent the misuse of non-profit organisations, including by terrorist groups.

'The FATF recommendations are meant to provide specific guidance to states on how to implement the requirement to criminalize terrorist financing, help them establish mechanisms to

prevent and detect terrorist financing, and assist in the prosecution of those offences, addressing all aspects of prevention of terrorist financing' (David, 2020: 473). Together, the UN and other conventions, the FATF standards and recommendations, and legislation and actions by individual states 'are meant to create a wide net' to counter the financing of terrorism (Davis, 2020: 473; Brzoska, 2011). As well as setting standards, the FATF also produces guidance, best practice papers and provides other technical advice to member states to implement its standards (FATF, 2022a: 8).

Assessment

The core functions of the FATF include ensuring that countries are appropriately and effectively implementing its standards. As it explains: 'Global safeguards to combat terrorist financing are only as strong as the jurisdiction with the weakest measures, with terrorist financiers able to circumvent weak AML/CFT controls to successfully move assets to finance terrorism through the financial system.'[5] Assessment can help identify countries with significant weaknesses in their AML/CFT regime, and the FATF can work with them (and apply pressure on them) to strengthen their regimes.

The FATF therefore undertakes 'Mutual Evaluations' with countries. These are 'peer reviews of each member on an ongoing basis to assess levels of implementation of the FATF recommendations, providing an in-depth description and analysis of each country's system for preventing criminal abuse of the financial system'.[6] Mutual evaluations comprise of two inter-linked components:[7]

a) **Technical compliance assessment** – this 'addresses the specific requirements of each of the FATF Recommendations, principally as they relate to the relevant legal and institutional framework of the country, and the powers and procedures of competent authorities. These represent the fundamental building blocks of an AML/CFT system'. Level of compliance for each recommendation is rated as one of the following: largely compliant, partially compliant, or non-compliant.

b) **Effectiveness assessment** – this assesses 'the extent to which a country achieves a defined set of [eleven] outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results'. Ratings for level of effectiveness are one of the following: high level of effectiveness, substantial, moderate or low.

Of the eleven immediate outcomes (IOs) used to assess effectiveness, those most relevant to CFT are as follows:[8]

- **IO 9 Terrorist financing investigation and prosecution** – Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.

[5] https://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html
[6] https://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)
[7] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfissuesnewmechanismtostrengthenmoneylaunderingandterroristfinancingcompliance.html
[8] https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html

- **IO 10 Terrorist financing preventive measures and financial sanctions** – Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO[9] sector.

Countries that fall short are offered technical assistance by the FATF. However, it also uses a 'name and shame' strategy to encourage compliance. The FATF produces two lists of countries based on their implementation of AML/CFT measures (Davis, 2020: 476):

a) Blacklist – countries with 'strategic deficiencies' in their AML/CFT regimes that 'pose a risk to the international financial system'. As of February 2019 the only names on the list were Iran and North Korea.
b) Greylist - countries with strategic deficiencies that are subject to an action plan (i.e. on-going process underway). As of February 2019, names on the list were: The Bahamas, Botswana, Cambodia, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen.

Davis (2020: 476) explains that, 'Presence on either of these lists can have implications for countries in terms of financial inclusion, correspondent banking relationships, and loans from the International Monetary Fund (IMF)'. However, she adds that the mutual evaluation process has come under criticism for being politicised.

Challenges

Brzoska (2011) is highly critical of the FATF's approach (and that of other bodies such as the IMF and World Bank) to assessing the effectiveness of CFT measures. He argues that these focus on outputs and outcomes, rather than on impact.

> Instead of assessing impacts of CTF measures, most official evaluations focus on output, on the adoption of agreed principles and best practice, and outcome, their implementation. Assessments are predominantly made against 'best practice' standards and regulations and not against evidence of benefits in reducing terrorist activity. They thus tend to identify implementation deficits, generally recommending remedies requiring additional CTF measures. Attempts to assess the actual effectiveness and efficiency of particular measures in reducing terrorist attacks are rare (Brzoska, 2011: 3).

Brzoska says such 'process oriented' assessments lead to recommendations for expansion of CFT measures – making the whole process even more divorced from what is actually happening in terms of terrorist activity.

However, Brzoska also acknowledges the difficulties in assessing impact, not least because of the dearth of available data, and the lack of a clear link between CFT and preventing terrorist attacks. On the former, he notes that some data is publicly available in some countries, e.g. Suspicious Activity Reports (SARs) and frozen assets, but 'much information is either secret or difficult to assess' (Brzoska, 2011: 10). Examples include financial transactions for the prevention of terrorist attacks, and the prosecution of terrorist groups. On the latter – establishing causality –

[9] Non-profit organisations.

he notes that, ‘there is very little publicly available information on attacks that were planned but did not take place – it is often difficult to assess whether or not lack of finance was a factor’ (Brzoska, 2011: 10-11).

Davis (2020: 485) identifies some measures of effectiveness of CFT measures, including ‘prosecutions of terrorist financing activities, which can include both operational and organisational financing by individuals within a specific jurisdiction, or the prevention of the establishment of entities for the purposes of terrorist financing’. She adds that, even where prosecution is not possible, ‘disruption of terrorist financing activities should still be considered a measure of success’. However, as Brzoska noted above, the challenge is in actually measuring these.

Despite their lack of focus on impact, Brzoska acknowledges the pressure for assessments, given that terrorism is such a major concern for the general public: ‘[p]olicy makers thus must demonstrate activity even in the absence of evidence of the effectiveness of activities. Because they cannot use standard measures of effectiveness, instead they may prefer to base their decisions on other considerations and factors, such as path-dependent behaviour, policy linkages, major events or outside pressures (Brzoska, 2011: 2).

Brzoska (2011: 11) suggests that an alternative approach to assessment could be to survey relevant audiences, though he accepts that results are not uniform nor very reliable:

> In the UK, in a report funded by the City of London in 2004, the average score of responses from the wider financial community to the question of the effectiveness of money laundering activities, including CTF, was quite high. On the other hand, in another survey of persons from the financial sector in Germany, Singapore and Switzerland, scepticism was high, and these activities were generally seen as ineffective.

In assessing effectiveness of CFT measures, it is also important to take into account negative consequences of these. Given the stress on NPOs, and ensuring these are not exploited by terrorist groups, greater regulation of financial flows could make it harder for charitable organisations to mobilise and access funds. A related concern is that, particularly in fragile and conflict affected states, it can make it difficult for humanitarian actors to operate where some engagement is needed with groups designated as terrorist. This, in turn, can have knock-on effects on the work they do and the assistance and services they can provide. Mackintosh and Duplat (2013: 12) note that: ‘The concern about the negative impact of counter-terrorism measures on humanitarian action is a pressing one because areas in which non-state armed groups designated as terrorist are often those where humanitarian needs are greatest’. They give case studies of the negative impact of CFT measures targeting Al-Shabab on humanitarian action in Somalia, and targeting Hamas in occupied Palestinian territory (Mackintosh & Duplat, 2013).

Similar negative effects can be seen on many legitimate businesses and entities, in particular in developing countries where many operate in the informal economy, and in particular money services businesses. The restrictions and reporting requirements imposed by CFT measures can make it difficult for them to operate. However, current assessments of CFT implementation do not seem to take these unplanned negative consequences into account.

4. Do CFT measures prevent terrorism?

As Brzoska (2011) points out, the real test of impact of CFT measures is whether they prevent terrorist attacks and facilitate the detention of terrorist groups and individuals. So, do they work?

According to Bauer and Levitt (2020: 67) they do:

> Disrupting terrorists' financial transactions makes it harder for them to travel, bribe officials, procure materials, provide for their own families, and, ultimately, engage in operations. Denying terrorists—as well as insurgents and proliferators—easy access to financial tools forces them to use more costly, less efficient, and often less reliable means of financing their activities.

Bauer and Levitt (2020: 67) acknowledge that new challenges – notably self-funded loner terrorists and territory-controlling (protostate) terrorist groups – mean specific CFT tactics and procedures might have to be adjusted. But they reject criticism that traditional tools are 'ineffective at preventing the kinds of self-funded attacks that have recently become common', arguing that 'such attacks often cost more than meets the eye; because even the cheapest attack is not free, when terrorists are frozen out of their bank accounts, they have to resort to riskier tactics'. They give the example of Ismail Issa, an ISIS[10] operative arrested while travelling from Germany to Syria (Bauer & Levitt, 2020: 67):

> The group had to send Issa with cash to shop for supplies rather than wiring money to an operative already in the country, precisely because it had become too difficult for IS members to transfer money without being picked up by the authorities. In this case, as in others, jihadists have grown so worried that their transactions are being monitored that they are too scared to collect the funds.

Their conclusion, in the words of then US Treasury Undersecretary David Cohen speaking in 2010, is (Bauer & Levitt, 2020: 67):

> We have no illusion that we can entirely prevent the flow of funds to terrorist groups. Some funds will find a way to flow. But that does not mean the effort is futile—far from it. What we have learned is that by deterring would-be funders and disrupting the financial facilitation networks, we significantly impede terrorists' ability to operate.

Davis (2020: 485), while not quite as assertive about the positive impact of CFT measures in preventing terrorism, essentially reaches the same conclusion: that they can make it harder for terrorist groups to operate (e.g. by necessitating funding arrangements to move 'underground') but will not be able to block them altogether. She identifies a number of reasons for this (Davis, 2020: 485):

- In practice, most terrorist groups, regardless of CFT activities aimed at them, have sufficient means to launch terrorist acts if not whole campaigns. Part of this challenge lies in the fact that many sources of terrorist funds are impervious to counterterrorism financing initiatives. For instance, many terrorist groups exploit the economic activity in

[10] Islamic State in Syria and Iraq, also referred to as Daesh.

the area where they are operating through taxation or extortion of funds from the local population. Restricting international financial flows or sanctioning those groups will have little impact on their ability to raise funds.

- Further, many terrorist groups employ money movement mechanisms outside of well-regulated sectors, using cash couriers or trade-based money laundering to move money for operational activities.
- Most terrorist cells *(of larger terrorist groups)* (and indeed, individual attackers) self-fund a good portion of their attack plans (which often cost very little), meaning that stopping the financing of these cells and individuals falls squarely on domestic/local law enforcement or security services, with little space for international CFT actors.

A recent article by Vision of Humanity (n.d.) identifies similar weaknesses in the current CFT framework:

1. **Developing countries are typically cash-based** – lots of transactions in such countries happen with cash, leaving no records or paper trail, and thus making monitoring of financial flows, and therefore enforcement of regulations, 'virtually impossible'. A related challenge is that such countries often have porous borders which are difficult to patrol, so terrorist groups can easily move funds across borders.
2. **Terrorist groups adapt quickly to new financing opportunities** – like organised crime groups (OCGs), terrorist organizations are able to quickly adapt, both taking advantage of new opportunities to raise funds, and of new technologies and instruments to move funds, e.g. crypto-currencies, Paypal (and other internet based payment services). Keeping track of rapidly evolving terrorist financing is a challenge.
3. **Terrorist groups can rely on self-funded individuals to carry out attacks** – some terrorist attacks can be very cheap to carry out, e.g. using vehicles, so groups can rely on self-funded individuals to perpetrate these.

Keatinge and Keen (2020) similarly question the overall design of the CFT regime. They note that it was designed in the wake of the 9/11 attacks, primarily to cut off funding to Al-Qaeda through the formal financial system. However, the terrorism and terrorism financing environment has changed drastically since then: sources of funding for terrorist groups have diversified; the nature of those carrying out terrorist attacks has changed, with lone actors/small cells as well as territory-controlling groups such as ISIS; and means of moving funds have also diversified, with less reliance on the formal financial system in place of new technologies and new payment systems. Given the major changes in the terrorist threat, they call for the post-9/11 CFT model to be reformed:

> The foundational elements of that model, including the criminalisation of terrorist financing, remain relevant. Other aspects, such as the focus on wire transfers and charities, while still relevant against certain risks today, reflect the specifics of the terror finance threat landscape at the time. However, that landscape has evolved, and so too should the global response (Keatinge & Keen, 2020: vii).

Keatinge and Keen (2020: ix-x) make a number of recommendations for CFT reform:

- clarify the objectives of CFT measures (ensuring these are risk-based and achievable);
- develop evidence-based CFT strategies;
- make greater use of financial intelligence;
- promote collaboration between counterterrorism and law enforcement officials, between public and private sectors, and between countries and within regions;
- and engage more actively with risks posed by new technologies.

Keatinge and Keen (2020) also claim that sometimes military force to destroy terrorist (controlled) assets or sources of funds, can be a more effective means of depriving them of funds than traditional CFT measures. 'Operations against ISIL are a case in point. According to one former US government official, the best CTF advice the US Treasury had during the height of ISIL's activity was to drop bombs on revenue generating assets such oil wells and tankers, as well as cash storage facilities' (Keatinge & Keen, 2020: 30).

5. Examples of success

Disruption of cyber-enabled terrorism financing[11]

In 2020 the US Justice Department announced the dismantling of three terrorist financing cyber-enabled campaigns, involving the al-Qassam Brigades (Hamas's military wing), al-Qaeda, and Islamic State of Iraq and Syria (ISIS). The coordinated operation represents the US government's largest-ever seizure of cryptocurrency in the terrorism context.

The three terror finance campaigns all relied on sophisticated cyber-tools, including the solicitation of cryptocurrency donations from around the world. The action demonstrates how different terrorist groups have similarly adapted their terror finance activities to the cyber age. Each group used cryptocurrency and social media to garner attention and raise funds for their terror campaigns. US authorities seized millions of dollars, over 300 cryptocurrency accounts, four websites, and four Facebook pages all related to the criminal enterprise.

Al-Qassam Brigades Campaign - The first action involved the al-Qassam Brigades and its online cryptocurrency fundraising efforts. In the beginning of 2019, the al-Qassam Brigades posted a call on its social media page for bitcoin donations to fund its campaign of terror. The al-Qassam Brigades then moved this request to its official websites, alqassam.net, alqassam.ps, and qassam.ps. The group boasted that bitcoin donations were untraceable and would be used for violent causes. Their websites offered video instruction on how to anonymously make donations, in part by using unique bitcoin addresses generated for each individual donor. However, such donations were not anonymous. Working together, IRS, HSI, and FBI[12] agents

[11] This write-up is entirely adapted from the US Justice Department's article: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns
[12] Inland Revenue Service, Homeland Security Investigations and the Federal Bureau of Investigations.

tracked and seized all 150 cryptocurrency accounts that laundered funds to and from the al-Qassam Brigades' accounts. Simultaneously, law enforcement executed criminal search warrants relating to US-based subjects who donated to the campaign. With judicial authorization, law enforcement seized the infrastructure of the al-Qassam Brigades websites and subsequently covertly operated alqassam.net. During that covert operation, the website received funds from persons seeking to provide material support to the terrorist organization, however, they instead donated the funds bitcoin wallets controlled by the United States.

Al-Qaeda Campaign - The second cyber-enabled terror finance campaign involved a scheme by al-Qaeda and affiliated terrorist groups, largely based out of Syria. These organizations operated a bitcoin money laundering network using Telegram channels and other social media platforms to solicit cryptocurrency donations to further their terrorist goals. In some instances, they purported to act as charities when, in fact, they were openly and explicitly soliciting funds for violent terrorist attacks. For example, one post from a charity sought donations to equip terrorists in Syria with weapons. Undercover HSI agents communicated with the administrator of Reminder for Syria, a related charity that was seeking to finance terrorism via bitcoin donations. The administrator stated that he hoped for the destruction of the United States, discussed the price for funding surface-to air missiles, and warned about possible criminal consequences from carrying out a *jihad* in the United States. Al-Qaeda and the affiliated terrorist groups together created these posts and used complicated obfuscation techniques, uncovered by law enforcement, to layer their transactions so as to conceal their actions.

ISIS Campaign - The final action combined the Department's initiatives to combat COVID-19 related fraud with combatting terrorism financing. It is related to a scheme by Murat Cakar, an ISIS facilitator responsible for managing select ISIS hacking operations, to sell fake personal protective equipment via FaceMaskCenter.com. The website claimed to sell FDA approved N95 respirator masks, when in fact the items were not FDA approved. Site administrators claimed to have near unlimited supplies of the masks, in spite of such items being officially-designated as scarce. The site administrators offered to sell these items to customers across the globe, including a customer in the United States who sought to purchase N95 masks and other protective equipment for hospitals, nursing homes, and fire departments. The authorities seized Cakar's website as well as four related Facebook pages used to facilitate the scheme. With this third action, the US averted the further victimisation of those seeking COVID-19 protective gear, and disrupted the continued funding of ISIS.

US efforts to stop ISIS funding[13]

The response to the challenge of ISIS financing ultimately mirrored two traditional and interdependent objectives that stood as the cornerstone of counter-terrorist financing efforts: (1) cut terrorists off from their source of funds and (2) deny them access to the global financial system. By suspending salaries to Government of Iraq employees in ISIS-controlled territory, authorities succeeded in lessening the liquidity for ISIS to tax and extort. The bombing of ISIS-controlled oil facilities and cash vaults hindered ISIS oil sales and destroyed one-time windfalls taken from banks vaults. Cutting off bank branches and exchange houses in and

[13] This write-up is entirely adapted from Bauer & Levitt, 2020: 65-66.

around ISIS-controlled territory made it harder for the group to move funds to support affiliates, foreign fighter travel and procurement efforts.

[Financial intelligence] and public-private partnerships focused on identifying and curbing illicit financial activity have proven particularly effective. In one particularly telling case, private sector financial data gleaned by finance ministries and shared with US military and law enforcement agencies helped identify financial targets for military strikes on ISIS oil infrastructure and cash depots. Ultimately, it was the territorial defeat of the caliphate that had the greatest impact on the organisation's financial footings.

Terrorist Finance Tracking Programme[14]

The Terrorist Finance Tracking Programme (TFTP) was set up by the US Treasury Department shortly after the 9/11 terrorist attacks. It allows the issuance of legally binding production orders to SWIFT[15] - a Belgium-based company with US offices that operates a worldwide messaging system used to transmit financial transaction information – seeking information on suspected international terrorists or their networks. Under the terms of the subpoenas, the US Government may only review information as part of specific terrorism investigations.[16] On 1 January 2010, SWIFT changed its messaging architecture, storing data in two processing zones – one zone in the United States and the other in the European Union. A new agreement was signed between the US and EU on the processing and transfer of information to the US Treasury Department.

TFTP has a number of advantages with regard to financial intelligence for CFT (EC, 2013[17]):

- It contains unique, highly accurate information that is of significant value in tracking terrorist support networks and identifying new methods of terrorist financing. In cases where little is known about a terrorism suspect beyond the individual's name or bank account number, TFTP-derived information can reveal critical pieces of information, including locations, financial transactions, and associates.
- The unique value of the TFTP lies in the accuracy of the banking information, since the persons concerned have a clear interest in providing accurate information to ensure that the money reaches its destination.
- As a result of the precision of the TFTP data, even when suspects are very careful with their bank transactions, it has also been possible to locate them through the payments and purchases of their close associates.
- The TFTP can provide key information about the movements of suspected terrorists and the nature of their expenditures. Even the 'non-activity' of one or more bank accounts tied

[14] This write-up is entirely adapted from Bauer & Levitt, 2020: 66-67.
[15] Society for Worldwide Interbank Financial Telecommunication
[16] https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp

[17] This write-up is entirely adapted from the European Commission's 2013 report on the value of TFTP provided data. (EC, 2013).

to a suspected terrorist, in terms of transactions, is a useful indicator of the possible departure of a suspect from a certain country.

- Based on the TFTP, it has been possible to obtain information on U.S. and EU citizens and residents suspected of terrorism or terrorist financing in third countries where requests for mutual legal assistance were not responded to in a timely manner.
- TFTP-derived information allows investigators to identify new streams of financial support and previously unknown associates, link front entities and aliases with terrorist organisations, evaluate/corroborate existing intelligence, and provide information that can be used to identify new targets for investigation.
- TFTP provides key insight into the financial support networks of some of the world's most dangerous terrorist organisations, including Al-Qaida, Al-Qaida in the Lands of the Islamic Maghreb (AQIM), Al-Qaida in the Arabian Peninsula (AQAP), Al Shabaab, Islamic Jihad Union (IJU), Islamic Movement of Uzbekistan (IMU), and Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF).

Bauer and Levitt (2020: 66-67) list the following achievements for TFTP:

- TFTP produced more than 18,000 financial intelligence (FININT) leads that US authorities shared with their European counterparts through February 2016.
- The TFTP has successfully intercepted many illegal transactions and thwarted many plots, such as threats to the 2012 Summer Olympic Games in London and a 2011 assassination plot to kill the Saudi Arabian Ambassador to the United States.
- In the case of small-scale plots by lone offenders or small groups, where international transactions are less likely to take place, TFTP has still been an effective investigative tool in the wake of an attack. It did this in the investigations that followed the 2013 Boston bombings, the January 2015 shooting at the offices of the magazine Charlie Hebdo, and the November 2015 attacks in Paris.

6. References

Brzoska, M. (2011). *The Role of Effectiveness and Efficiency in the European Union's Counterterrorism Policy: The Case of Terrorist Financing*. Economics of Security Working Paper 51, Berlin: Economics of Security.

Bauer, K. & Levitt, M. (2020). 'Funding in Place: Local Financing Trends Behind Today's Global Terrorist Threat'. *Evolutions in Counter-Terrorism*, Vol. 2 (November 2020): 47-76. The International Centre for Counter-Terrorism – The Hague (ICCT). https://icct.nl/app/uploads/2020/12/Special-Edition-2-3.pdf

Davis, J. (2020). ‘Chapter 14: Prevention of Terrorist Financing’ in Schmid, A. (ed.), *Handbook of Terrorism Prevention and Preparedness*. (The Hague, ICCT Press). https://icct.nl/app/uploads/2021/10/Chapter-14-Handbook.pdf

European Commission (EC) (2013). *Joint Report from the Commission and the US Treasury Department regarding the value of TFTP provided data.* https://ec.europa.eu/home-affairs/system/files/2020-09/20131127_tftp_annex_en.pdf

FATF (2022a). *International standards on combating money laundering and the financing of terrorism & proliferation*. Financial Action Task Force, updated March 2022. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FATF (2022b). *Report on the state of effectiveness and compliance with the FATF standards*. Financial Action Task Force, April 2022. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Report-on-the-State-of-Effectiveness-Compliance-with-FATF-Standards.pdf

Keatinge, T. & Keen, F. (2020). *A sharper image: Advancing a risk-based response to terrorist financing*. Royal United Services Institute (RUSI). https://rusi.org/explore-our-research/publications/occasional-papers/sharper-image-advancing-risk-based-response-terrorist-financing

Mackintosh, K. & Duplat, P. (2013). *Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action*. UN OCHA and Norwegian Refugee Council. https://www.nrc.no/globalassets/pdf/reports/study-of-the-impact-of-donor-counterterrorism-measures-on-principled-humanitarian-action.pdf

Maza, K., Koldas, U. & Aksit, S. (2020). ‘Challenges of combating terrorist financing in the Lake Chad region: A case of Boko Haram’. *SAGE Open* (April-June 2020). https://journals.sagepub.com/doi/full/10.1177/2158244020934494

Vision of Humanity (n.d.). ‘Preventing Terrorist Financing: Are regulations enough?’ https://www.visionofhumanity.org/combating-the-financing-terrorism/

Key websites

- Financial Action Task Force (FATF): https://www.fatf-gafi.org/home/

Suggested citation

Idris, I. (2022). *Effectiveness of Different Methods to the Counter Financing of Terrorism.* K4D Helpdesk Report 1133. Brighton, UK: Institute of Development Studies. DOI: 10.19088/K4D.2022.091

About this report

This report is based on six days of desk-based research. The K4D research helpdesk provides rapid syntheses of a selection of recent relevant literature and international expert thinking in response to specific questions relating to international development. For any enquiries, contact helpdesk@k4d.info.

K4D services are provided by a consortium of leading organisations working in international development, led by the Institute of Development Studies (IDS), with Education Development Trust, Itad, University of Leeds Nuffield Centre for International Health and Development, Liverpool School of Tropical Medicine (LSTM), University of Birmingham International Development Department (IDD) and the University of Manchester Humanitarian and Conflict Response Institute (HCRI).